



MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

Open University of Cyprus
Faculty of Economics and Management

Master's Joint Degree Programme
Enterprise Risk Management (ERM)

Master Thesis

Crisis Information Management (CIM) in
Intergovernmental Organizations

(Effect of Information Management Factors to Crisis &
Business Continuity Management)

IOANNIS REMATISIOS

SUPERVISOR: Dr Anastasis PETROU

MAY, 2022



MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

This page is intentionally left blank

Table of Contents

Table of Contents3

Chapter 1: Introduction7

1.1 Problem Formulation, Aim and Objective7

Chapter 2: Literature Review9

2.1 Initial literature review9

2.2 Extended literature review17

Chapter 3: Intellectual Framework29

3.1 PPT framework29

3.2 PPRR framework30

3.3 ISO 22301:2019 Security and resilience – BCMS35

Chapter 4: Methodology and Methods37

4.1 Limitations40

4.2 Disclaimer notes40

4.3 Sources and Data41

4.4 Key Words42

4.5 Survey questionnaire formulation42

Chapter 5: Findings and Analysis46

5.1 1st Iteration – Findings form initial literature analysis46

5.2 2nd Iteration – Survey results and consolidated comments49

5.3 3rd Iteration – Analysis from additional literature and previous results68

5.4 Additional Discussion72

Chapter 6: Conclusions – Recommendations79

References83

ANNEX I: Abbreviations & Acronyms89

ANNEX II: Main Definitions90

List of Figures

Figure 1: Sapriel crisis management model (CS&A)9

Figure 2: Jaques (2007), crisis management model10

Figure 3: Kash & Darling 1995 Model analysis (crisis cycle flow chart)11

Figure 4: The development of business continuity management – periods, drivers, and practices; Herbane B. (2010)12

Figure 5: Development of issues with & without management intervention; Gonzalez-Herrero & Pratt (1995)13

Figure 6: Elements for Effective Information Management, Meesters K., 2021, Crisis Information Management: From Technological Potential to Societal Impact15

Figure 7: Business contingency planning and Integrated business contingency framework (Sapriel, © 1991-2019 CS&A). For the purpose of this paper figures are merged & edited by the author to stress their relationship.20

Figure 8: High reliability management: a nominal crisis cycle; P.R. Schulman, E. Roe / Policy and Society 30 (2011) p.132.21

Figure 9: OCHA, The UN Cluster Approach in Crisis Management; Humanitarian Crisis Management and Humanitarian Civil-Military Coordination; Presentation from R. Reario (NATO Crisis Management course, 12 May 2021)23

Figure 10: MIDAS Process diagram (IOM, 8 Feb. 2021)25

Figure 11: Displacement Tracking Matrix (DTM), UN – IOM, 2019, <https://emergencymanual.iom.int/entry/19108/displacement-tracking-matrix-dtm>26

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

*Figure 12: PPT framework explained from an Information & Knowledge Management (IKM) perspective*²⁹

*Figure 13: PPRR Framework model basic concept*³⁰

*Figure 14: Sapriel 2003, BCM model, Prevention level – reduction of risk*³¹

*Figure 15: Learning Barrier Model (Veil, 2011) – Response level*³²

*Figure 16: Risk and crisis management in facilities, Model of L. Barton & D. Hardigree, in Facilities, Vol.13 Aug 1995, MCB University Press*³³

*Figure 17: Three-Stage Crisis Cycle (Veil, 2011)*³⁴

*Figure 18: PPRR as Business Continuity Management Framework*³⁴

*Figure 19: PDCA Model, ISO 22301:2019 Implementation Guide, T. Bevan, UK*³⁶

*Figure 20: Research methodology schema based on Grounded Theory*³⁷

*Figure 21: Overall occurrence of terms in CIM context per IM factor (PPT) (Average values of observations from all 20 articles reviewed per factor)*⁴⁶

*Figure 22: Demographics of survey participants per area of expertise*⁴⁹

*Figure 23: Chart for survey Question 1*⁵⁰

*Figure 24: Chart for survey Question 2*⁵¹

*Figure 25: Chart for survey Question 4*⁵⁷

*Figure 26: Chart for survey Question 5*⁵⁸

*Figure 27: Chart for survey Question 6*⁵⁹

*Figure 28: Chart for survey Question 7*⁶⁴

*Figure 29: Chart for survey Question 8*⁶⁵

*Figure 30: Chart for survey Question 9*⁶⁶

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

Figure 31: 2021-2023 Emerging Technology Roadmap for Large Enterprises, Deployment risks and enterprise values (Gartner, 2021)75

Figure 32: Deloitte, DI_2021-Tech-Trends, TechTrends2021-Delloitte, Macro technology forces, Taxonomy for emerging tech.77

Figure 33: Triple Helix model for Crisis Information Management (CIM) (Rematisios, 2022)81

Figure 34: IGO Crisis Information Management (CIM) Constellation, Rematisios _82

List of Tables

Table 1: Organizations with which survey participants have had work experience41

Table 2: Survey questionnaire45

Table 3: Code/terms per IM factor46

Table 4: IM code legend46

Table 5: Code identification - Code/terms appearance within the context of PPT framework47

Table 6: Data results from survey Question 150

Table 7: Data results from survey Question 251

Table 8: Data results from survey Question 457

Table 9: Data results from survey Question 558

Table 10: Data results from survey Question 659

Table 11: Data results from survey Question 764

Table 12: Data results from survey Question 865

Table 13: Data results from survey Question 966

Table 14: Average score of PPT factors per publishing time-period68

Chapter 1: Introduction

1.1 Problem Formulation, Aim and Objective

Heretofore, published research in crisis management (CM) and business continuity management (BCM) has provided a reasonably good focus on models and frameworks which mention people, process, and technology, as critical elements of the crisis information management (CIM) paradigm.

Yet, there is paucity in the development of theory and empirical outputs with a direct focus on people, process, and technology (hereinafter PPT) from within the CIM research paradigm where the above three areas are of vital concern in their entanglement and in relation to crisis management and business continuity management. Furthermore, lack of interdisciplinary knowledge within crisis and business continuity management about CIM and its core PPT areas is outstripping professional ability to make more connected decisions using technologies in a more sophisticated manner to link people and processes during business continuity management efforts. As a result, there is no common approach from the scholars on the balance between the three PPT areas during any of the crisis phases.

Subsequently, a study is proposed herein aiming to critically and with a multidisciplinary approach, discuss the various implications and complexity of Information Management (hereinafter IM) factors that can affect crisis and business continuity management for Intergovernmental Organizations (IGOs). The initial aim is to examine an indicative sample of related literature and provide an understanding of the interdependencies between “people” “process” & “technology” (as basic IM elements), during crisis and business continuity management. Targeted survey is intended to explore the perception and understanding of the field experts on the topic and identify any subjectivity gap that may arise by the perception of the importance level that is given to each of the three IM elements (people, process, technology). The dissertation will build on existing knowledge base, using existing theories such as the

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

PPRR model (Prevention, Preparedness, Response & Recovery), and explore the idea of a multidimensional theoretical model that would include interdependencies of the three examined IM elements (factors) of the study.

The main objectives of this paper are considered the following:

- ✚ Identify the relationship and impact of “technology” on “people” in IM for business continuity and crisis management.
- ✚ Identify the relationship and impact of “technology” on “processes” in IM for business continuity and crisis management.
- ✚ Analyze data from survey regarding perception on balance of PPT factors within a general PPRR framework, and from an IGO point of view.
- ✚ Enhance existing theories or address new perceptions considering the research outcome, that benefit the effectiveness of IGOs from a CIM perspective.

Benefits from this study include accomplishment of its aim and objectives but also contributing to professional knowledge in CIM as an interdisciplinary area of theory and empirical research. Furthermore, other benefits from this study include the way the three IM factors interact in existing theoretical frameworks, and a more direct understanding of the importance of CIM in my area of professional work from a business continuity management perspective.

Chapter 2: Literature Review

2.1 Initial literature review

Targeted literature review includes articles, journals, papers on CIM, crisis management and business continuity on international organizations, digital transformation on business continuity, contingencies planning for uncertainty, etc. Selected articles are mainly based on core theoretical frameworks in the field of crisis and business continuity management. Content is expected to be more “process” oriented; however, this is an intentional effort to create a baseline based on fundamental theories of the subject from recognized authors.

We first look for “information management” content in theoretical framework articles and within the context of our research subject. The later is a challenge and requires careful analysis of the context to ensure relativity with CIM and the pertinent PPT factors.

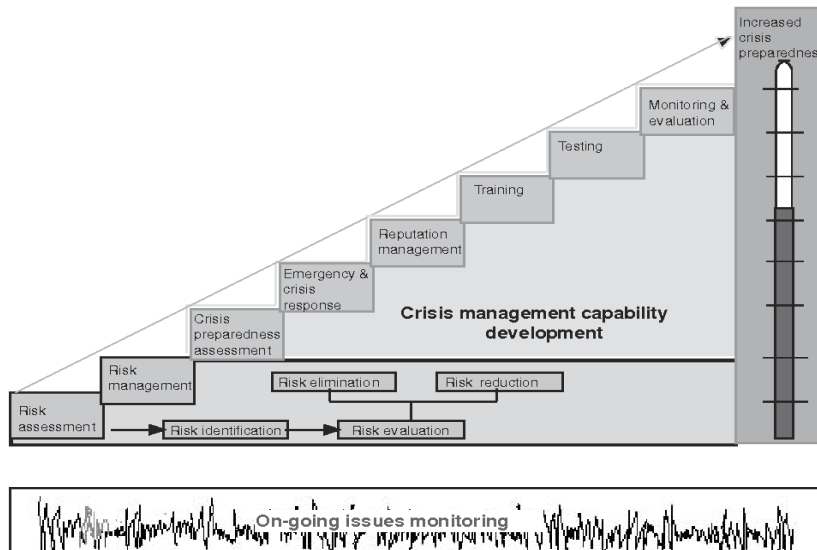


Figure 1: Sapriel crisis management model (CS&A)

According to Sapriel, his stepladder CM model, is a type of self-assessment model for organizational level of crisis preparedness; not in a scientific way, but in an aspirational way. Therefore, it cannot be used to calculate the maturity level of crisis preparedness. The on-going efforts to monitor and assess the way the organization is

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

prepared to respond to a crisis, either in a calculative or a progressive manner, is taken for granted. According to Sapriel the model is not a destination, but rather a journey, which is not reflected in the schema where relations appear very linear. Management of risks and complex problems require mandates from top hierarchy of the organization to implement crisis management (“people” focus). Sapriel emphasizes the importance of training and testing and the need for endorsement by senior management.

Nevertheless, the way training and testing are placed in this stepladder process model type by Sapriel can be easily misunderstood. Both training and testing should be part of continues improvement irrelevant to the occurrence of a crisis. It is a preparation and readiness activity of people, processes and tools (technology) that also helps on the evaluation and lessons-learned at the aftermath of a crisis. For this purpose, it is important that firms continuously update their crisis response plans after enduring a crisis and this applies also to IGOs. The two steps of training and testing can be executed via modeling and simulation tools, scenario exercises, testing of contingency plans or partially crisis response plans, with allocated budget.

A more non-linear holistic view to crisis management is the model illustrated by Jaques, where post-crisis activities loop back to preparing and managing future crisis, while clusters and activities can also overlap (Jaques, 2007: 150-151).

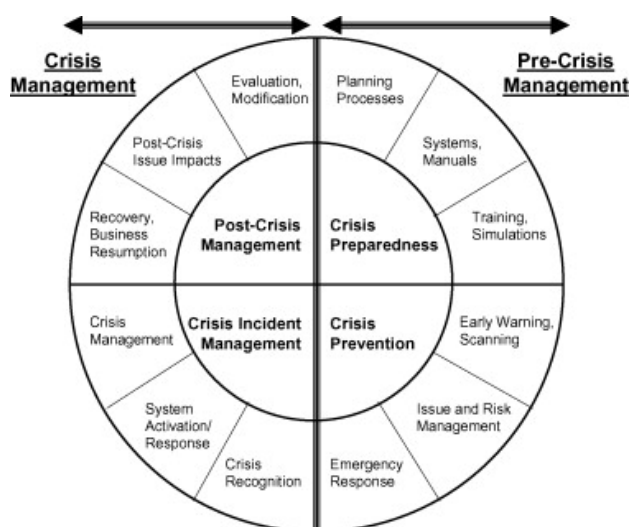


Figure 2: Jaques (2007), crisis management model

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

From a PPT framework perspective Jaques heavily focus on process related notions while describing their models, leaving very little to technology or tools.

Kash and Darling in their model analysis they also emphasize the role of “people” in a cycle flow chart from prodromal to resolution stage.

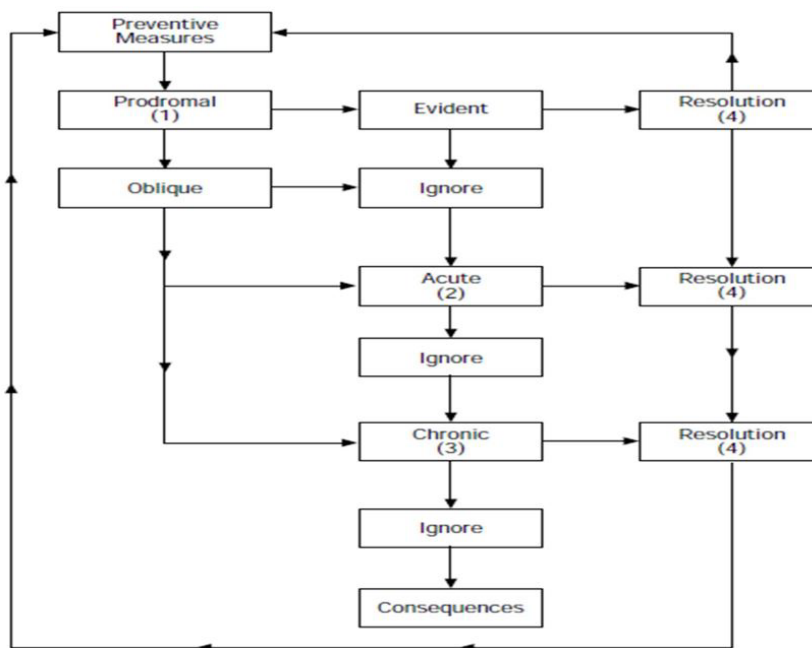


Figure 3: Kash & Darling 1995 Model analysis (crisis cycle flow chart)

Kash & Darling explored a dynamic environment of enterprises where crisis may be inevitable and possibly intense, despite all the efforts to detect the operating environment. The critical factor in this model is not just the recognition of the crisis but to achieve this in due time, in order to address all the issues and plan accordingly. Great importance is given to the identification the early signals at the first (prodromal) phase of a crisis which is difficult to detect (despite any preventive measures in place). Evaluation of data is required to determine the nature of the crisis. Early signals can be theoretical or technical and we should return to this notion at a later analysis stage.

The approach continues with schematics that present the anatomy of the crisis, and possible corrective actions or interventions when required. In the acute crisis stage symptoms demand urgent attention and corrective action, like diverting funds or other

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

resources to confront the emerging situation. Kash & Darling allude to the balance between the three IM factors (people, process and technology) in terms of strategic planning and contingency forecasting, where successful crisis management would come from prevention and preparation of the organization followed by accurate intervention (Kash & Darling, 1998: 181-185). In chronic crisis stage organizations are used to “quick-fix” approaches and reach the point of immediate action by management once and for all as there is no alternative anymore.

Herbane (2010) on the other side, investigates the regulatory and legislative history of the last 4 decades, relating to BCM as a management practice, and its evolution in terms of period, drivers, and practice.

Period:	Drivers:	Practice:	Nature of Progress:
Mid-1970s → mid-1990s	Emerging legislation	Disaster Recovery Planning ↓ Business Continuity Planning	Development ↓
Mid-1990s → 2001	Emerging standards	Business Continuity Management	↓
2002 → 2005	Acceleration and focus	↓	Diffusion ↓
2006 → 2010	Competing standards and breakout	↓	Standardisation?

Figure 4: The development of business continuity management – periods, drivers, and practices; Herbane B. (2010)

Indirectly, he analyses the “process” perspective of the PPT IM framework, and argues that the events of 9/11 2001 was fundamental, that triggered many changes to BCM practices, followed by an acceleration in the “*introduction of, and greater focus upon, guidelines, standards and legislation requiring organizations to have and develop business continuity planning capabilities*” (Herbane, 2010: 292). This acceleration of competing standards transformed practices in both industrial and national context, which led to the creation of international standards.

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

From the “people” point of view, along with the need of internal practitioners and professional certification of the organization, Herbane emphasizes the importance of external stakeholders and their accountability, such as national and local governments, network participants like supply chain partners, industry associations and technology service providers (Herbane, 2010: 994). The later stretches to the technology theme of PPT framework underlining the strategic role of BCM in terms of understanding vulnerabilities deriving from technology failure like in IT/cyber-security, pandemics/vaccination research and terrorism (Herbane, Elliott & Swartz, 2004).

According to Gonzalez-Herrero and Pratt, there are four phases in their crisis management process model.

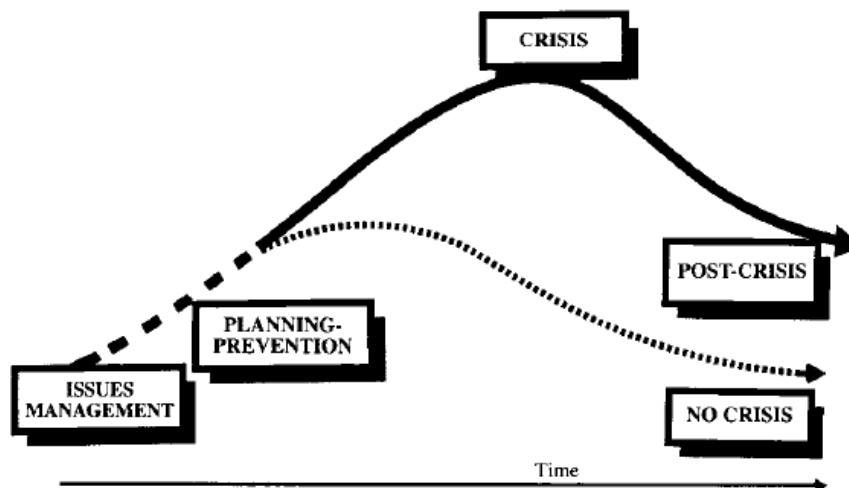


Figure 5: Development of issues with & without management intervention; Gonzalez-Herrero & Pratt (1995)

First, the issues management where we scan the environment and look for trends as hints for the near future, and collect data on potential issues and evaluate them, while we create a communication strategy in an attempt to prevent the occurrence of a crisis. Second is planning-prevention phase, where we use information, warning, and internal communications systems (Gonzalez-Herrero and Pratt, 1995: 27-28). During planning we exercise activities of crisis management process as starting point especially when crisis is recognized as imminent. Some of the activities are to set a proactive policy and

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

analyze organization's links with its constituencies, preparing contingency plans. Designate members of crisis management team and determine communication plan. Assess the dimensions of the crisis and the level of control that the organization has over the crisis, while determining the various options available for specific courses of action.

Third phase is the crisis where organization has lost all proactive initiatives and its response is limited to reacting to crisis event and using contingency measures to reduce damage or negative consequences. This stage includes evaluation of the response to the crisis, communication with constituencies on the actions being taken to solve the problems, attempting to obtain support from experts and implement internal communications program. Last phase is the post-crisis where organization continues to communicate and inform stakeholders, monitor issues until their impact is reduced, and evaluate the effectiveness of the existing crisis plan as well as the response by the management and employees of the organization with the aim to incorporate the feedback into an improved plan with long-term communications strategy for future crisis (Gonzalez-Herrero, Pratt: 29).

Return to "normality" is a rather subjective statement. Recovery point at the post-crisis stage is not an absolute return to the initial status at pre-crisis stage. The new reality may be considered as a point of the new normality with the experience and lessons-learned from the crisis event, that moves the "normality" to a different level.

Hecht (2002) addresses the differentiation between continuity (which avoids or minimizes the impact of a failure), and recovery which presupposes an event that cause failure. In business continuity and from strictly IT standpoint, the main requirements are availability and connectivity (Hecht, 2002: 448). In Hecht's approach, with availability, organizations need the right people with the right skills to have rehearsed different crisis scenarios with documented processes to retrieve and process the data and make it available to decision makers for business continuity. Connectivity requires

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

the adequate technology in place to detect outage in time and automatically divert networks and workflows to ensure business continuity.

For Meesters (2021) Crisis Information Management is about the role of information in reducing uncertainty in a crisis, allowing decision-makers to assess situations, “*evaluate alternatives and coordinate efforts between stakeholders*”, and he provides a recent example of IM efforts undertaken by UN-OCHA during Covid-19 to globally collect, process and disseminate information (Meesters, 2021:154).



Figure 6: Elements for Effective Information Management, Meesters K., 2021, Crisis Information Management: From Technological Potential to Societal Impact

In Figure 6 above, he illustrates the elements for effective IM in crisis, highlighting the requirement for organizations to consider “*procedures, capacities and culture*” in order to leverage the potential of information and technologies during crisis, through a paradigm shift “*towards an inclusive and reciprocal approach*” (Meesters, 2021: 156-158). This article encompasses one of the most inclusive approaches in terms of CIM factors (PPT).



MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

2.2 Extended literature review

There is a considerable acceleration in the pace of technological progression in our society, which creates an exponential approach to future crisis and business continuity management.

In times of extreme uncertainty organizations require a new management model that can assume the extreme circumstances as a normal situation. Traditional management operation models can easily find themselves facing existential threats. For IGOs and their area of operations, the threat extends to the regions, countries, and societies they support or the regional or international social systems and balance that they sustain. The unprecedented crisis of Covid-19 pandemic could resemble in business terms the economic crisis of 2008-2009 but the pandemic is more severe in qualitative terms as it directly affected the public health system and resulted in a global economic recession (McKinsey & Company, 2020: 2). The recent health crisis had a faster domino effect globally, and almost all business sectors as well as crisis response agencies (either national or at IGO level) had no means to respond in timely manner.

Asian Development Bank, in its disaster management handbook (2008) extensively discusses about information management in the context of disaster management and specifically in organization, planning and response to a disaster situation. Information in an organizational system needs to be relevant, accurate and of high quality, managed by expert staff. Carefully selected sources may provide two types of information: crisis information (dynamic) that apply directly to the disaster situation, and background (static) information such as records of previous disasters or map information useful for the specific situation. (ADB, 2008: 131-132). Information management during crisis¹ is critical especially during the response phase, in terms of information collection, assessment or evaluation, decision making and dissemination both vertically and horizontally. During planning phase, the identified IM components are facilities,

¹ Terms disaster and crisis can be used interchangeably at the analysis of ADB.

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

systems and personnel involved with emphasis in the effectiveness of the Emergency Operations Center (EOC) (ADB, 2008: 157).

Asian Development Bank indirectly also analyzes all aspects of the PPRR model. Prevention and mitigation as part of the long-term measures; Preparedness as major factors prior to disaster impact; Response upon the disaster impact with the required logistics, and Recovery together with post-disaster review as part of the major post-impact factors. In the PPT framework, ADB handbook explains in detail the requirements for people and processes. Although technology is not mentioned per se, it extensively refers to tools in terms of machinery, special operation tools and equipment, logistic tools, microcomputers and special GIS tools and applications such as aerial photography and satellite imagery that may assist in hazard mapping and assessment of a situation. Many IGOs provide international assistance to major disaster or international crisis events. These types of assistance are described by ADB, as pre-disaster assistance (preventive and in preparedness, such as EOCs, special infrastructure, or monitoring and early warning systems); assistance in response operations (providing experts and special equipment or supplies), assistance in recovery programs (infrastructure, financial, agriculture and service expertise), and finally assistance in future development through long-term development programs (like transportation infrastructure and agriculture) (ADB, 2008: 103-105).

Goda, Tyrachuk and Khylo, (Eds., 2016) analyze the international crisis management in a collaboration framework between IGOs such as NATO, EU, OSCE, with a variety of conflict management tools depending on the essence of the operation (peace keeping, peace building or peace enforcing or combination of them). On one hand, establishing standards, interoperability and training are some of the key areas for NATO in crisis management (Goda et al, 2016: 59). Coordination between IGOs was tested in various cases such as support to the Minsk agreement, Bosnia & Herzegovina war, Kosovo conflict, Afghanistan, with most challenges emerging from effective communication (in terms of strategic and operational communication) and information

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

management (including flows of misinformation). EU on the other hand, has been using other various instruments to support crisis management, but the most important tool in conflicts and crisis management for the effective collaboration of IGOs is “reliable information on the ground” (Goda et al., 2016: 89) and this can come with skilled people, effective processes and legislation, and interoperable tools and technology.

The first step towards organizational resilience for disasters and emergencies, is leadership, and leading emergency management is about Prevention, Preparedness, Response and Recovery. In Australia there are different variations of the PPRR model used by emergency management organizations where the “people” factor is stressed mainly in emergency management cycles dealing with natural disasters. According to the Australian Governmental Initiative (<https://resilience.acoss.org.au/>, accessed 20 Apr 2022), roles and responsibilities in every phase of the emergency management cycle is important to be clearly defined by leadership.

Getting back at the Sapriel and his “pre-loss, loss, post-loss” framework of integrated business contingency, as we can see in the edited Figure 7 below, there is a relationship between the crisis stages and the potential losses in a way that they could much the PPRR model, in terms of anticipation, response and recovery, while maintaining the strategic communication between stakeholders and the relevant crisis information flow across these phases.

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

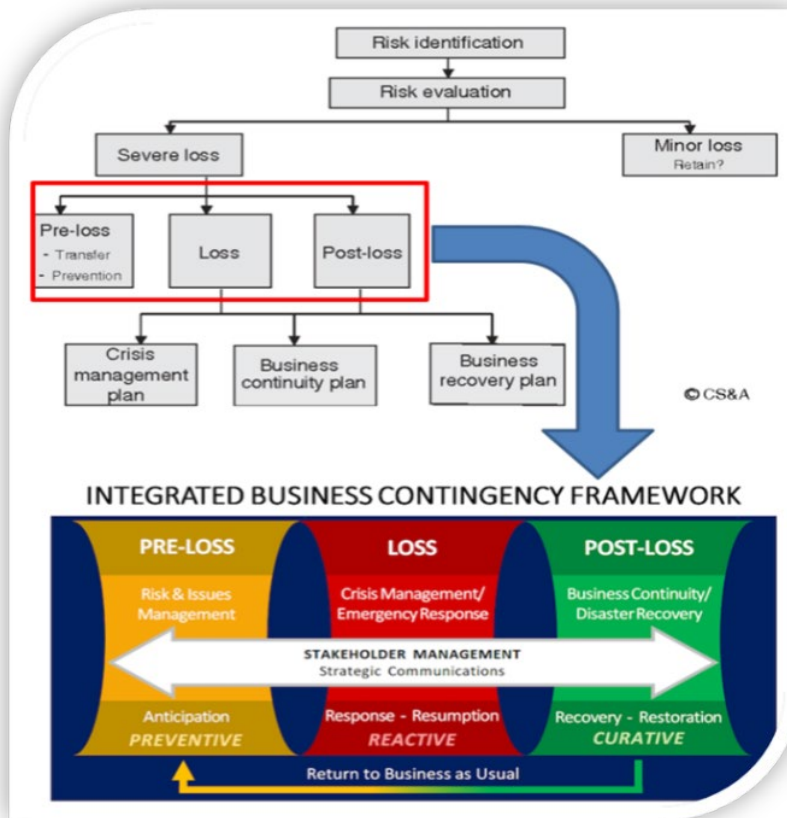
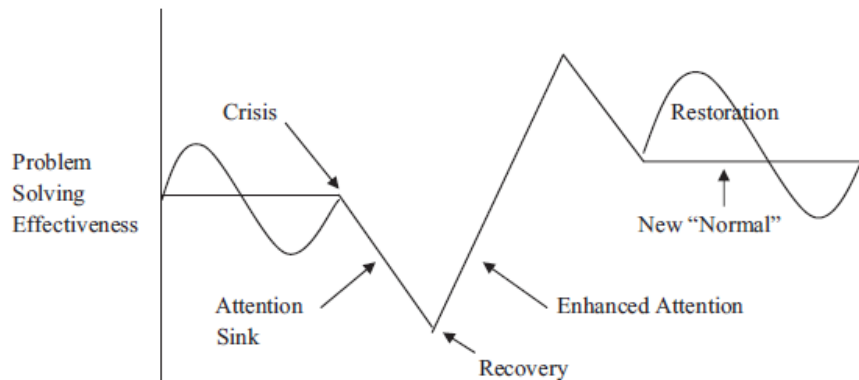


Figure 7: Business contingency planning and Integrated business contingency framework (Sapriel, © 1991-2019 CS&A). For the purpose of this paper figures are merged & edited by the author to stress their relationship.

Return to business-as-usual (as shown in the business contingency framework model above) is almost never at the same level as before crisis. The new normal after restoration is at a different level and dimension as it takes account all the lesson-identified, and lessons-learned from the crisis event and new features have been introduced in the business processes and contingency plans to adapt to the new reality. The nominal crisis cycle from Schuman & Roe shows exactly that perspective, and it is not something new as it has been introduced to the research community already by Bales in 1953. Covid-19 pandemic is a typical example of this approach, where the restoration point in social and business life is considered more of a new normal rather than a full recovery from crisis. One would think the level of people, process and technology determines the respective level of the new normal at the restoration point.

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT



*Adapted from Bales (1953)

Figure 8: High reliability management: a nominal crisis cycle; P.R. Schulman, E. Roe / *Policy and Society* 30 (2011) p.132.

The initial examined literature is related more to the theoretical framework of crisis and business continuity which partially explains the focus on “process” and “people”, rather than “technology”. As the beginning of the century was marked by the unprecedented 9/11 terrorist attacks, process and technology factors became the center of gravity for states and international organizations involved in international crisis and major disasters, to update procedures and tools necessary for the preparation, prevention, response and recovery of such disruptive events. The traditional volunteering social movement in the US helped the state authorities focus on the coordination and procedural part of crisis management while the “people” factor was taken for granted. Similarly in other major crisis events from natural disasters like earthquakes in Pakistan (2005), Iran (2003) and Haiti (2010), and the disaster from earthquake and tsunami in Indian Ocean (2004), triggered the need to have updated processes and adequate technology available to confront the challenges. The scholarly debate on theoretical framework that continued the next decade started emphasizing the importance of “people” factor in Crisis Information Management. Lessons-learned from the Indian Ocean tsunami in 2004 forced international community including governments of vulnerable nations and IGOs, to invest more on tools and technology related on early warning and preparedness for such disasters.

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

The Earthquake and Tsunami in 2011 was one of the worst disasters in Japanese history. The 9.0 magnitude earthquake created a disaster that claimed around 20,000 lives (Britannica, 2022), leaving more than 450,000 people homeless. Damages to infrastructure were far greater than any other tsunami in modern history, with material losses of \$300 billion and a tsunami that resulted in a nuclear meltdown, releasing radioactive materials at the Fukushima power plant. Millions of households left without electricity and running water while many thousands had to evacuate. The level of preparedness (within the PPRR model) was fundamental for this crisis management in an organized manner that kept “people”, “process” and “technology” factors as balanced as possible by the national authorities. In pre-crisis times the important operating principle is for decision makers to understand the kinds of events (or signals of events) that can trigger a crisis and based on them, establish an appropriate monitoring system. Such an example is the *“Intergovernmental Oceanographic Commission’s early warning systems, which rapidly relay data of approaching tsunamis to potentially affected communities”* (McKinsey & Company, 2020: 5)

Within UN Agencies, Crisis Information Management is approached with clusters per response sector such as emergency telecommunication, food security, health, logistics, nutrition, emergency shelter, education, sanitation and other. As shown in Figure 9 from OCHA below, the aim of such approach is to provide predictability and accountability to sectors, as well as better support to national-led response tools and interoperability through common standards.

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

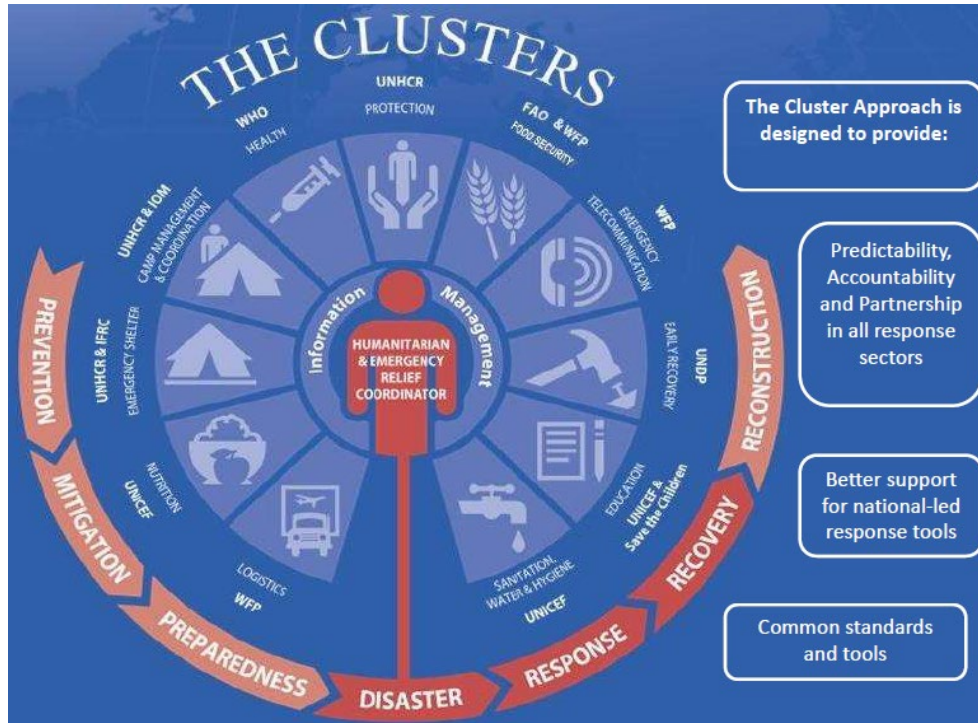


Figure 9: OCHA, *The UN Cluster Approach in Crisis Management; Humanitarian Crisis Management and Humanitarian Civil-Military Coordination; Presentation from R. Reario (NATO Crisis Management course, 12 May 2021)*

It is a balanced approach between people, process and technology/tools, and is designed in an expanded PPRR cycle, that includes dedicated phases of prevention, mitigation, preparedness, disaster, response, recovery, and reconstruction.

In international crisis events synergies from multiple IGOs and state governments take place in a coordinated manner. Processes, skilled staff, and technology may vary and not always in line with the coordinated plan. The need for cooperation and coordination between IGOs in international crisis or conflicts was highlighted by the OSCE² Sec. Gen. in 1995, along with the parallel efforts by UN (“Agenda for Peace”) and NATO (Partnership for Peace). OSCE was established as the primary instrument for early warning, conflict prevention and crisis management among its member states,

² With 57 participating member states (from Vancouver to Vladivostok) and 11 partners for co-operation, OSCE is the world’s largest regional security organization.

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

with emphasis on preventive diplomacy. The need for reinforcing co-operation was underlined in the sense of a better understanding of the comparative advantages of the IGOs. On his fundamental question “what is the role of international organizations in conflict management” the Sec. Gen. urged the need to “*be clear as to what they can do and what they cannot do*” (1995). Promoting the importance of international politics and the will of states and their societies to make necessary efforts (in particular personnel and financing) including unavoidable sacrifices for crisis management, was his answer to the potential “failure” of international organizations. Since then, people’s expertise and skills for crisis management have been constantly developed, and processes have become much more lean, automated, and effective in a coordinated manner. At the same time, technology has developed at such pace that has given great potential to crisis and business continuity management tools, instruments, and techniques, but has also increased vulnerabilities and new potential causes of crisis, conflicts or disasters worldwide.

UN-IOM (International Organization for Migration) has been using specialized tools such as Displacement Tracking Matrix (DTM) and Migration Information and Data Analysis System (MIDAS), which have helped UN efforts in migration and border management assessment, intelligence, and risk analysis, and taking decisions regarding migration facilitation and providing technical solutions that prevent or respond to international conflicts and crisis.

On another example, developed by ION in 2009, MIDAS has the capability to process and analyze data and information in real time across any border network, with governments having the exclusive ownership of the recorded data. For the first time in 2016³, Burkina Faso was able to electronically monitor migration flows at the border crossings with Ghana, Mali and Ivory Coast, after installation of the Migration Information and Data Analysis System (MIDAS). This was a partnership effort between

³ [Migration Information and Data Analysis System \(MIDAS\) Goes Online in Burkina Faso | International Organization for Migration \(iom.int\)](#) (last accessed 19 Feb 2022)

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

the G5⁴ countries Sahel, IOM and Japan, and it is an example of successful intergovernmental effort for the confrontation of immigration related crisis.

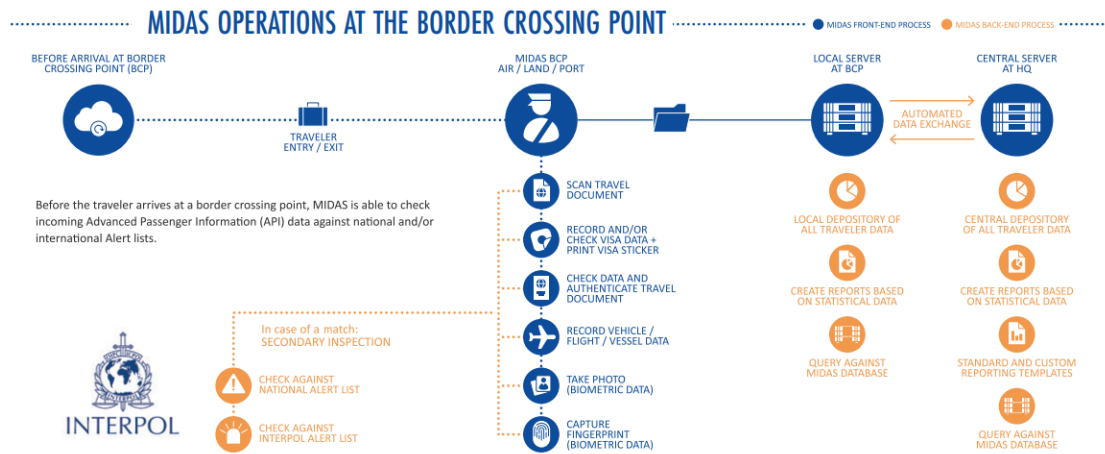


Figure 10: MIDAS Process diagram (IOM, 8 Feb. 2021)

By 2018, 20 countries world-wide were using MIDAS as a comprehensive and affordable border management information system (BMIS). The availability of the tool enabled the governments to mobilize and train personnel (“people”) and initiated new interoperable “processes” based on the tool’s adaptable functionalities, able to interconnect to other BMIS as it is compliant with international standards (ICAO & ISO). MIDAS is not just a border security technology, but it contributes to the “constitution of new domains of political intervention and new modalities of divisibility” (Singler, 2021: 460), and therefore contributes to the whole spectrum of PPRR model as an enabler for a new process executed by skilled operators.

Another important tool for IOM is the Displacement Tracking Matrix (DTM) (IOM Crisis Response Plan – 8 Oct 2021). Following the 2010 earthquake in Haiti hundreds of thousands affected migrated to Brazil, Chile and Argentina where they settled. In recent years accumulating factors contributed to their ability to integrate, resulting to a continuation of migration this time towards the north crossing the Darien Gap to Central

⁴ The G5 Sahel Force was officially established in 2017 to respond to the expansion of armed and violent extremist groups and to the deteriorating security situation in the region of west Africa. [OHCHR | G5-Sahel](#) (last accessed 20 Feb 2022)

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

America, Mexico and ultimately United States. IOM is utilizing the Displacement Tracking Matrix (DTM) system to provide an evidence-based decision making for interventions linked to community-based disaster management and climate change adaptation projects. According to IOM it is a system that captures, processes and disseminates multi-layered information on the mobility, locations, vulnerabilities and needs of displaced and mobile populations throughout the course of a crisis ([IOM, Emergency Manual](#), 2019). As a tool, brings data and information for better preparedness, targeted response and support to transition to sustainable return to recovery. It is therefore enabling the process by IOM to effectively execute the plan with the available skilled operators.

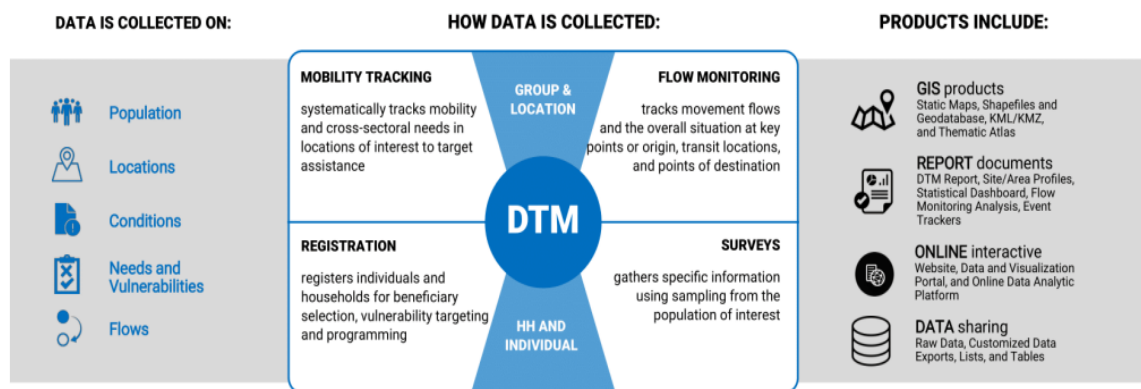


Figure 11: Displacement Tracking Matrix (DTM), UN – IOM, 2019, <https://emergencymanual.iom.int/entry/19108/displacement-tracking-matrix-dtm>

The system was initially conceptualized in Iraq in 2004 and since then gradually improved for migration crisis, conflicts, and natural disasters. Comparing to the pre-2004 period, this decentralized innovative approach of the tool makes the big difference in crisis management, as it can provide critical, reliable, and timely information to decision-makers and responders to a crisis event.

European Union (EU) has managed to make valuable civilian contributions in conflict and post-conflict environments, especially in aggregating and coordinating

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

national resources (RAND, 2010). In addition, policing operations have been beneficial although mainly at legal advisory level (RAND, 2010: 20-21)

According to RAND (2010) EU needs to overcome some staffing problems with its civilian crisis management and response capability. There are proposals for establishment of national contingencies within EU missions (such as those in Kosovo and Afghanistan), so nations will have to commit resources as part of the process. The gap of staff deployment during crisis mainly derives from the nature of the “process” (and the collective will to change it) that creates a financial disincentive for governments and the forces (“people”) involved, while the “technology” is already available.

Military crisis has certain decision-making process, and crisis management in international organizations like NATO follow specific protocol based on consensus and unanimous decisions. Peace keeping operations in coordination with other IGOs like the EU are proven to be even more complicated when both military and civilian missions are taking place in the same area of operations. Obviously processes that affect information exchange between the organizations is the key to successful cooperation during crisis. Both EU and NATO have had military operations in parallel at the same regions, such as African Union Mission in Sudan, Support to AMIS (Sudan/Darfur), Counter-piracy operations (Ocean Shield and EUNAVFOR). Fahren-Hussey points out this unique fact of overlapping operations with the two organizations covering the same issues under either EU’s Petersberg tasks or under NATO’s non-Article 5 operations. In fact, nations that are members of one organization but not the other are pledging the same forces (Fahren-Hussey, 2009: 47), making availability of resources (in terms of CIM, personnel/people and technology/arms) a great challenge for crisis management.

Cooperation between international organizations during crisis is often based on the level of agreed cooperation between a number of member states (as a subset of an IO⁵) with agreed resource dependencies (either in material, like funds and personnel, or

⁵ We use IO & IGO interchangeably in this particular case referring to the publication of Harsch M.

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

symbolic such as legitimacy). According to Harsch on interorganizational cooperation, two organizations “*will cooperate well when both perceive that each other’s resources are essential and non-substitutable and gauge their dependence to be similar.*” (Harsch, 2015: 4). The case study of cooperation between UN and NATO during crisis raises the issue of the power of dependence and autonomy concerns of the IGOs. The balance of the dependence and autonomy is directly linked with scrutiny by member states and organizational officials. From the PPT framework perspective, “people” seems to be the critical factor for an effective coordination between two IGOs. Harsch emphasizes the theoretical analogy of cooperation between international firms and nations, based on three arguments: the hegemonic interest of the participants, the organizational culture (norms and approaches), and the management approaches (based on interpersonal trust). All the arguments are (indirectly) highlighting the importance of the “people” as CIM factor.

In summary, the literature review conducted in this chapter reveals a plethora of approaches on how the three information management factors (people, process, technology) are perceived from various frameworks, theories or specific studies. In some cases, “people” is the critical factor that determines the viability of an emergency or disaster recovery plan, while in other cases “process” is the element that holds together a crisis management and the collaboration between IGOs on CM and business continuity management, considering availability of resources (funding, tools, equipment, specialists, etc).

However, in terms of PPT, the existing literature does not exhaust the relationship of the three factors with CIM in a balanced and multidisciplinary approach, especially from the IGO perspective. The published work has not enough depth in the area of PPT and there is no clear connection of the information management (IM) discipline from the technology perspective, with crisis and business continuity management. After introducing three basic and widely accepted frameworks on IM and CM/BCM in the next chapter, we will then further explore the PPT aspects within the CIM discipline, in an intent to bridge this theoretical and methodological gap.

Chapter 3: Intellectual Framework

3.1 PPT framework

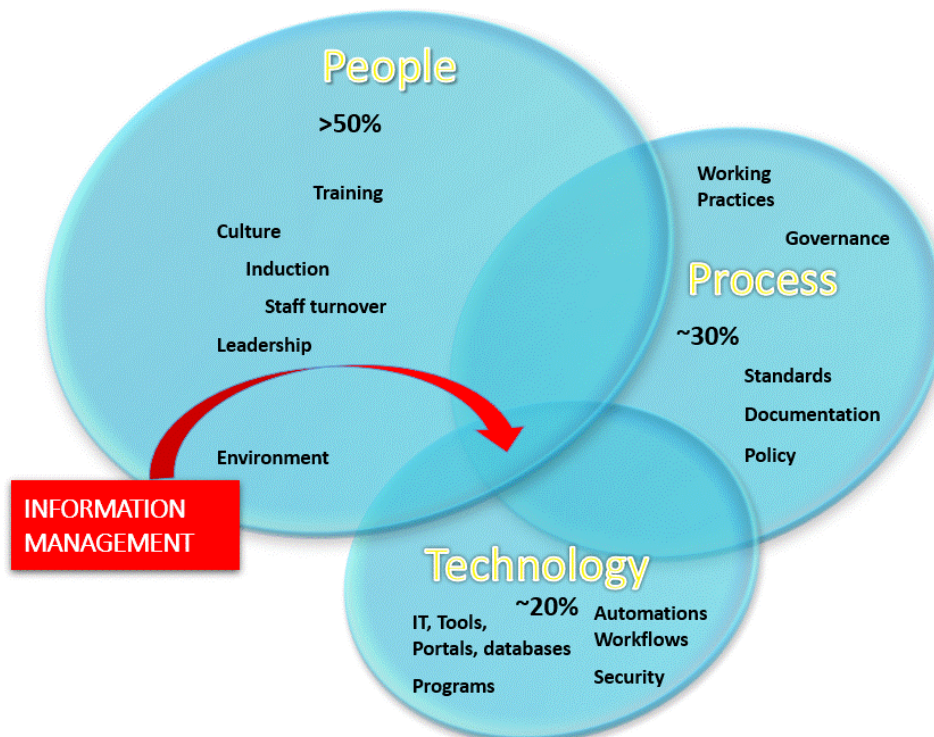


Figure 12: PPT framework explained from an Information & Knowledge Management (IKM) perspective

The term, *people, process, technology* refers to the methodology in which the balance of people, process, and technology drives action towards the objectives of the organization. While “People” perform specific types of work based on existing “processes”, it is the “technology” that enables the achievement of the goals and improve or streamline those processes. During crisis, goals and objectives are time sensitive and the balance between those three information management elements (PPT) are critical for crisis and business continuity management and assists the organization on the decision making of implementation of new technologies. Intergovernmental Organizations are inclined to lengthy, complicated, and bureaucratic processes due to the complexity of such structures and their legal and decision-making framework.

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

Experts from knowledge management domain such as Dilip Bhatt (2001) use the same model and same components but believe that “people” factor covers 70% of the effort required for the learning objective of the organization, with process and technology on 20% and 10% respectively. The justification is that technology is easier and quicker to implement, while on the other extreme, procedural and people issues can cost more and take much longer to implement changes.

In business management as well as IT management, a proper balance between the three elements of the PPT framework is required for smooth and streamlined business operations. If suitable processes are not in place, people may be ineffective, and technology can fail. Usually, the latest available technology is expensive and does not always offer a high return on investment (ROI), so organizations need to ensure it runs smoothly. Also, employees need to know how to use the technology that is available in an intergovernmental organization and ensure that integrates well with other related processes, otherwise there is no value creation from its original investment.

3.2 PPRR framework



Figure 13: PPRR Framework model basic concept

Prevention – Elimination or reduction of risk (or the effects of an incident) is included here, and we refer to actions undertaken in advance, often referred as

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

mitigation. After proper risk identification and assessment, proper measures are ensured in place to reduce potential loss of life, property, and business damage. Constructions to protect from tidal waves, alternative sources of electricity in case of blackout, or backup communication systems are some examples. These activities are constantly happening during the prevention phase within the framework of risk management (prevention of risks or foreseen disruptive events). Sapriel's BCM model is capturing this at the Pre-loss stage.

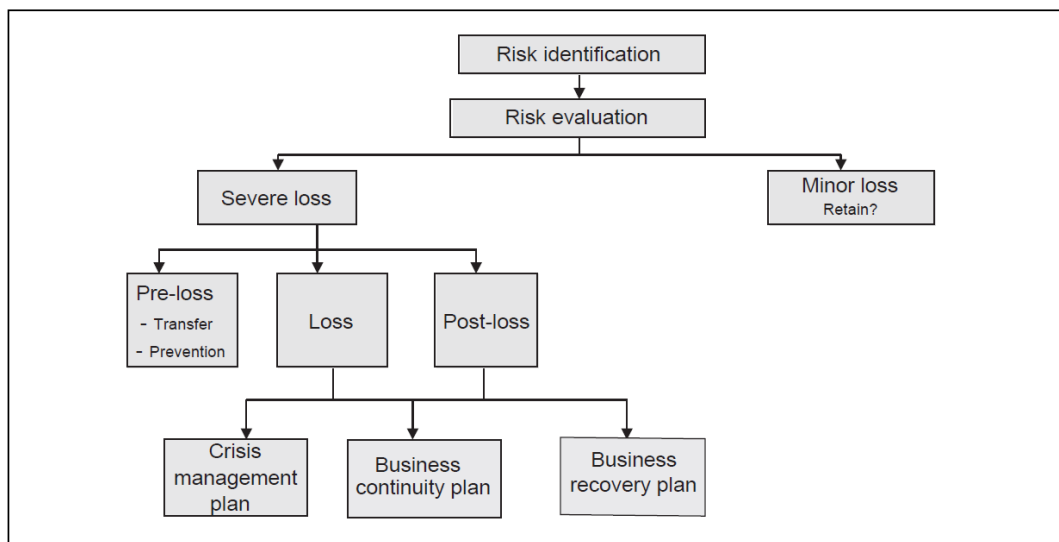


Figure 14: Sapriel 2003, BCM model, Prevention level – reduction of risk

Preparedness – Planning for the worse-case scenario in terms of risk and impact. Test plans, arrangements, training activities, and information sharing in order to prepare communities when a high risk materializes into a major crisis. Actions are taken prior to an accident occurring, to ensure effective response and recovery ([The PPRR risk management model | Business Queensland](#), last updated 21 May 2021). These are continuing activities (not one-time events) and act as a catalyst for the effectiveness of the next phase when major disruption occurs. Therefore, preparedness is all about being proactive and focused on planning.

Identifying top-level and lowest level functions and processes, plus any other critical functions of the organization, is an example for analysis of business area

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

impacts. Within the preparedness aspect of the PRRR model, business impact analysis (BIA) is in central focus, suggesting a prioritization of the top-level functions and processes.

Elliot, Swartz and Herbane (2010) attempt to approach BCM from a rather socio-technical perspective. Based on the three stages of crisis (pre-crisis, trans-crisis and post-crisis), both disaster recovery planning and crisis management determine the business continuity management of the organization. DRP approach is traditionally focused on IT failures and natural disaster, while CM approach is more directly related to BCM in a sense that crisis incubates during the pre-crisis phase pending the critical event that will activate the crisis. As some CM theorists describe accidents as normal, it becomes difficult to define the three CIM factors (PPT) for those approaches depending on the case and their context (Elliot et.al., 2010: 438)

Response – Actions or intervention activities that are happening during or immediately after a major crisis or emergency. During crisis there are clearly pre-defined steps of response with the priority of saving human lives and protecting community assets (mainly infrastructure and community's physical environment), and usually measured in hours, days or weeks. Response is mainly captured within Incident Response Management and includes also prevention of incident escalation, involving actions from operations, management and communications parts of the organization.

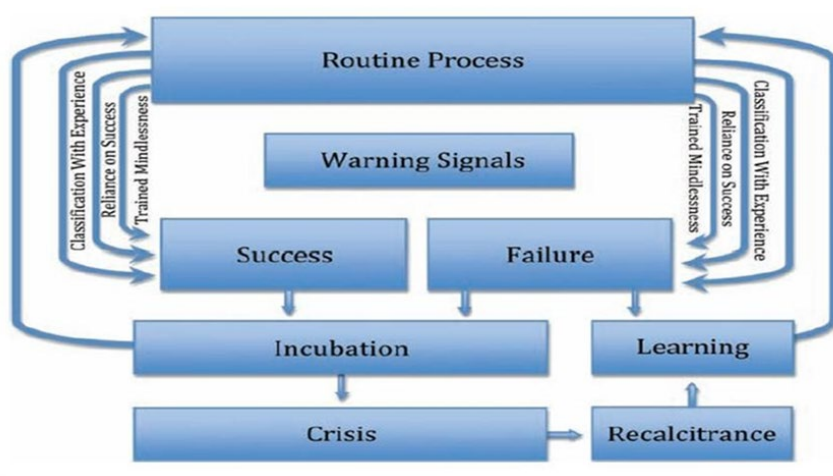


Figure 15: Learning Barrier Model (Veil, 2011) – Response level

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

Crisis information flows in the response aspect of the PPRR model can be explained by Veil in the model with three main elements. Classification of experience, reliance on success and trained Mindlessness. It is a recurring process feeding the success or failure respectively, while feedback is returned back to the process from the incubation or from the learning experience of the model.

As interrelationship between the risk manager and the crisis manager as functions in crisis management in the context of facilities management, is highlighted by Barton and Hardigree (1995) and shown in the figure below.

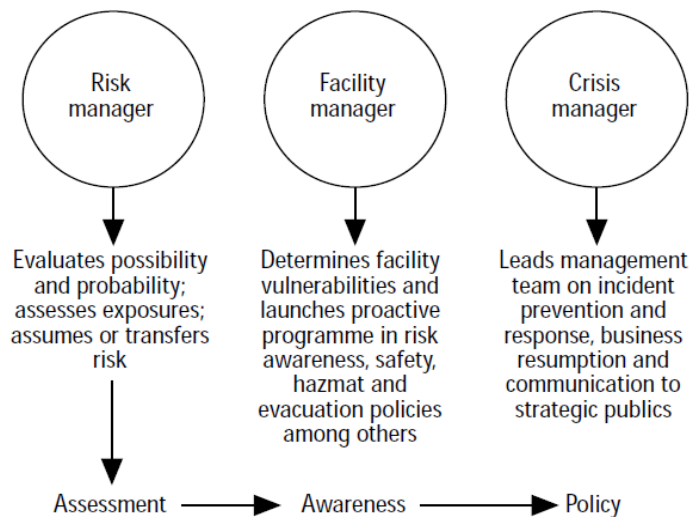


Figure 16: Risk and crisis management in facilities, Model of L. Barton & D. Hardigree, in *Facilities*, Vol.13 Aug 1995, MCB University Press

Recovery – This is a process coordinated among all stakeholders with the aim to support emergency-affected communities in reconstruction of their physical infrastructure and to restore their social, economic, physical, or emotional wellbeing. The process is usually measured in months or even years.

The cycle model by Veil (2011), gives a first impression of a repetitive process but it is actually not, and it reminds us of the iterative method that applies also in the recovery aspect of PPRR model.

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

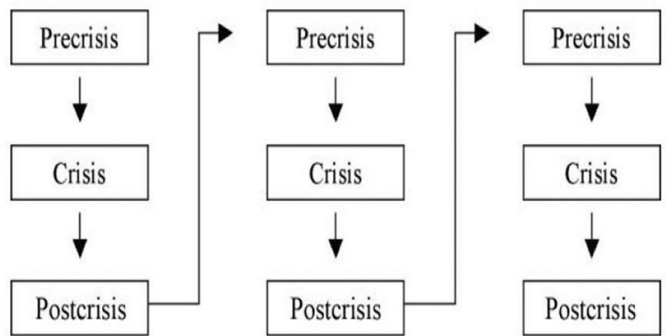


Figure 17: Three-Stage Crisis Cycle (Veil, 2011)

One of the in-built vulnerabilities of planning process is that it requires multi-agency cooperation and coordination. The barriers to the collaboration between agencies include differences in organizational goals, professional cultures, lines of accountability, political control style and decision-making cycles. Many of the organizations dealing with crisis planning, involve actors in the voluntary and private sectors. (Boin, McConnell, 2007: 53)



Figure 18: PPRR as Business Continuity Management Framework

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

The above cyclical representation of the PPRR model is important in its nature as it highlights the requirement to continuously manage emergencies (not just during the crisis “hot season”). The phases also blend into each other and often overlap rather than being discrete categories. A useful framework for the emergency management sector in IGOs, that is responsible to design the plan and allocation of responsibilities, with the use of business continuity components such as risk assessment, impact analysis and recovery strategies.

3.3 ISO 22301:2019 Security and resilience – BCMS

Within the worldwide federation of national standard bodies, this ISO standard specifies the structure and requirements for implementing a BCMS with the aim to develop business continuity for the organization to successfully manage a disruption.

It is the most widely known business continuity management system standard that places emphasis on:

- Understanding the organization’s needs and expectations, in order to frame the scope of the management system,
- Establishing business continuity objectives, in order to set its baseline and boundaries,
- Defining and operating the relevant processes and response structures, in order to ensure that the organization will survive from the operations disruptions and
- Monitoring the performance of the management system, in order for it to operate effectively and towards its continuous improvement.

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

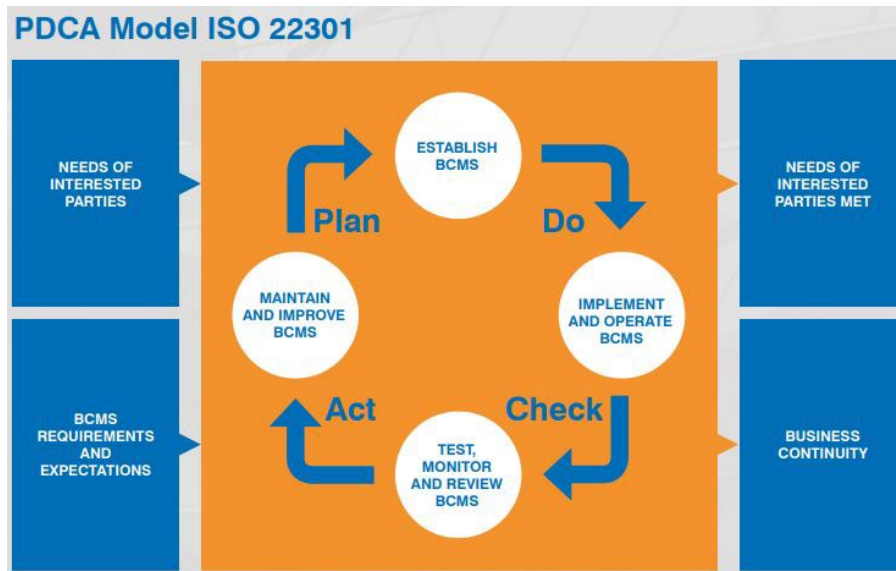


Figure 19: PDCA Model, ISO 22301:2019 Implementation Guide, T. Bevan, UK

This international standard applies the PDCA (Plan-Do-Check-Act) cycle in order to implement, maintain and continually improve the effectiveness of an organization's BCMS (ISO 22301:2019; para 0.3), ensuring at the same time some consistency with other management system standards such as ISO 9001. This consistency with ISO9001 establishes the connection of its IKM related requirements. The clause under Section 7 (Support) refers to "*Organizational Knowledge*" while the term "*Documented Information*" replaces the references "documents" and "records" of the previous version of the standard. The first deals with competence, awareness and Communication, and the need of the personnel's contribution. The second determines the level of information management within the organization that is necessary to control its Quality Management System.

The volume of documented information should not be standard or taken for granted and therefore is dependent on the size and complexity of the organization. Furthermore, the "*control of documented information*" (ISO 22301:2019; para 7.5.3) gives great emphasis on access control of documented information, revealing the importance of information security especially in multinational and international organizations.

Chapter 4: Methodology and Methods

Combination of questionnaires and repeated reviews of data and literature, in the lines of Grounded Theory, aiming to derive new theory from data collection and their qualitative analysis.

Grounded theory is a qualitative research method that enables the researcher to derive new theories based on the iterative collection and analysis of real-world data and information.

The phenomenon studied in this dissertation has no previous comprehensive theory and I therefore look for novel theory without preconceived hypothesis, enhancing theory development using existing theories and frameworks as a ground. The research methodology is iterative and not linear, using a cycling process between data collection and analysis, establishing better understanding of the particular issues I am examining. Analysis is data-driven. Compare data with data, and then data with category and then category with other categories.

Using grounded theory, we continuously collect and analyze data and information until we reach theoretical saturation, which is the point at which new data cannot contribute any new insight to the evolving theory.

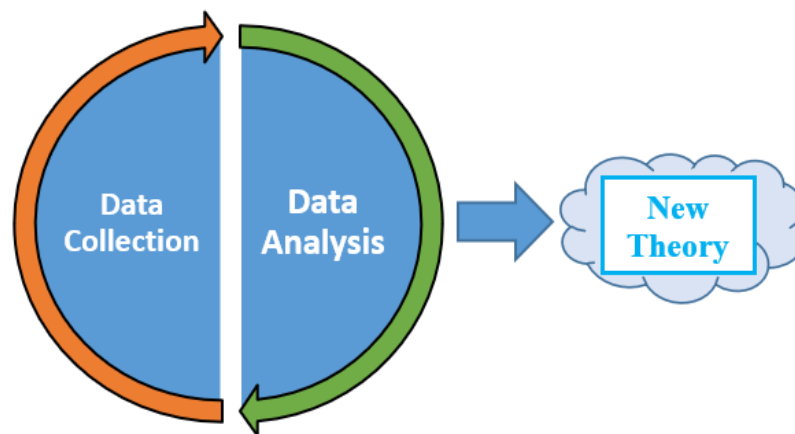


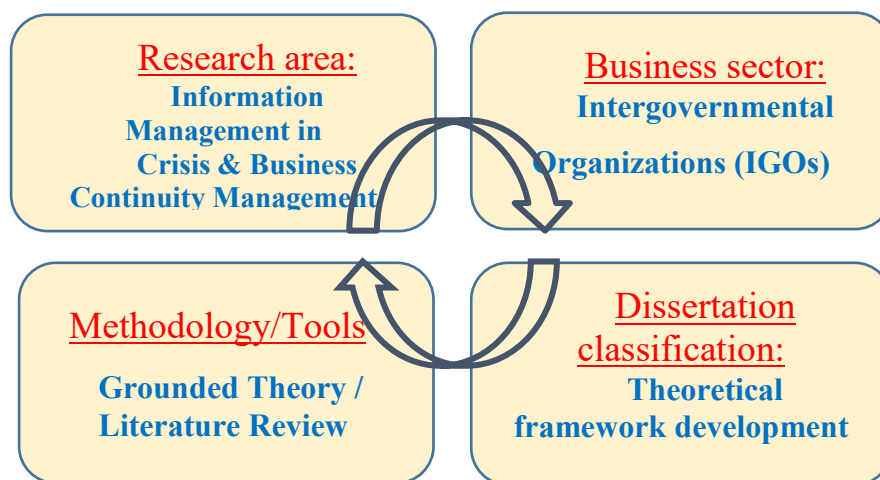
Figure 20: Research methodology schema based on Grounded Theory

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

The data collection process is called theoretical sampling in the Grounded Theory context. Literature review findings and gathered evidence-based data and information available in primary and secondary sources, case studies in specific related thematic areas, and opinions from surveys with semi-structured and open-ended questions.

Typical steps of grounded theory

1. Determine initial research questions
2. Recruit and collect data (theoretical sampling)
3. Break transcripts into excerpts (open coding)
4. Group excerpts into codes (open coding)
5. Group codes into categories (axial coding)
6. Analyze more excerpts and compare with codes
7. Repeat steps 2-6 until you reach theoretical saturation
8. Define the central idea (selective coding)
9. Write your grounded theory



- **First iteration**

An initial literature review of basic theoretical frameworks from scientific articles on crisis and business continuity, and analysis of related PPT reference on these related

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

articles, based on grounded theory. In this phase we search for selected codes/terms in text (as keywords) and count the number of appearances in CIM context.

- **Second iteration**

In this iteration a survey is conducted with SMEs from ~25 Organizations & Agencies.

The questions are related to their perceived preparedness/readiness of their organization for a major crisis (major disruption due to a disaster or catastrophic event) and the effect of change in a IM factor to the crisis and business continuity management of the organization.

Pre-assumption on Crisis categorization

External

- Public health crisis at global scale (i.e., covid-19, 2020-21)
- Financial crisis (i.e., 2008 financial crisis in US)
- Environmental crisis (including natural events) (i.e., Japan earthquake 2011)
- Security Crisis (including armed conflicts, terrorism cyber-attacks) (i.e., 9/11 attacks, USA 2001)

Internal

- Organizational (i.e. management change and confidence crisis)

For the purpose of this study, we consider only the external types of crisis in areas where IGOs are turned upon to solve issues with immediate effect to the society.

However, we do not neglect the internal (organizational) type of crisis, hence we include it in the questionnaire of our survey, for objectivity and transparency purposes.

- **Third Iteration**

Further literature review (combination of scientific articles, reports from case studies and books) and re-iteration and analysis of initial questionnaire results.

The general framework of the survey questions will be:

Results will be with more qualitative characteristics, revealing perceptions on the required level of effort on the three IM factors, presented as partially quantitative

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

analysis of the results with their qualitative interpretation (including open-ended questions). Study material used for this dissertation include, but not limited to:

- Related research literature and gathered online information.
- Collection of official documents (archives, public disclosed documents, reports)
- Selected audits and discussions with subject matter experts.

4.1 Limitations

Data sources and literature used are certainly non exhaustive and the findings or conclusions are open to constructive criticism. A selective number of international organizations in combination with governmental organizations and structures is used, with an indicative selection of cases mentioned as examples for the developing arguments. This paper is primarily focused on the impact and interdependencies of CIM within the organization (affecting the operations of the organization), and secondly on the possible efforts to manage and respond to an international crisis (as for instance providing humanitarian aid to a war/conflict zone, or to a natural disaster area). Analysis is based on major disruptive crisis events, external to the organization but with international impact, while minor/internal organizational crisis is not considered in the scope of this thesis.

4.2 Disclaimer notes

All answers/responses are kept anonymous. Target audience of the survey have previous related experience working for or with IGOs.

There is no direct connection between an organization and a specific survey response. Any opinions derived from the survey are not personalized or connected to a specific organization.

Personal contacts and hearings were conducted during the research period to capture insightful information and knowledge from selected experts in related fields. Unless

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

otherwise stated, any opinions expressed herein are solely those of the author, and do not in any way represent the views or opinions of any other person or entity.

4.3 Sources and Data

Initial set of 20 selected articles from journals and scientific papers on the research subject followed by additional bibliography related to CBCM, CIM and relevant case-study articles. Results from questionnaire distributed to target audience of field experts. Survey participants have previous working experience with the following organizations

Table 1: Organizations with which survey participants have had work experience

UN Office for the Coordination of Humanitarian Affairs (OCHA)
UN International Children's Emergency Fund (UNICEF)
IMO, International Migration Organization,
UN DRR, Office of Disaster Risk Reduction,
UN High Commissioner for Refugees (UNHCR), UN Refugee Agency
UN Framework Convention on Climate Change (UNFCCC)
International Renewable Energy Agency (IRENA)
World Meteorological Organization (WMO)
Organization for the Prohibition of Chemical Weapons (OPCW)
Comprehensive Nuclear-Test-Ban Treaty Organization (CTBTO)
North Atlantic Treaty Organization (NATO)
Organization for Security and Co-operation in Europe (OSCE)
Organization for Economic Co-operation and Development (OECD)
European Commission (EC)
EUROSTAT
EU Intellectual Property Office (EUIPO)
European Parliament
EU Agency for Space Programme (EUSPA)
EUROPOL
European Space Agency (ESA)
European Patent Office (EPO)
European Defence Agency (EDA)
European Medicines Agency (EMA)
World Bank Group (WBG)
Asian Development Bank (ADB)

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

4.4 Key Words

Crisis Management, Business Continuity Management, Information Management, People, Process, Technology.

4.5 Survey questionnaire formulation

The survey consists of semi-structured questions to a sample of 41 subject matter experts, including open-ended questions. Some of the open-ended questions may be revisited separately if clarifications required by the participant. Verbal answers are treated with logical interpretation of content and words is used to avoid misunderstandings.


The aim is to avoid potential bias, focus on confidentiality among the participants' opinions and viewpoints (due to subject and organizational sensitivities), reducing the effects of personalities (i.e.: dominant individuals), eliminating manipulation and coercion to shift viewpoints, and removing effects of an individual's status or role. Standardized question templates used to construct the survey (via survey account on *surveymonkey.com*)

Q1	
Type	Matrix / Rating Scale (Required to answer)
Question	<p>Given the explanation of the 3 Information Management (IM) factors below:</p> <ul style="list-style-type: none"> • Technology: Existing & backup technology available within your organization, to implement the business continuity plan effectively. • Process: The updated roadmaps, plans, processes, and procedures in place for business continuity during a major crisis event. • People: Adequate number of skilled staff available for all activities required, for smooth business continuity during a major crisis event <p>On a scale from 1 to 5, (with 5 being the most) how would you rate the importance of the above IM factors from business continuity perspective during major crisis, in your organization/agency.</p>
Options	3 options (People. Process, Technology) with five columns weighted (1 to 5) – Number of rows respondents must answer: exactly 3
Q2	
Type	Matrix / Rating Scale (Required to answer)

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

Question	From your experience with IGOs, what is the perceived level of preparedness on each of the three Information Management aspects (PPT), with respect to crisis and business continuity management?
Options	3 options (People, Process, Technology) with five columns weighted from 1 to 5 on level of preparedness (5 being the most); Number of rows respondents must answer: exactly 3
Q3	
Type	Comment Box (open-ended – free text) (Required to answer)
Question	Exponential technological progress of the last decades, led to even more unpredictable risks (both threats & opportunities) at national and international level. How do you think this trend can affect crisis & business continuity management in intergovernmental organizations?
Options	n/a
Q4	
Type	Scale Range (Required to answer)
Question	Given PPT (People, Process & Technology) as the main factors of Information Management please answer the following to the best of your knowledge. For one indicative unit of change in “Technology” as Information Management factor, what is the perceived change required in “People”, for an effective Crisis Management and Business Continuity Plan? (Range: -10 to 10) Note: Each unit of change (left or right) corresponds to a 10% change (positive or negative) in required level of effort of “Technology” against “People”.
Options	Scale labels (-10 to 10), step size: 1, Start position: Center
Q5	
Type	Scale Range (Required to answer)
Question	Given PPT (People, Process & Technology) as the main factors of Information Management please answer the following to the best of your knowledge. For one indicative unit of change in “Technology” as Information Management factor, what is the perceived change required in “Process”, for an effective Crisis Management and Business Continuity Plan? (Range: -10 to 10) Note: Each unit of change (left or right) corresponds to a 10% change (positive or negative) in required level of effort of “Technology” against “Process”.
Options	Scale labels (-10 to 10); step size: 1; Start position: Center
Q6	
Type	Matrix / Rating Scale (Required to answer)

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

<p>Question</p>	<p style="text-align: center;"><small>Business Continuity Planning Process</small></p>  <p>In a scenario based on the simplified PPRR model of Business Continuity Planning; As major external risks start to materialize, you are asked to make a decision for an IGO regarding the commitment and allocation of the remaining available contingencies of the organization, for upcoming crisis & business continuity management. Represent your choices on sharing the resources among the three IM factors (people, process, and technology). Please select up to two columns per row.</p>
<p>Options</p>	<p>Number of rows respondents must answer: All; Randomize Rows for Each Respondent; Three rows (people, process, technology) and five columns (Prevention, Preparedness, Response, Recovery); Ranking from 1 to 5; Option for comments (3 lines; max 100 characters)</p>
<p>Q7</p>	
<p>Type</p>	<p>Ranking (Required to answer)</p>
<p>Question</p>	<p>From your experience with IGOs, how would you rank the crisis categories described below, with regards to their criticality on organizational strategic goals and objectives?</p> <ul style="list-style-type: none"> ▪ Global Public Health crisis (i.e., Covid-19 pandemic) ▪ Global Financial crisis (i.e., 2008 financial crisis) ▪ Global Environmental crisis (i.e., natural events such as earthquakes and tsunamis, or extreme weather-related events such as floods, wildfires, snowstorms, hurricanes, landslides) ▪ Global Security crisis (i.e., war conflicts, social unrest, refugee crisis, terrorism, piracy, and cyber-attacks) ▪ Internal (organizational crisis)
<p>Options</p>	<p>Ranking from 1 to 5 (unique numbers/ranks)</p>
<p>Q8</p>	
<p>Type</p>	<p>Multiple Textboxes (Required to answer)</p>
<p>Question</p>	<p>With regards to prevention and preparedness as part of business continuity planning in an IGO, how do you think the efforts (in %) are shared among the three IM factors (people, process, technology). Please enter only the presentence number with no symbols – Sum of the three entries should equal 100)</p>

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

Options	should be only number and the sum should equal 100; Sum of all options selected must add up to 100
Q9	
Type	Matrix / Rating Scale (Required to answer)
Question	Considering the accelerating technological advancements (in IT, robotics, AI/ML, quantum computing, space, civil engineering, telecommunication, transportation, genomics, cyber, medicine, etc.), how would you reconsider the importance rate of the IM factors in response/recovery of major crisis, disaster, or disruption, in an IGO? (Note that “technology” includes also critical infrastructure.)
Options	Three options (People, Process, Technology) with five columns weighted from 1 to 5; Additional text box for comments (max: 3 lines / 100 characters)
Q10	
Type	Single Textbox (Not required to answer)
Question	Name the organization(s) or agency(ies) you have work experience.
Options	n/a

Table 2: Survey questionnaire

Chapter 5: Findings and Analysis

5.1 1st Iteration – Findings form initial literature analysis

Analysis of IM elements that contextually appear in research reference for crisis management and business continuity management. 20 reference articles reviewed to identify context related directly to information management and its factors (people, process & technology). Based on grounded theory, research process in this iteration is performed intuitively and with a homogeneous approach, meaning that terms or codes that appear multiple times in a paragraph is counted as one occurrence.

Code/terms per IM factor
People
<i>leadership / management</i>
<i>staff/employees/personnel</i>
<i>human assets</i>
<i>human perception</i>
<i>subject matter experts</i>
<i>skills / experience / training</i>
<i>communication with stakeholders</i>
Processes
<i>Standardization</i>
<i>decision making process</i>
<i>procedure / model</i>
<i>scenario / simulation</i>
<i>process map / planning approach</i>
<i>activities, input/output</i>
<i>Documented information/procedures</i>
Technology
<i>special tools and machinery</i>
<i>software/hardware</i>
<i>IT assets / devices</i>
<i>information systems</i>
<i>Grid / network</i>
<i>technical functions</i>
<i>IT infrastructure</i>

Table 3: Code/terms per IM factor

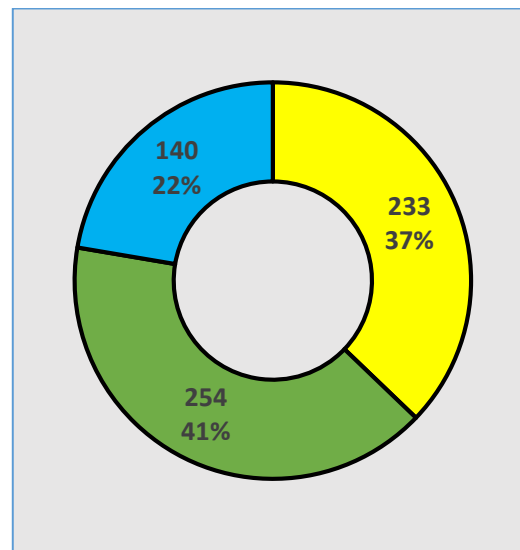


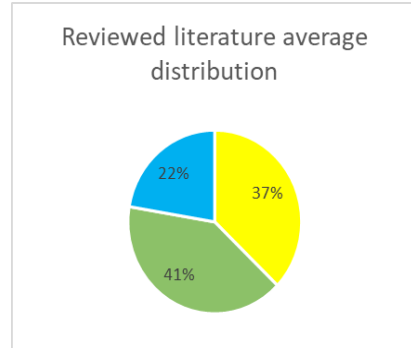
Figure 21: Overall occurrence of terms in CIM context per IM factor (PPT) (Average values of observations from all 20 articles reviewed per factor)

Crisis IM Code Legend
People
Process
Technology

Table 4: IM code legend

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

First results show that process related context is dominating the reviewed articles with 41%. A significant portion of the context is also dedicated to the “people” factor (with 37%), while “technology” related codes/terms appear more rarely at 22%. These first findings do not seem a surprise; in fact, the context of ISO 22301:2019 was also examined for the same codes and the result was overwhelming with “process” related terms appearing 3 times more than “people” and 10 times more than “technology”.



Code identification in text, associated with the three IM factors (People, Process, Technology) and related terms, and in the context of the subject of crisis management, contingency planning and business continuity management.																						
es that certain term appears in the reference article, within the context of information management PPT framework (People, Process, Technolo																						
Code/terms per theme	Ref #1	Ref #2	Ref #3	Ref #4	Ref #5	Ref #6	Ref #7	Ref #8	Ref #9	Ref #10	Ref #11	Ref #12	Ref #13	Ref #14	Ref #15	Ref #16	Ref #17	Ref #18	Ref #19	Ref #20	SUM	
People																						
leadership / management																						
staff/employees/personnel																						
human assets																						
human perception	12	12	4	15	8	11	10	24	10	18	10	14	18	16	4	16	7	14	3	7	233	
subject matter experts																						
skills / experience / training																						
communication with stakeholders																						
Processes																						
standardization																						
decision making process																						
procedure / model	16	9	3	10	25	14	14	26	9	8	11	11	17	13	6	16	13	15	10	8	254	
scenario / simulation																						
process map / planning approach																						
activities, input/output																						
Documented information/procedures																						
Technology																						
special tools and machinery																						
software/hardware																						
IT assets / devices	11	9	6	9	2	3	15	2	7	8	3	2	9	12	3	10	7	7	7	8	140	
information systems																						
Grid / network																						
technical functions																						
IT infrastructure																						
																					total	627

Table 5: Code identification - Code/terms appearance within the context of PPT framework

Therefore, the literature around the theoretical frameworks and concepts of crisis and business continuity management has an expected level of emphasis on process and people.

More specifically, authors and subject matter experts such as Gibb, Jaques, Veil, Sapriel, Darling, Gonzalez-Herrero & Pratt seem to be more inclined towards process

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

related terms and analysis, and with very limited reference to technology related terms in CIM context.

On the other hand, articles and literature from Coombs, and Hecht, have a great proportion of their theoretical context, with reference to technology and tools related terms/codes. Kash & Darling, Lindstrom, Samuelson, Hagerfors and Heba, pay significant attention to “people” in the context of crisis information management within their theoretical analysis papers, while Swartz, Elliott and Herbane during the 90s were focusing mainly in people and technology, being some of the very few exceptions that process related terms are not dominating their articles at the time.

Based on the IKM paradigm of PPT, Bhatt (2001) and other scholars of earlier years, agree on a sociotechnical system design as organizational perspective where technical aspects do not imply material technology but rather aspects of organizational structures and procedures and related knowledge. Since then, the speed of crisis management processes and related CIM functions has always followed (but not led) the rapid technological advancements. The 9/11 attacks as a historic event, was a landmark that drove many scholars towards more comprehensive analysis of technical aspects.

The challenge of today is not the availability of the information but rather the structure, design and management of information flows that eventually support decision making. That includes technology, quality control and security, availability of “intelligent” technology of sensing and scanning.

Humans are trying to figure out what is important and useful from the immense flow of information, and then trying to “train” technology do that more accurately, in order to enhance and optimize decision making at strategic management level.

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

5.2 2nd Iteration – Survey results and consolidated comments

A survey with a questionnaire of 9 questions (required to answer) was administered for this dissertation and distributed to 55 SMEs (with experience in IGOs) from which 41 responded. The results presentation and analysis that follows, reflects the 41 responses in 9 survey questions in sequence (Q1-Q9) (see questionnaire formulation table in Ch.4.5). The survey was administered online via URL link distribution to individuals, or personal email invitations, during a period of 2 months, from 15 January to 15 March 2022.



Figure 22: Demographics of survey participants per area of expertise

Questions #3 and #6 include open ended portions captured in online text box and consolidated for this results overview.

Weighted average scores were calculated via survey platform data analysis.⁶

$$\bar{x} = \frac{\sum_{i=1}^n w_i x_i}{\sum_{i=1}^n w_i}, \quad \bar{x} = \frac{w_1 x_1 + w_2 x_2 + \dots + w_n x_n}{w_1 + w_2 + \dots + w_n}$$

W = weighted average;

N = number of terms to be averaged

w_i = weights applied to x values;

⁶ Weighted values are automatically calculated by the survey platform, courtesy of *SurveyMonkey* account of the author, © 1999-2022 (As of July 1, 2021, SurveyMonkey Inc. became Momentive Inc.)

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

x_i = data values to be averaged

❖ Q1.

On a scale from 1 to 5, (5 being the most), Importance rating of IM factors (PPT) from business continuity perspective during major crisis.

	1 Less important		2		3		4		5 Most important		Total	Weighted Average
People	0.00%	0	4.88%	2	9.76%	4	29.27%	12	56.10%	23	41	4.37
Process	2.44%	1	2.44%	1	19.51%	8	56.10%	23	19.51%	8	41	3.88
Technology	2.44%	1	4.88%	2	31.71%	13	36.59%	15	24.39%	10	41	3.76
											Answered	41

Table 6: Data results from survey Question 1

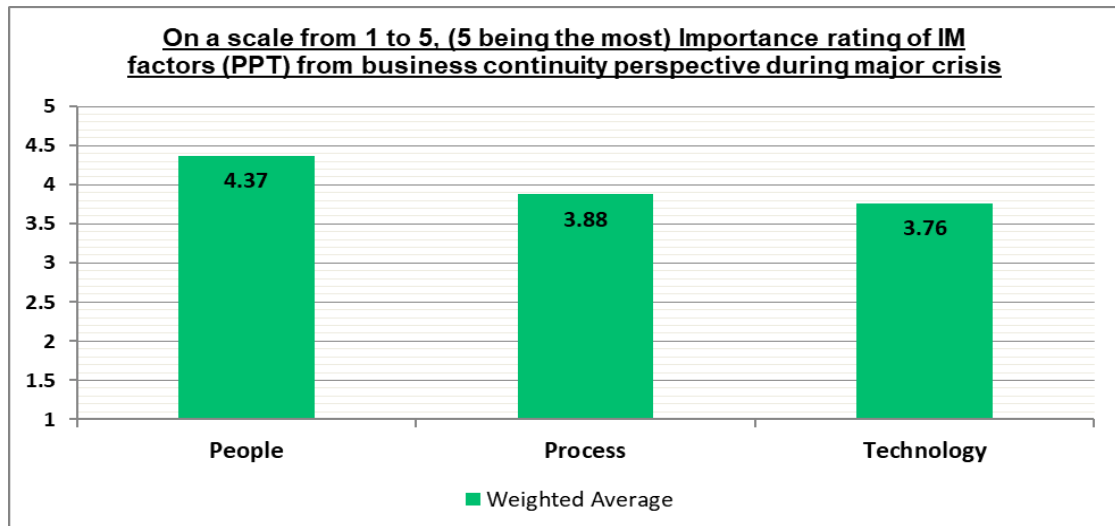


Figure 23: Chart for survey Question 1

Data results from the first question show that “people” factor is the dominant one (in weighted average value) as an immediate first response of the experts (with 56% ranked as the “most important”, followed by process and technology). This is also the general perspective of the information knowledge management (IKM) community, and it is reflected in much of the examined literature. The fact that technology was given a value of 3 (average importance), 13 times out of 41 is something that needs to be further explored.

Comparing with the results from the first iteration, it does however divert from the tendency of the theoretical scholars to invest more on process in the examined literature.

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

❖ Q2.

From your experience with IGOs, what is the perceived level of preparedness on each of the three Information Management aspects (PPT), with respect to crisis and business continuity management?

	Not prepared at all	Some but not enough	Average or just enough	Sufficient preparedness	More than enough	Total	Weighted Average					
People	0.00%	0	19.51%	8	53.66%	22	21.95%	9	4.88%	2	41	3.12
Process	0.00%	0	24.39%	10	26.83%	11	43.90%	18	4.88%	2	41	3.29
Technology	0.00%	0	26.83%	11	36.59%	15	29.27%	12	7.32%	3	41	3.17
											Answered	41

Table 7: Data results from survey Question 2

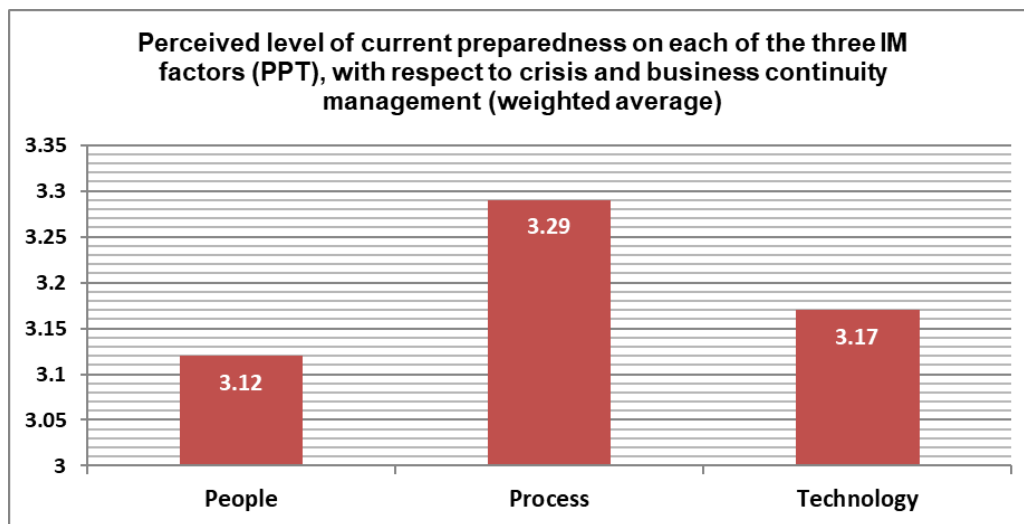


Figure 24: Chart for survey Question 2

According to the participating audience, process is believed to be the IM factor with the most sufficient level of preparedness in IGOs, while people is the factor with less preparedness, ranked mostly as “average or just enough”. In a multinational and intergovernmental environment, it is expected to have a fluctuating and dynamic rotation of skilled staff on key positions pre-agreed by the member nations that, at times, may create some gaps at the level of preparedness.

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

Technology is considered to be also at average level of preparedness but with plenty of room for improvement as a considerable percentage (26.8%) of the questioned audience believe that the preparedness in technology is not enough.

❖ Q3 (open-ended)

How exponential technology progress trend, affects CBCM in IGOs⁷

Subject matter experts from IGOs (such as business continuity & crisis managers, business managers, risk managers, IT & Technology managers) believe Technology is essential to crisis management. For some of the participants, the most prominent examples are energy production and mobility. Growing reliance on technology for business without well thought through and well exercised continuity management can create detrimental issues. But if well thought through and exercised, today's technology can make IGOs fully resistant against crises. But it needs to be a clear organizational objective, well resourced, led by top management and regularly exercised. Remote working capabilities, storage in secure clouds, distributed teams – technology enables all of this and by this many physical risks of crises can be mitigated.

It is believed by many participants that uncertainties will increase in the future and that exponential theories (such as Moore's law) are proven to be catalysts on the effect of technology to crisis and business continuity management. Accelerating technology has started to leave humans ("people" factor) behind, disrupting the overall balance between PPT in CIM. According to a response, "people" and "process" factors can be more manageable and predictable by the organizations in the PPT equation, hence prevention and preparedness (from the PPRR model) are becoming more crucial for this chase of tech advancement in the future. Exponential technology advancement creates big challenge and demand on tech preparedness for crisis.

⁷ Personal identity of answers from open-ended questions is not disclosed as agreed in advance with survey participants. Some of the participants were contacted at a third iteration phase of the analysis for further explanation and input, but we consolidate all responses in this section.

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

On the other hand, some experts believe that there is too much focus and responsibility placed on technology with the view that technology will solve all problems during a crisis. Experts from the humanitarian crisis management domain (such as UN agencies) believe that despite our technological dependency we count on highly prepared staff able to circumvent crisis when they come. The fact of having contingency plans helps with the time it takes to overcome crisis.

A general perspective is that exponential technology affects all organizations; not only intergovernmental and being able to manage the unknown unknowns, is what can make the difference.

Another interesting observation from the experts is that in the past, business continuity was in many cases possible through reversion to manual processes when technology failed. In the current environment, due to the quantity of information being processed, manual procedures are no longer viable so a critical technology failure may cause a cessation of business. In addition, with the increase rate of technical complexity, the number of technical risks increase (for example security), hence, the business continuity planning becomes more complicated, more difficult to maintain and keep up to date. Consequently, technology as an IM factor has to be based on lean processes, and vice-versa; lean processes need to be based on current (not obsolete) technology.

The increased dependencies upon technology to perform all types of businesses have made the organization more vulnerable, thus have a negative impact on crises and BCM by acknowledging the importance or shift of the focus to crisis and business continuity management and its importance within an organization. Although the basic mechanisms remain diachronic (disruption happens and forces recovery efforts), technology as factor has increased the speed by which disruption can take place, as well as the severity of a disruption.

On a different point of view, it all depends on the nature of business. In general, IGOs adapt to an environment with risks that cannot be identified and assessed adequately and so may not be treated or mitigated proactively. If someone considers that IGOs are in general less adaptable and flexible than private sector in finding

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

innovative solutions or coping with unprecedented threats, then one can also assume that the negative impact could be significant and lasting.

Although in crisis both challenges and opportunities can emerge, exponential technological progress has brought up more vulnerabilities to organizations. It is believed by some of the target audience of the survey, that the exponentiality of technological advancements is a potential threat or opportunity that is not usually considered in the scenario-based preparedness and planning, and intergovernmental organizations are impacted by technological progress and change. Furthermore, as expressed by many from the technology and IT domain, the complexity of information systems leads to an increasing reliance on asset and configuration management. Cyber threats is a domain by itself where restoration of systems is time critical. This affects the level of Business Continuity configuration data that needs to be maintained. In addition, as change creates risks, opportunities and choices, technological progress has caused a significant increase on complexity (society in all its facets, including the economy), so that “what is going on” seems ever more opaque. There are more actors involved now than ever before, hence coordinated effort and concerted action are more difficult to achieve. Finally, this exponential trend puts pressure on dedicated and active management and investment to at least stay at par.

On another perspective from survey participants, progress in technology makes communication and collaboration much more rapid and smooth. Unfortunately, this takes the technology focus away from leaders establishing redundant processes, often instead relying on elaborate technologies. In the event of a technology failure, individuals and teams may be prepared at performing their duties in degraded state; even if they still have the tools, they need to do the majority of their urgent functions.

From the “people” perspective, a survey participant mentioned that generally, staff have difficulty simultaneously performing their daily duties and keeping up with new technology; very few staff actually understand the detailed workings of new systems as they are introduced. In times of crisis, business continuity is sometimes threatened by the introduction of chaos and the fact that few people will understand sufficiently how

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

the process work within the technology, in order to either continue the system in a new environment or restore the system if it goes down entirely or needs replication. So, the impact can be quite significant if processes and people are not kept pace. Others also believe on the relativity of the issue versus the time, meaning that fundamentally “people” or staff are considerably the same as a century ago, being field experts and working with the certain speed, methods, and technology available.

On other inputs from participants on this open-ended question, technological progress has always worked as a game changer (just think the atomic bomb). Depending from which side you see it, it implies risks and opportunities. Today the biggest challenges are connected to information related novelties such as, for example, use of deep fakes on social media for counterinformation. Organizations can train staff to face those challenges, but it is much more difficult with bigger general audiences, and the impact can be unpredictable. Today, business continuity by intergovernmental organizations is highly dependent on technology (allowing to connect to networks from anywhere at any time). If you lose this capability, in most cases continuity cannot be ensured. Therefore, continuity is easy when you have them operational, but if you lose them there is often no "old fashioned" plan B. Frankly speaking, this becomes noticeable to more organizations as dependency on high tech increases.

From the IT perspective, it is expressed that looking only at the risks and potential threats (rather than opportunities), cyber-attacks, failure of systems and protection of data seem to be the major concerns, especially where systems and networks are connected and can lead to cascading failures. Cloud and shared infrastructure can expose IGOs to new risks like services availability, data leaks that are out of their direct control. Large organizations and institutions are often behind technological trends and risks, which might lead to grave impacts in such a scenario. Securing expertise on site and adaptability should be taken into consideration early on. Advances in cyber-attack and customer demand for uninterrupted services particularly to critical services, demands more robust, timely and automatic responses to mitigate such threats. AI and Data Analytics will be crucial in supporting such capabilities. An expert points out the

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

over-reliance issue; when a disaster strikes, people are unprepared with alternatives (loss of cellular/telecom, for example, or data protection issues, hacking data, ransomware, etc.).

Equipment, Hardware and Software Obsolescence and high rate of developing technologies in systems and their underlying subsystems, increase risks relevant to security, budget derail and adequate highly skilled resources.

It is a common understanding among survey participants that unpredictability will likely grow in the real world. But an IGO must also embrace technological change to be able to manage this unpredictability and its damaging effects.

Technological progress has not been directly linked to crisis management and business continuity plans. In some cases, organizations are surprised by the technological gap when hit by a technology related crisis.

Attention must be paid to preparedness and alerted state on what new is coming from technological innovation that can act as a risk factor (disruptive technology as a cause of a crisis). It is generally believed that exponential technological progress can have great impact in crisis management capability, and it is relative to the overall performance of the organization during crisis.

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

❖ **Q4.**

For one indicative unit of change in “Technology” as Information Management factor, what is the perceived change required in “People”, for an effective Crisis Management and Business Continuity Plan?

Answer Choices	Avg Number (from 41 responses)	Total Number	Responses	
scale range (-10, 10)	2.15	88	100.00%	41
			Answered	41

Table 8: Data results from survey Question 4

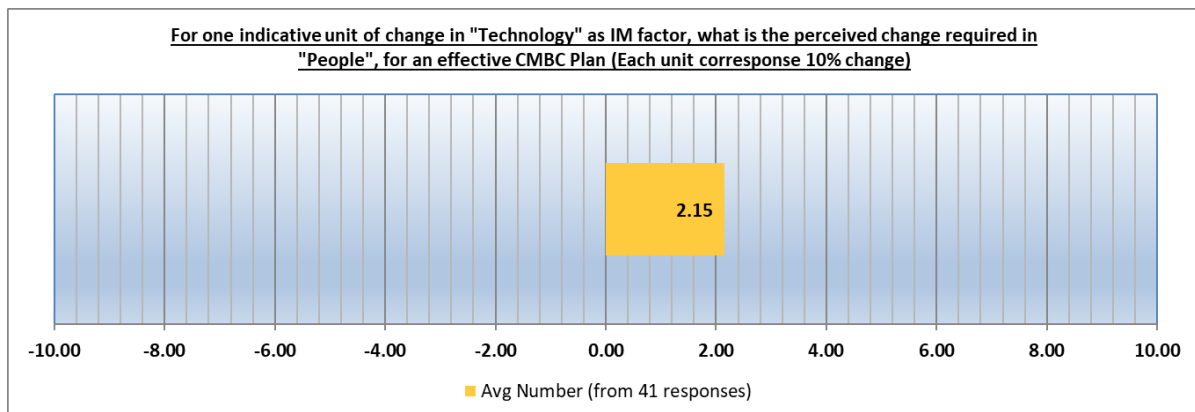


Figure 25: Chart for survey Question 4

According to the survey results, the perceived change requirement in “people” (as IM factor), based on an indicative unit change in “technology” factor, is 2.15 which means that more than 20% of change effort in “people” is required for every unit (10%) of change in “technology” in the organization for effective crisis and business continuity management. This is in line with the perception of importance of people as IM factor against technology as derived from results of the first question.

The participating audience of the survey have made a clear and strong point advancing the need of skilled people in crisis and business continuity management (as level of effort) for every incremental change in technology affecting the organization.

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

This however reflects the initial reaction to technology change as it is the initial stage when an increased number of people is normally needed to be trained and familiarized with the technological change in an organization.

❖ **Q5.**

For one indicative unit of change in “Technology” as Information Management factor, what is the perceived change required in “Process”, for an effective Crisis Management and Business Continuity Plan?

Answer Choices	Avg Number (from 41 responses)	Total Number	Responses	
scale range (-10, 10)	1.39	57	100.00%	41
			Answered	41

Table 9: Data results from survey Question 5

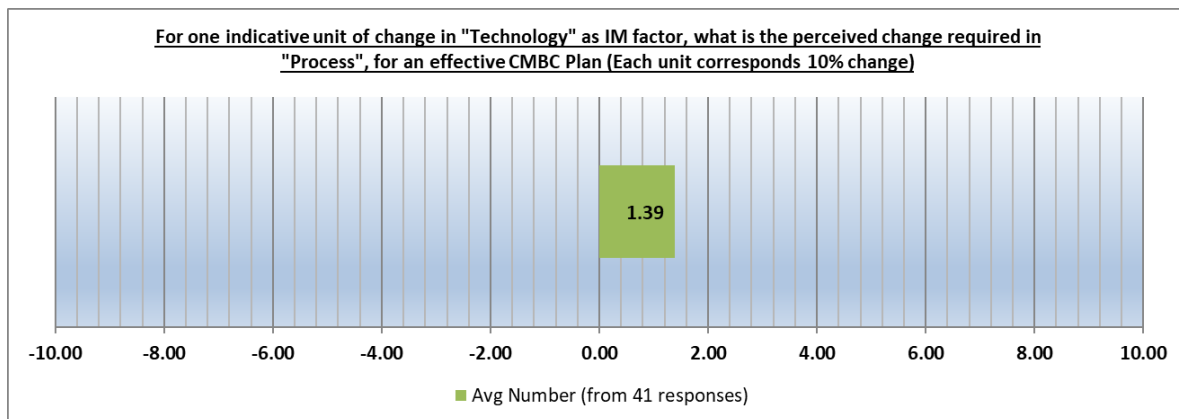


Figure 26: Chart for survey Question 5

According to the survey results, the perceived change requirement in “process” (as IM factor), based on an indicative unit change in “technology” factor, is 1.39 which means that more that ~14% of change effort in process is required for every unit (10%) of change in technology in the organization for effective crisis and business continuity management. Here the gap between technology and process seems much smaller and process is perceived to be more dynamic and ready to change and adapt to the need of the crisis situation.

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

The combination of the results from questions 4 and 5 are in line with the overall expert's opinion on the importance rating of the IM factors as described in question 1, putting people (followed by process) as the key factor within the PPT IM framework.

❖ **Q6.**

In a scenario based on the simplified PPRR model of Business Continuity Planning; Represent your choices on sharing the resources among the three IM factors (people, process, and technology). (Justify your selection if required)

	Prevention		Preparedness		Response		Recovery		Total
People	39.02%	16	60.98%	25	65.85%	27	24.39%	10	41
Process	34.15%	14	51.22%	21	68.29%	28	34.15%	14	41
Technology	48.78%	20	26.83%	11	56.10%	23	56.10%	23	41
Explain your main reason behind your selected answers.									28

Table 10: Data results from survey Question 6

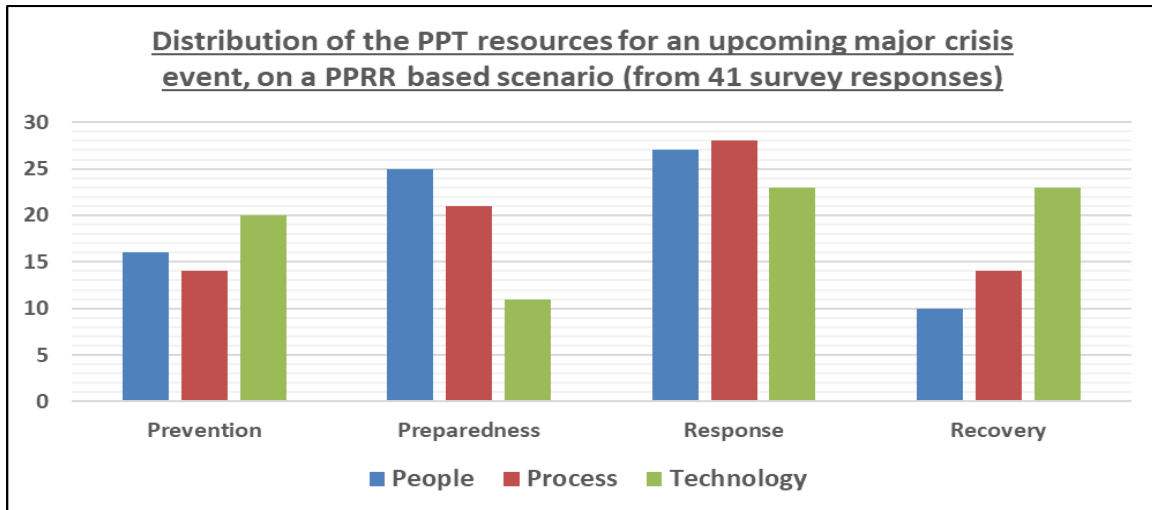


Figure 27: Chart for survey Question 6

The results on this question as shown in the table and figure above, reveal the importance of people and process (as IM factors) during the preparedness and response in the PPRR model, and the equal importance of technology in the prevention, response and recovery phases of the model. Another significant point on the chart is the low

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

requirements chosen for “people” during the recovery phase and for “technology” during the preparedness phase.

Participants were also asked to optionally justify their selections. Technologists from IGOs mentioned that humans represent the first line in any response to change / crisis in any project, while processes provide the needed certainty and “rule of law” for the recovery process. Finally, technology is the element that can respond to the need to be prepared. All three elements are needed in the prevention domain.

According to another comment, technology needs to be reliable for an ensured recovery. People need to be well trained in order to be able to respond to the crises and processes need to be prepared. However, technology is an enabler. People is the real key resource in business continuity. Process is just an inhibitor to effective execution.

Input from another participant suggests that technology can help reduce the likelihood of incidents occurring and will be key in responding to them when they do occur (e.g. clustering and failovers). People will be required in all aspects but should be trained/exercise (preparedness) in the processes and will be key in the response when technology will not be available to assist. The processes for response and recovery must be well-defined as when an incident occurs, a repeatable process must be available.

Others suggest a solid process in the response and recovery phase as process needs to be well understood and exercised by people during preparedness, and technology is a prevention mechanism as well.

Given the constraint we set in this question in choosing two columns per row, and although participants believe they are all relevant to establish an effective crisis management and business continuity process, some experts would choose response and recovery at the expenses of prevention and preparedness. But without the latter, the response and recovery mechanisms and processes will never be effective. In that respect, an expert correctly emphasizes that the factors are not mutually exclusive. Predictable processes can enable a solid prevention and preparedness stance. People and technology can go the extra mile and play a more significant role to operationalize the BCP – in terms of readiness, response, and recovery.

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

Some participants from senior programme management and risk management domain, believe the focus needs to be given to people and process as these are normally the most neglected parts.

From another point of view, it is believed that it is important to be able to have robust 'business as usual' coping methods. When circumstances are beyond our control, the ability to recover could become paramount. Another expert would ensure that "business as usual" processes prevent disruptions, and if a disruption occurs, then ensure there are good processes to respond and recover. In addition, ensure that staff is prepared/trained for managing disruptions and are using the response processes to ensure full recovery. Technology is seen as the first line of defence in preventing a disruption (keeping intruders out, ensuring redundancy of systems and data etc.) but also as a means to a speedy response and thus recovery.

Experts from technology management domain, suggest "people" for the anticipation, "technology" for the aftermath and clean-up, and "process" in-between. This approach also complies with the best practices of the general PPT framework, where we start with "people", then address the "process" and last but not least top it off with "technology". According to others, staff and processes should be prepared to respond to business continuity disruption whereas technology should provide a line of defense (prevention) and be positioned to automate recovery as much as possible.

In a simplified model such as PPRR, some experts would reason that technology should be designed to prevent disruption under crisis situations and to quickly recover from an event. People should be trained to prepare for an event and instructed how to respond adequately. The processes should be defined and communicated to the people as to how to respond to an event and recover from an event. An additional input suggests that people need to lead the way. Technology aids recovery and process links the two outside of crisis.

A quick and effective response resides in prepared people that can count on reliable technology used through clear processes.

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

Risk management plans are often strategic, over-arching, while technology is constantly evolving. Therefore, Preparedness and Response might be more directly effective towards ensuring continuity of technology operation in times of crisis, while the risk management plan delineates the process related to technology in a more overall strategic manner.

Some participants point out that we use technology to mitigate the known threats and ensure capabilities to recover from any threat. We ensure processes, procedures and instructions are efficient and effective at treating incidents and recovering impacted capabilities. Regarding people, we ensure robust risk management and resources needed to adequately treat incidents.

For many risk and crisis management experts, people and process are the two important factors for prevention and response phase of the PPRR model. Technology role is less important as it is providing the tools for people to implement the processes.

Finally, knowledge is key to prevention and preparedness. Appropriate technology and educated people require efficient resources to support their effectiveness, and crisis response requires high people effort with an understanding of the process.



MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

❖ Q7.

How would you rank the crisis categories described below, with regards to their criticality on organizational strategic goals and objectives?

Crisis category	1		2		3		4		5		Total	Ranking Score
	Weight	Score value	Weight	Score value	Weight	Score value	Weight	Score value	Weight	Score value		
Global Public Health crisis	17.07%	7	34.15%	14	17.07%	7	21.95%	9	9.76%	4	41	3.27
Global Financial crisis	12.20%	5	19.51%	8	29.27%	12	29.27%	12	9.76%	4	41	2.95
Global Environmental crisis	9.76%	4	24.39%	10	26.83%	11	21.95%	9	17.07%	7	41	2.88
Global Security crisis	48.78%	20	12.20%	5	7.32%	3	12.20%	5	19.51%	8	41	3.59
Internal (organizational crisis)	12.20%	5	9.76%	4	19.51%	8	14.63%	6	43.90%	18	41	2.32
											Answered	41

Table 11: Data results from survey Question 7

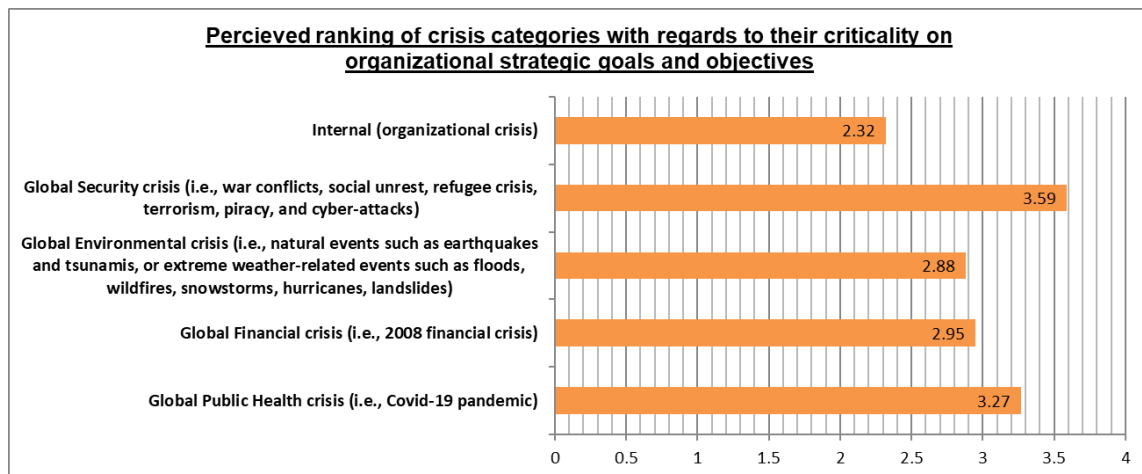


Figure 28: Chart for survey Question 7

Global security crisis is clearly the number one perceived crisis category as ranked among the 41 survey participants. Conflicts, refugee crisis and social unrest during the last years in different parts of the world may have contributed to the high ranking of this type of crisis, followed by the global public health crisis, obviously influenced by the recent covid pandemic, the persistence of which may have affected the opinion and perception of the experts. Global financial crisis and environmental crisis are closely following the ranking with marginal difference. Internal (organizational) crisis is a type that is not often occurring in IGO's as much as it occurs and affects businesses and the profit oriented private sector in general.

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

Overall, the perceived ranking is considered as expected by the author with no major outliers in comparison with business in industry & private sector.

❖ **Q8.**

With regards to prevention and preparedness as part of business continuity planning in an IGO, how do you think the efforts (in %) are shared among the three IM factors (people, process, technology).

Answer Choices	Average	Total Number	Responses	
People	33.95	1392	100.00%	41
Process	32.02	1313	100.00%	41
Technology	34.02	1395	100.00%	41
	100.00		Answered	41

Table 12: Data results from survey Question 8

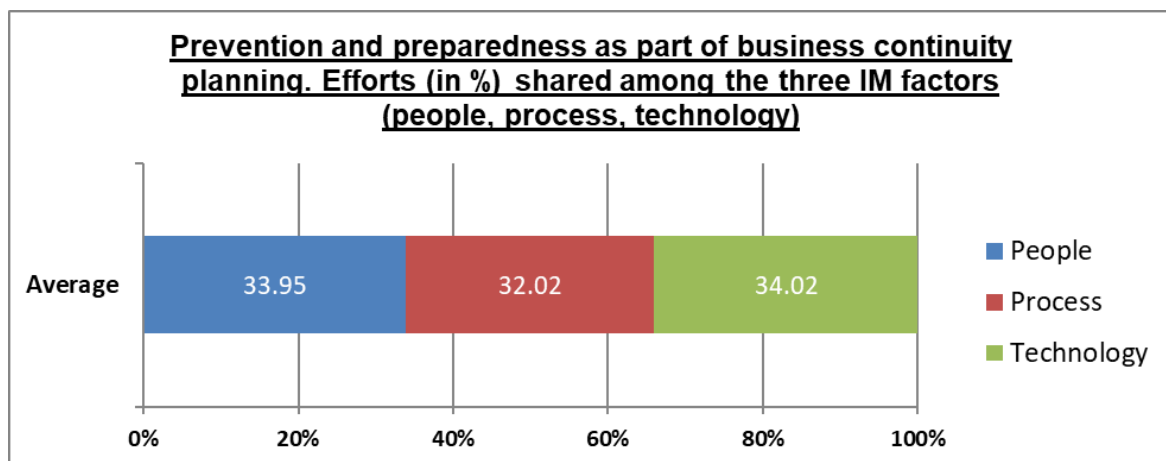


Figure 29: Chart for survey Question 8

There is an impressive balance in the results, between the three IM factors. Efforts among the factors “people”, “process” and “technology” are equally distributed (between ~32 and ~34 %) as part of business continuity planning at the prevention and preparedness stage of the PPRR model. The slightly increased percentage of technology is negligible but indicative to the perceived need to ensure that the required technology and tools are in place, especially in an approaching crisis situation. For IGOs this is a significant change of mindset from the traditional perception and theoretical framework to a more holistic approach of the three (PPT) factors. Nevertheless, it would be

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

interesting to distinguish the results depending on the background of audience (for example CM/BCM specialist versus IT and technology specialists).

❖ **Q9.**

Considering the accelerating technological advancements how would you reconsider the importance rate of the IM factors in response/recovery of major crisis, disaster, or disruption, in an IGO? (“technology” includes critical infrastructure.)

	1 Less important		2		3		4		5 Most important		Total	Weighted Average
People	0.00%	0	7.32%	3	7.32%	3	48.78%	20	36.59%	15	41	4.15
Process	4.88%	2	4.88%	2	26.83%	11	51.22%	21	12.20%	5	41	3.61
Technology	2.44%	1	2.44%	1	21.95%	9	26.83%	11	46.34%	19	41	4.12
											Answered	41

Table 13: Data results from survey Question 9

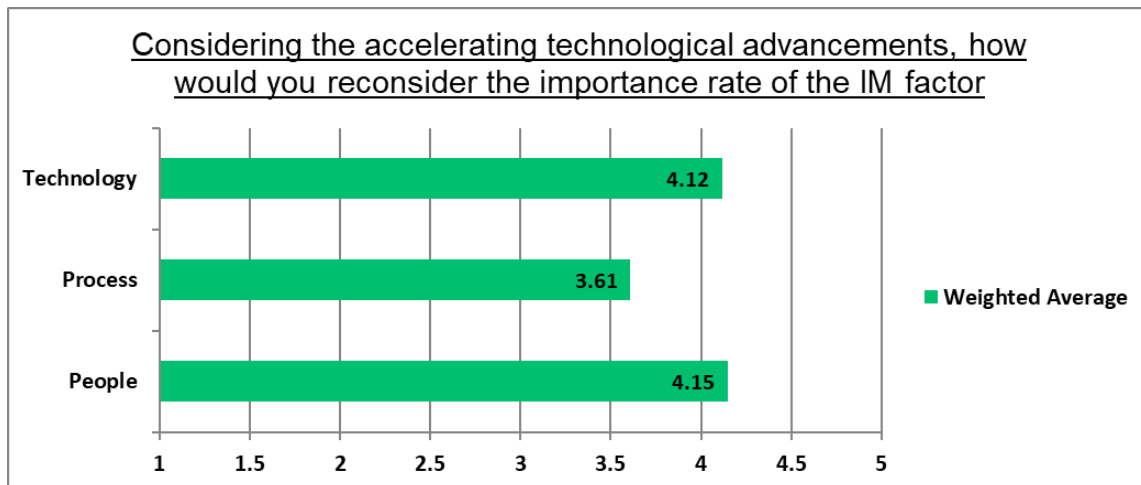


Figure 30: Chart for survey Question 9

Introducing in the discussion with the survey participating some data and facts regarding the accelerating technology in various and diverse domains of our society, we seek for a “second thought” on the importance of the three IM factors and the balance between them with regards to crisis and business continuity managements from an IGO perspective.

The accelerating developments of the digital era in multiple domains such as robotics, AI/ML, quantum computing, space, VR, civil engineering,

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

telecommunication, transportation, genomics, cyber, medicine, blockchain, etc., is something that is in constant progress and often we take it as normal during the last few decades although it is something unprecedented. As a result, experts (both from risk and crisis management, and from programme management domains), perceive the existence of technology in the organization as a fact or standard, focusing on the areas where traditionally crisis management and business continuity is shifting the center of gravity of efforts, which is people and process.

Comparing the results with the Q1 where we grasped the first unbiased perception of the experts, we can clearly see the change. Based on equally used weighted average calculations, “people” remain in first position of importance (with 4.15) as a CIM factor, while we have a considerable drop of the value of “process”, mostly at the expense of “technology” which is now valued (with 4.12) almost in par with the “people” factor. This is obviously a revisionist approach of the question where participants had the time to consider the deeper implications of the three IM factors and their inter-relationship based on objective data and information.

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

5.3 3rd Iteration – Analysis from additional literature and previous results

In this phase we first attempt a re-arrangement of the data results of the first iteration in publication chronological order (based on the date of publications of articles), and cross-reference of the average values of the PPT factors per decade that the articles are published.

PPT factors	Average score per time-period articles published ⁸		
	1990s	2000-2010	2011-2021
People	<i>11</i>	<i>10.8</i>	<i>14.8</i>
Process	<i>11.8</i>	<i>13.2</i>	<i>12.8</i>
Technology	<i>7.2</i>	<i>8.4</i>	<i>6.3</i>

Table 14: Average score of PPT factors per publishing time-period

We notice a consistency on the dominance of people and process factors over technology, during the last 3 decades, and a considerable drop in technology score value (in comparison with “people” and “process”) during the last decade.

So, why such big gap between technology on one side and people/process on the other?

Firstly, the events of 9/11 were a catalyst for the perception of crisis management process and technologies used in the first decade of the century when global security was the type of crisis that occupied most analysts. Even publications on the theoretical frameworks of CM, DRM and BCM, had a considerably increased consideration of process and technology (as CIM factors) in their context during that decade. Especially regarding technology, the scoring in appearance of relevant terms on literature from the first research iteration increases by ~17% for this decade (2000-2010).

Similarly, the decade that followed (2010-2021) was marked by many natural disasters, environmental and humanitarian crisis, especially in parts of the world that population is most vulnerable (i.e., major conflicts in areas of Africa and middle east, earthquake in Haiti 2010, earthquake, and tsunami in Japan 2011, followed by the nuclear disaster in Fukushima, wildfires in California 2018 & 2020 and other). Those events triggered the urgent requirement of mobilization of more volunteers to crisis regions, which justifies the significant score increase (37%) of “people” related terms.

⁸ Based on the data of the first iteration

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

The event in Japan (2011) is a perfect example of a multi-faceted crisis that cannot be seen as a confined task to a single sector. The initial hit by the tsunami was a natural disaster event but the domino effect to the Fukushima power station turned a natural disaster into a nuclear one, which has resulted in huge health related and financial crisis for the nation and not only. In addition, credibility of Japanese media and government was challenged, running the high risk of an internal communication crisis. A year later at the opening speech of an OECD workshop on Inter-Agency Crisis Management, the Swiss federal chancellor pointed out that in this global environment there is an urgent need to reform state CM organizations and as the distinction between domestic and external crisis becomes more blurred, *“it no longer makes sense to have different concepts and instruments to deal with these two different situations”* (Casanova, 2012). She concluded that we need a global crisis management that can coordinate resources and stakeholders from all sectors through a coherent strategy with more cooperation between nations, and partnerships with business and industry. As we cannot rely any more on reactive crisis management, we need to focus more on prevention and preparedness such as the early warning systems in the case of Japan. And indeed, the earthquake early warning system (EEW) that was developed in 2007, saved millions of lives providing those precious 15-20 seconds of advanced warning signal, enough for people to take proper actions (either intuitive or according to prior planning). The effectiveness of the technology (data mining & exploitation, hardware, sensors, software and analysis algorithms) relied on training and education of people (including at schools), on the system itself and on standard emergency procedures (Fujinawa, Noda, 2013: 341-342). Hence, a fully balanced CIM between people, process, and technology.

Given the increasing interchangeability of the use of terms BCM and CM, Elliot, Swartz and Herbane (2010), explain the distinction between the two, in a way where the former has the tendency to be more *“business-centric”* (for companies, customers, suppliers, etc.), and the later *“tends to be sociocentric”* (Elliot et al, 2010:438), such as governmental or intergovernmental organizations, public bodies or local communities.

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

This however can affect the perception of experts in IGOs towards CIM factors and their level of significance in crisis and business continuity management. Herbane et al. (2004) introduce the term “*speed*” as a critical and profound capability for business recovery in organizations which requires a-priori readiness such as well-practiced emergency plans and provision of resource redundancies at the “preparedness” phase. Speed here is important for the reduction of exposure of the business to additional or residual risks and collateral damage of the business during recovery, and this would apply as well to IGOs within a general PPRR model.

Elliot et al. (2010), introduces the boiled egg syndrome that makes organizations comfortable with continuity of events, and should alarm senior management of organizations and states. Technology change (in Elliot’s historical context) is a factor that determines the effectiveness of BCM as a process. Information and communication technology (ICT), although seem steadily changed, in reality these technologies that increase their capacities exponentially with great reliance on supply chain, are critical for potential business interruptions. The affordability (constant decrease of costs of new technology) contributes to the speed of required change to “*organizational processes, systems, and operations*”, and due to the increasing dependability of technology-based systems, proper management of technology and IT exploitation are skills that determine organizational advantage in the digital age. (Elliot et al., 2010: 3-6).

As per OECD report, the progress in science, technology and information management (IM) achieved globally in recent decades, “*has led to a better understanding of the exposures of the built environment to hazards and threats, and the vulnerabilities of populations, economic assets and environmental resources*” (Baubion, 2013: 5), which indicates that technology as a CIM factor provides the increased resilience required by “people” & “processes” to provide risk and crisis management ensuring business continuity. To that extend, OECD promotes inter-governmental exchange of information, practices and experience, to deliver the fundamental role of governments within IGOs coordination in crisis management.

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

There is an important gap created from the difference between the trajectory view of our institutions and the exponential change of technology that directly affect the “process” factor. As explained by Azhar, most of the institutions in our society follow a linear trajectory with law and political systems, social norms, legacy companies, and intergovernmental organizations, are all just trying to incrementally adjust to change, as stability is an important force within those institutions. As a result, the incapacity of the institutions (including IGOs) to change at the accelerating speed of technology, creates a gap that translates into an exponential risk of future new unknowns and crisis situations (from environmental, to financial and security related). But the “people” factor is also intensively affected by the exponential growth of technology as our approach to work/labor is based on fundamentals from the 19th and 20th century. Azhar explains further on this. New technologies allow firms and workers to bid on short term tasks through gig-working platforms at a cost of a more secure and dependable employment. It becomes more efficient for organizations to get the right skills at the right time, even when there is an urgent requirement due to a crisis. People are human beings and as their employment status is unstable there are questions raised (like what rights do they have? Does this process empower them or dehumanize them?) that can affect their actual performance as skilled staff in a crisis event. This is the human aspect of the exponential gap affecting the IM PPT framework in crisis management.

Following our own suggestion from the analysis of question Q8 of the survey (distinguishing the background of the participants), we can suggest that, in comparison with technologists, the theorists and policy makers have a more distant approach and opinion on the technology factor and its importance in CIM.

5.4 Additional Discussion

Technology acceleration and effect on CIM

How does the technology acceleration of the 21st century affect the crisis and business continuity management systems? Today's world doesn't resemble the past as both interdependencies and nonlinearities have increased.

Digital revolution is changing the fundamentals of society as we know it. Emerging technologies such as artificial intelligence, machine learning, internet of things (IoT), biotechnology or synthetic biology, and quantum computing, provide not only unconventional opportunities, but also unconventional threats (such as cyberattacks) that can create great challenges at both national and international level.

Many intergovernmental organizations are often dealing with international crisis events (such as financial, health, humanitarian, environmental, security, etc.) that require great level of coordinated efforts with other organizations, NGOs, or national governments, either before, during, or after crisis, to confront the impact or negative consequences to the organizations themselves and to the society as a whole.

To that extend, a reliable model and crisis management process is as good as its weakest link, one of which is the person ("People" factor) putting it in action. Building consensus for rapid decision making, does not fully apply to crisis management, hence the role requires direct command and control capabilities, by persons who have the ability to handle extreme stress, and ability to see things clearly. One who is a good listener and able to prioritize with sense-making capabilities, one who shows empathy and is able to take decisions in situations of extreme uncertainty, and at the same time build trust and confidence with stakeholders.

But in a digital era where technology is advancing in unprecedented pace, and computers have already the capability to simulate many of the decision-making process thinking of humans through machine learning and artificial intelligence, the primary importance of "people" factor is becoming overtaken by events.

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

Furthermore, crisis & disasters do not guarantee change and learning. For instance, terrorism, technological development, or climate change can have catastrophic consequences, and therefore we should enhance societal resilience (Boin, McConnell, 2007: 57), and in that respect Crisis Information Management (CIM) plays a critical role. The recent scientific and technological progress, combined with better connections between technical and risk management agencies, resulted in strengthening the “*capacities of nations to forecast, warn, and activate emergency plans*” (Baubion, 2013: 16). The tools of course are not the panacea of the crisis, and governments need to detect a broader scope of links to the threat and implement preparedness measures accordingly. According to OECD (2013), governments should develop strategic foresight capacities to detect early signs (through horizon-scanning and risk radar tools) to better anticipate uncommon crises that cannot be managed with standard procedures based on traditional crisis tools (such as scenario-based planning or risk assessment based on historical events).

Predicting the future against an exponential curve is very hard for both private and public sector. According to Azhar (2021), International Energy Agency (IEA), an intergovernmental organization founded in 1974 in the wake of the global oil crisis, its World Energy Outlook was predicting for years the amount of electricity generated by solar power. IEA was systematically getting its forecasts wrong. Especially during the last decade witnessing an exponential technology of solar energy dropping in price and increasing in scale much faster than any prediction or technology outlook.

From another perspective, technology reaches maturity, a novel principle that makes the old design or principle locked-in as Arthur (2011) describes it in his arguments on the adaptive stretch of technology. As IGOs are complex and bureaucratic entities, change and adaptation to new technology is cumbersome. One of the reasons of the persistence of the “*old principle*” (apart from practical and economic) is also psychological. It is true that users or practitioners are comfortable using existing technology or tools in their crisis management or business continuity plans but are not

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

comfortable with the change and vision of the new technology, using the good old but valid mentality “if it is not broken don’t fix it” or “why change something that works well”. In crisis environment however, early adaptation (at prevention and preparation stages) is vital, and organizations need to be able to foresee those changes and adapt not only with the change of tools, but also adapt process and people, accordingly and swiftly. It is “*not just a new way of doing things, but a new way of seeing things.*” (Arthur 2011: 139).

There is an increasing discussion from the scientific community on exponential technological progress. However, in existing literature it is not directly connected to crisis and business continuity management. The acceleration of technology is discussed more in terms of non-linearity of technological change (i.e., human flight or genome/DNA sequencing), also on financial aspects in comparison with exponential decrease in costs (such as increased product quality, computing efficiency, computer storage, etc.), or as an analysis of forecasts and trends of disruptive technology including technology hype-cycles and adoption curves. All the above is useful information for crisis and business continuity managers or disaster recovery experts.

Yet, the effect that technology acceleration has to crisis and business continuity management in the modern world, has not been taken into great consideration during planning or at any pre-crisis activity of prevention and preparedness. Today there are even more accelerated achievements in technology that disrupt the business as usual more frequently and in a way that policy makers in IGOs can hardly anticipate the change requirements for crisis management plans, contingencies and recovery and business continuity plans.

In a Gartner research paper on emerging technology roadmap for large enterprises⁹, IT Professionals from 437 Organizations collaborated to benchmark adoption plans, anticipated value and risk for 111 infrastructure and operations technologies (Gartner,

⁹ As per Gartner, large enterprises are defined as organizations with more than \$1 billion in revenue.

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

2021). We can see in Figure 31 that there is a number of new technologies with high deployment risk (and value) in the areas of network, security and IT automation. This roadmap also collectively illustrates how complex the challenges or risks really are, for IGOs that are involved in global or regional crisis management. Dual use technologies can contribute to social progress but also increase uncertainty that can lead to major crisis or disasters.

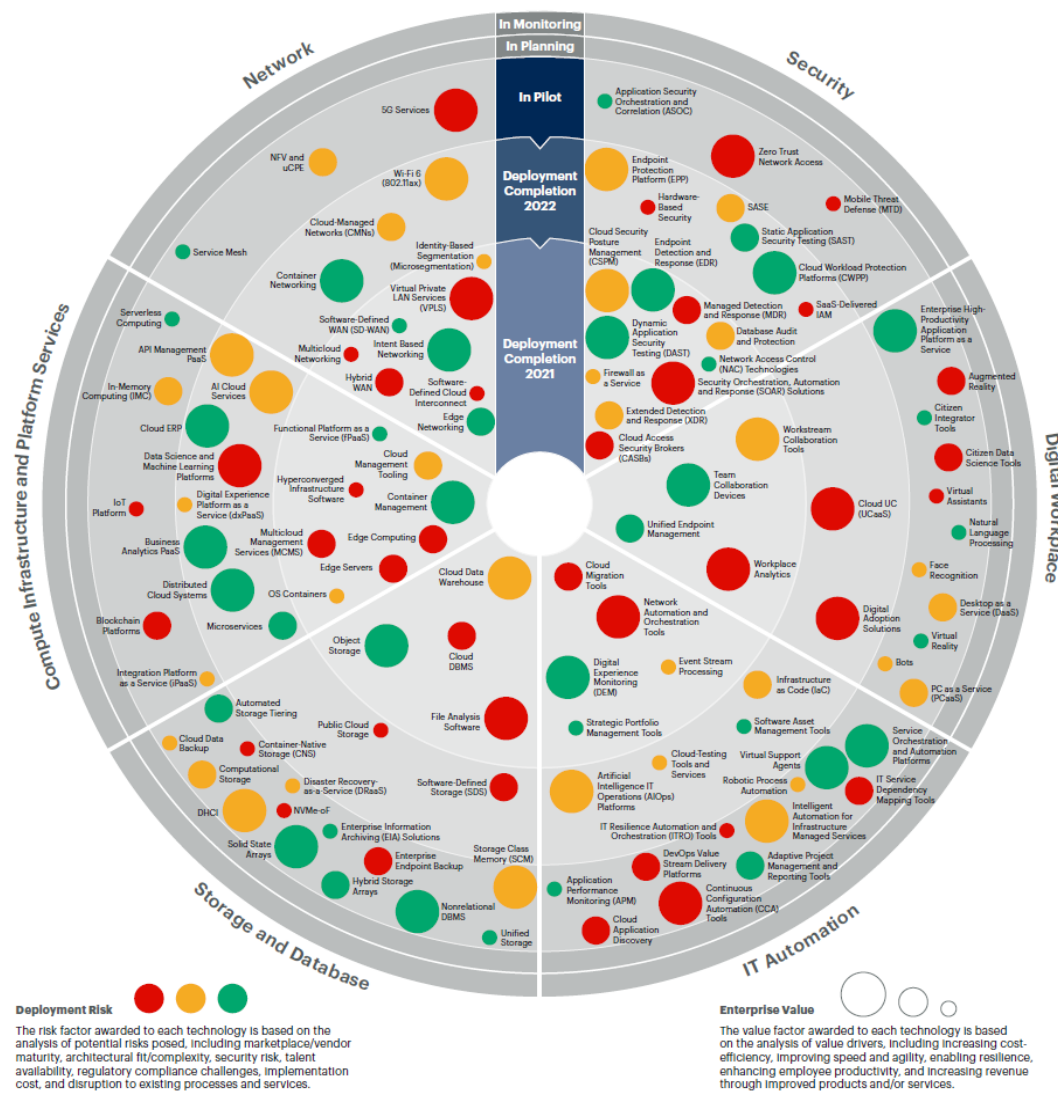


Figure 31: 2021-2023 Emerging Technology Roadmap for Large Enterprises, Deployment risks and enterprise values (Gartner, 2021)

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

Although this roadmap refers to enterprises and the effect of the risks to their value, including cost-efficiency, agility and productivity, IGOs are indirectly and often directly affected by those escalating risks that materialize into crisis, not just internal for the enterprises but at regional, national or international level.

And this is just the civil perspective of the emerging and disruptive technology risks. On the military and defence side of the equation, the security related vulnerabilities from rapid development of dual-use technologies imposes risks that can lead to potential crisis or conflicts (domestic or international) such as cyber-attacks, terrorist attacks and armed conflicts. Horizon scanning and analysis of tech trends from risk and crisis management perspective is therefore an important element for keeping the right balance between the three IM factors (people, process and technology).

From the IT security point of view, Schneier (2013) argues that the landscape became so complicated that it can no longer be managed and controlled by humans or procedures and suggests that technology is needed to leverage security controls. Therefore, the known PPT framework needs to be rebalanced in favor of automation.

As we rely so much on policy and people, neither of which is reliable enough (from IT security perspective), especially when dealing with fast-changing, large-scale infrastructures (Schneier, 2013). Of course, we need to consider the perception of uncertainty. Evaluating the criticality of a threat and probability of occurring, generates a human misconception of the interdependencies between the three IM factors (PPT). Any combination of sub-products of the three factors may create uncertainty or something impossible to predict and considered unlikely to happen (black swan).

Business continuity management (BCM) is influenced by dynamic exogenous factors that affect information management and is related to constant technological change. Senior managers and executives were never in the position to predict a typical failure or a typical success. The “*socioeconomic randomness*” (Taleb et al. HBR, [2009](#)), has proven that predicting major changes is almost impossible. On top of this if we add the exponentiality of technological advancement during the last decades, the

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

randomness effect can have greater impact in our capacity to predict, prevent, prepare and plan for the next major crisis or disruptive event.

We can identify some of the CIM critical success factors based on the three IM (PPT) themes.

- **People: Training & Leadership.**

Constantly trained personnel with updated skills, leadership committed to all 4 aspects of PPRR model for effective CBCM.

- **Process: Culture (both corporate and inter-organizational).**

In business, organizational culture is a source of competitive advantage linked to profits and economic performance. When facing an international crisis, most IGOs (not pursuing a profit) often require a high level of collaboration and coordination with each other depending on the type of crisis.

- **Technology: Availability of effective IT/CIS and related tools.**

Technology as cause and technology as effect to a crisis (positive and negative impact)

Having the ability as organization to lookout for upcoming disruptions through emerging technologies that can become a threat and create potential crisis situation, and the ability to analyze potential consequences and prevent or prepare for such impacts, is an irreplaceable capability for the effectiveness of IGOs mission.

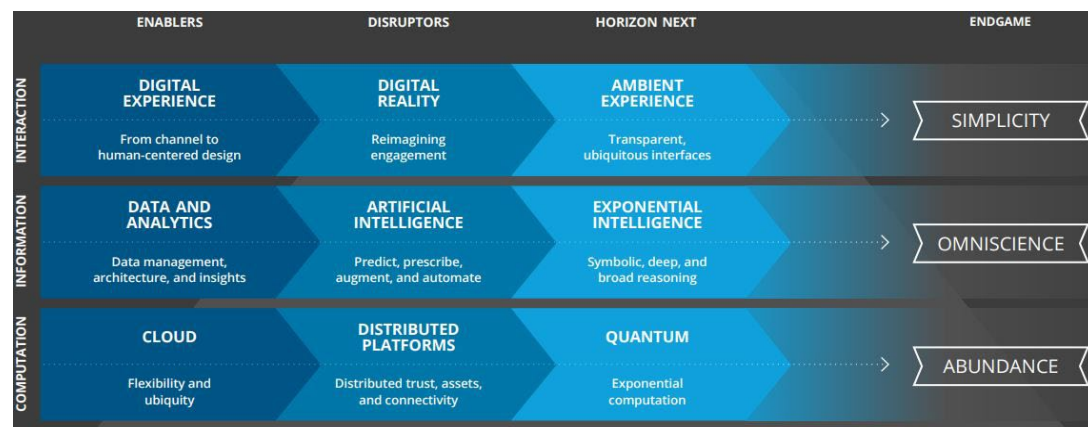


Figure 32: Deloitte, DI_2021-Tech-Trends, TechTrends2021-Deloitte, Macro technology forces, Taxonomy for emerging tech.

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

“Horizon next” in the above figure is where we find the new ambient experience of interaction, the exponential intelligence of information analysis and the exponential computation such as quantum. It is what the CTO of Deloitte calls “over the rainbow”.

Exponential technologies do not affect only the business sector as we have seen with large tech-driven companies that tend to become bigger than ever before in a way that leads to a winner-takes-all market. They also affect and transform geopolitics in global scale. As per Azhar (2021) there are two aspects of this dimension of rewiring trade, conflict, and global balance of power. First is the re-localization of the exponential age (contrary to the globalization of the industrial age), where new innovations are providing the capability of local regions to be autonomous in terms of commodities, product manufacturing and energy, which leads to tensions between national and regional governments. Second aspect is the shift of the patterns of global conflict as part of a warfare transformation, where nations or non-state actors are able to use new technologies and adversarial tactics reducing the cost of initiating a conflict. As a result, societies will be more vulnerable from attacks and will be less capable to defend themselves (Azhar 2021: 11). In order to be ready and prepared for crisis by “disruptors” governments and IGOs should engage in some comprehensive horizon scanning of what comes next and how it could disrupt both business and society.

In an automated digital era, “people” and “process” still work on human timescales, but not computer timescales, and this may require a rethinking of the way IGOs prioritize and balance the three (PPT) factors in their CM and BCM plans.

Many IGOs today are dealing with some type of global crisis as their main area of operations. It is more important that IGOs are tech savvy at equal level as private sector and industry. Following a linear trajectory (Azhar, 2021: 70), legacy companies, NGOs, political systems and intergovernmental bodies, “*have only ever known how to adapt incrementally*” because as institutions, they are fundamentally built on “*stability*” as a critical factor. This creates the exponential gap between our institutions (including IGOs) capacity to change and adapt, and the accelerating speed of new technologies.

The identified gap directly affects the first part (PP part) of the PPRR framework in crisis and business continuity management.

Chapter 6: Conclusions – Recommendations

In my attempt to contribute to the scholarly literature, this dissertation proceeded through research and analysis of the three information management factors (people, process, technology) in an area where crisis and business continuity managers meet the technologists during a period of time that advancements in technology created a gap in our perception of linear thinking and assumption that change takes decades to occur. In reality, the emergence of this gap during the last decade left many organizations unprepared and exposed to risks, while the diminishing costs of information and data processing gave opportunities to those who could foresee this change.

If CIM is a function of people, process and technology, big proportion of the people and process factors are being gradually absorbed and transformed by technology, tools and automations. As long as innovation and new technology are fueled with serious investment by both private and public sector, the speed of technological advancement will increase at a pace that “technology” as IM factor will always lead the change and the need of rebalancing with “process” and “people”.

Companies are focusing on costs of their inputs assuming they remain similar every year (perhaps with slight change due to inflation). However, IGOs with (generally speaking) break-even financial objectives, can be better prepared for major crisis in an exponential age and maintain a well-balanced CIM system.

Results of the survey and discussions with open-ended question, provide plenty of room for interpretation but also seem to present a combination of perceptions of uncertainty versus impact and probability. Depending on the chronological point in time that theories are developed, and opinions are captured through the literature, there is a subjectivity gap based on the perception of the experts. The gap is also evident from

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

the survey results, as responses of experts from IGOs tend to deviate depending on their role and experience.

From literature review and analyzed results of the survey, it is evident that an interconnected spiral effect is emerging as a result of the interdependencies between the three CIM factors.

Concluding on one of the main objectives of this dissertation on identifying the relationship and impact of “technology” on “people” and “process” in CIM, we can say with confidence that the balance between them (PPT) directly affects the effectiveness of crisis and business continuity management in IGOs. Based on these interdependencies, a helix model approach is proposed for CIM.

In the traditional IM concept, the elements of “people” and “process” dominate the scientific literature and the current framework paradigms. The investigation of the reasons behind that gap between technology on one side and people & process on the other, lead this research effort to a conclusion of re-imagining the IM factors in the framework of Crisis Information Management. The proposed idea of a multidimensional model (CIM Triple Helix model) encompasses the interdependences of the three IM elements in a way that PPT control and connectivity is based on a sensitive balance of a helix model interaction (Figure 33). In this model, Technology (as a CIM element), becomes an equally critical factor that drives the balance between all three PPT IM elements.

Although the level of each required effort needs to be balanced for the framework to remain under control, due to the changing landscape of crisis in general, it is the technology that leads the path towards future upcoming disruptions and uncertainties in the exponential age. In that sense, the strategic role of IGOs need to be further enhanced for major disruptive crisis events.

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

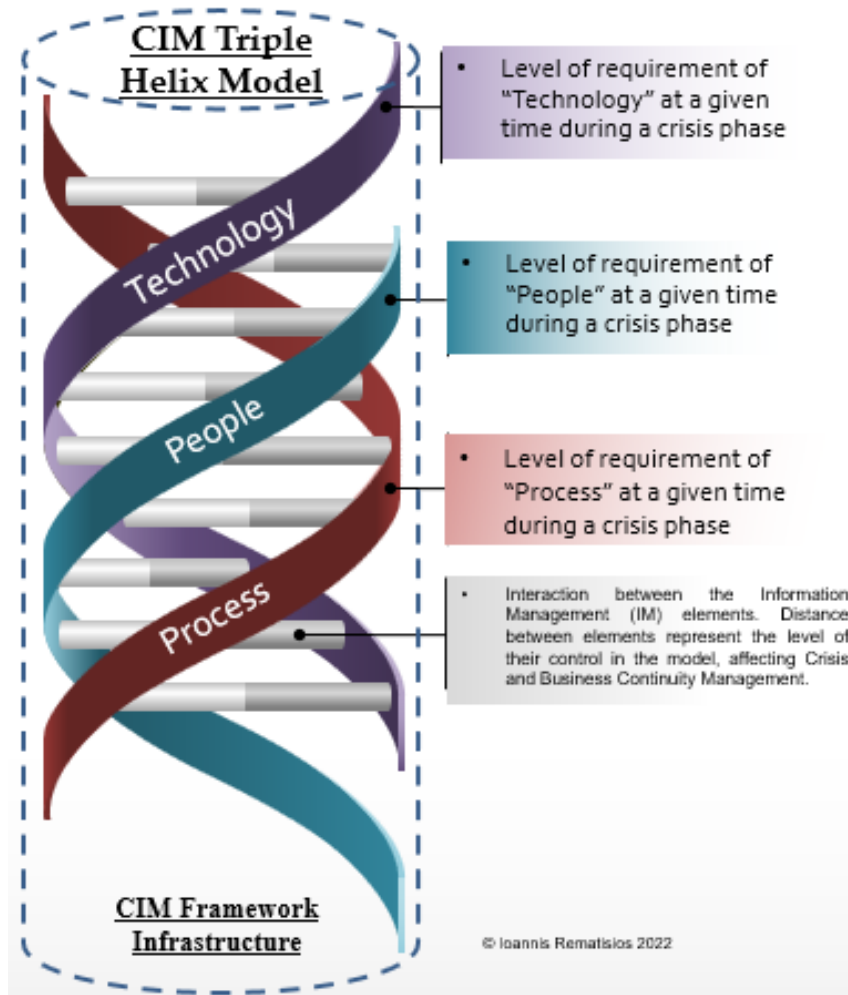


Figure 33: Triple Helix model for Crisis Information Management (CIM) (Rematisios, 2022)

The technological exponential gap is made of two forces according to Azhar (2021); the inherent difficulty of making predictions in the exponential age, and the inherent slowness of institutional change. IGOs may realize this gap even wider with the complex and bureaucratic decision-making process in multinational or intergovernmental environment. And as technology takes-off, business, governments and social norms remain almost static, and this applies also to business continuity and crisis management. As shown in the CIM triple-helix model, the interconnection between the three (PPT) CIM factors remain very fragile. Many IGOs (i.e. EU, NATO, OSCE, UN, World Bank) deal to a great extent, with major international crisis or

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

disruptive events affecting regional or global communities, hence, there is no tolerance margin for the risk of “breaking” the helix in this model. The impact and consequences of PPT misbalance, could be severe outside the boundaries of the organization. Therefore, the balance between the three factors should be carefully monitored by all stakeholders in IGOs, regardless the type of crisis (Figure 34), with increased attention to fast-paced technology advancements that can disrupt crisis and business continuity management plans at any time.

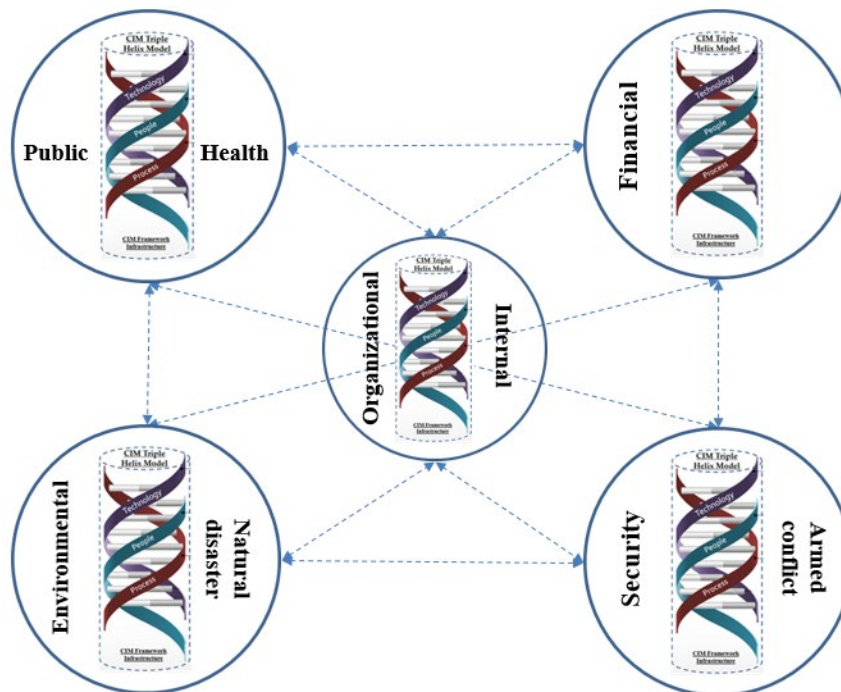


Figure 34: IGO Crisis Information Management (CIM) Constellation, Rematisios I.

In a global economy and society where everything becomes interconnected, technology is deemed to be the accelerating factor of constant change in people and process requirements. Hence, IGOs and their respective governing bodies will require a greater effort of collaboration (“people”) and interoperability between “processes” applied and “technology” used, to confront multiple major crisis events and BCM at international level. The proposed model is not a stand-alone one but is meant to be part

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

of connected helixes within an international CIM constellation, that this dissertation proposes for further research.

References

- Azhar A., (2021), *Exponential*, Penguin Random House, UK.
- Arthur B., (2011), *The Nature of Technology*, Free Press, Simin & Schuster Inc., New York.
- Baldwin B., (2016), *The great convergence*, President and Fellows of Harvard College, USA.
- Barton L. and Hardigree D., (1995), *Facilities*, Article “*Risks and crisis management in facilities*”, Vol.13 Number 9/10, pp. 11-14, © MCB University Press, [Last accessed: 28 Feb 2022].
- Baubion C., (2013) *OECD Risk Management: Strategic Crisis Management*, OECD Working Papers on Public Governance No.23, Available at <https://dx.doi.org/10.1787/5k41rbd11zr7-en>, [Last accessed: 15 Apr 2022].
- Bhatt G.D., (2001), “*Knowledge management in organizations: examining the interaction between technologies, techniques, and people*”, *Journal of Knowledge Management*, Vol. 5 No. 1, pp. 68-75. <https://doi.org/10.1108/13673270110384419>
- Boin A., McConnell A., (2007), *Preparing for Critical Infrastructure Breakdowns. The limits of Crisis Management and the Need for Resilience*, Journal of Contingencies and Crisis Management, Vol 15 Number 1, Blackwell Publishing Ltd.
- Calder A., (2021), *ISO 22301:2019 and Business Continuity Management*, IT Governance Publishing.

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

Casanova C., (2012), Opening speech at the Workshop organized by OECD (28 Jun 2012), on *Inter-Agency Crisis Management*, Available at (oecd.org), [Last accessed: 09 Mar 2022].

Chivvis C., (2010), *EU Civilian Crisis Management*, © RAND Corporation [Last accessed: 20 Mar 2022]

Clark R., (2016), *Business Continuity and the Pandemic Threat*, IT Governance Publishing.

Coombs T., Holladay S., (2012), *The Handbook of Crisis Communication*, Blackwell Publishing Ltd.

Coombs T., (2020), *Crisis Management and Communications* (Updated September 2014) – Institute for Public Relations.

Coombs T., (2022), *Ongoing Crisis Communication; Planning, Managing and Responding*, 6th ed., Sage Publications Inc., Texas USA.

Darling, (1994), *Crisis-Management in International Business*, Leadership & Organization Development Journal, Vol. 15 No. 8, 1994, pp. 3-8, © MCB University Press Limited.

Fujinawa Y., Noda Y., (2013), *Japan's Earthquake Early Warning System on 11 March 2011: Performance, Shortcomings, and Changes*, Earthquake Spectra, Volume 29, No. S1, pages S341–S368, Earthquake Engineering Research Institute.

Elliot D., Swartz E., Herbane B., (2010), 2nd ed., *Business Continuity Management, A Crisis Management Approach*, Routledge.

Estall H., (2012), *Business Continuity Management Systems*, BCS, The Chartered Institute for IT, UK.

Fahron-Hussey, (2019), *Military Crisis Management Operations by NATO and the EU*, Springer VS.

Gibb, Buchanan, (2006), *A framework for business continuity management*

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

Goda S., Tyrachuk O., Khylo M., (Eds.), (2016), *International Crisis Management: NATO, EU, OSCE and Civil Society* (Collected Essays on Best Practices and Lessons Learned), IOS Press © 2016, Amsterdam-Berlin-Washington DC.

Gonzalez-Herrero and Pratt, (1995), *How to manage a crisis before it hits*, Public Relations Quarterly.

Harsch M., (2015), *The Power of Dependence NATO-UN Cooperation in Crisis Management*, Oxford University Press.

Heba A., Desha C., Ranse J., Roico A., (2021), *Planning and assessment approaches towards disaster resilient hospitals – A systematic literature review*, Elsevier Ltd.

Hecht J., (2002), *Business Continuity Management*, Communications of the Association for Information Systems: Vol. 8, Article 30, DOI: 10.17705/1CAIS.00830, AIS Journals at AIS Electronic Library (AISeL).

Herbane B, Elliott D., Swartz E., (1997), *Contingency and Continuity- Achieving Excellence Through Business Continuity Planning*, Business Horizons Nov-Dec 1997 issue.

Herbane, B., Elliott, D., & Swartz, E., (2004), *Business continuity management – time for a strategic role?*, Long Range Planning, 37, 435–457, Elsevier Ltd.

Herbane B., (2010), *The evolution of business continuity management A historical review of practices and drivers*

Höynck W., (1995), Speech by the OSCE Secretary General at Urho Kalevi Kekkonen-Seminar “OSCE and Crisis Management”, Pielavesi, 3 Sep 1995, Available at <https://www.osce.org/files/f/documents/1/d/36958.pdf> [last accessed 20 Mar 2022]

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

Jacobsen K., (2015), *The Politics of Humanitarian Technology: Good Intentions, Unintended Consequences and Insecurity*. Abingdon: Routledge.

Jaques T., (2007), *Issue management and crisis management An integrated, non-linear relational construct*

Jaques T., (2010), *Embedding issue management as a strategic element of crisis prevention, Disaster Prevention and Management*, Vol. 19 No. 4, Emerald Group Publishing Ltd.

Kash T., Darling J., (1998), *Crisis management prevention, diagnosis and intervention*, *Leadership & Organization Development Journal* 19/4 [1998] 179–186, MCB University Press

Kovoor-Misra S., (1995), *A Multidimensional Approach to Crisis Preparation for Technical Organizations-Some Critical Factors*, *Technological Forecasting and Social Change* 48, 143-160, Elsevier Science Inc.

Kornprobst M., (2019), *Co-Managing International Crises*, Cambridge University Press.

Lindstrom J., Samuelson S., Hagerfors A., (2010), *Business continuity planning Methodology*, *Disaster Prevention and Management* Vol 19 No 2, pp.243-255, Emerald Group Publishing Limited.

Meesters K., (2021), *Crisis Information Management: From Technological Potential to Societal Impact*, Department of Management, Tilburg School of Economics and Management, Tilburg, The Netherlands.

OECD (2015), *Disaster Risk Financing: A global survey of practices and challenges*, OECD Publishing, Paris.

OECD Library, [The 2008 financial crisis – A crisis of globalisation? | READ online \(oecd-ilibrary.org\)](https://doi.org/10.1787/19936753), ISSN: 19936753 (online) <https://doi.org/10.1787/19936753>

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

Our World in Data, (2022), Article topic: *Innovation and Technological Change, Technological Progress*, Available: <https://ourworldindata.org/technological-progress> [Last accessed: 12 Mar 2022]

Phillips B., Landahl M., (2021), *Business-Continuity-Planning*, Elsevier Inc. UK.

Schneier B., (2013), Blog post titled: “[People, Process, and Technology](#)” on Schneier on Security, Last accessed [3 Apr 2022].

Singler S., (2021), *Biometric statehood, transnational solutionism and security devices: The performative dimensions of the IOM's MIDAS*, Article on journal: *Theoretical Criminology*, Vol.25(3), Sage Publishing.

Stanton R., (2005), *Beyond disaster recovery. The benefits of business continuity*, *Business Continuity, Computer Fraud & Security*, pp.18-19, issue July 2005.

Swartz, Elliott, Herbane, (1995), *Out of sight, out of mind – the limitations of traditional information systems planning*, Volume 13 Number 9/10, pp. 15–21, © MCB University Press.

Taleb, N., Goldstein D., Spitznagel M., (2009), *The Six Mistakes Executives Make in Risk Management*, *Harvard Business Review*, Available at [The Six Mistakes Executives Make in Risk Management \(hbr.org\)](#), [Last accessed: 12 Apr 2022].

Veil S., (2011), *Mindful Learning in Crisis Management*, *Journal of Business Communication*, Volume 48, Number 2.

Watters J., (2014), *Disaster Recovery Crisis Response*, Apress.

Website: Resilient Community Organizations, *Six steps to resilience, Emergency Management: Prevention, Preparedness, Response & Recovery*, Available at: <https://resilience.acoss.org.au/the-six-steps>; [Last accessed: 28 Apr 2022].

Website: *Displacement Tracking Matric (DTM), IOM Emergency Manual*, Available at: <https://emergencymanual.iom.int/entry/19108/displacement-tracking-matrix-dtm>, last updated Apr 2019, [Last accessed: 08 Mar 2022].



MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

Website: *ISO 22300:2021, Security and resilience – Vocabulary*, Publication date: 2021-02, Ed.3, Available at: <https://www.iso.org/standard/77008.html>, [Last accessed: 22 Feb 2022].

ANNEX I: Abbreviations & Acronyms

Acronym	Description
BCMS	Business Continuity Management System
BCM	Business Continuity Management
CBCM	Crisis and Business Continuity Management
CIM	Crisis Information Management
CIS	Computer Information Systems
CIO	Chief Information Officer
CM	Crisis Management
CTO	Chief Technology Officer
DRP	Disaster Recovery Planning
EOC	Emergency Operations Center
EU	European Union
IGO	Intergovernmental Organization
IKM	Information Knowledge Management
IM	Information Management
IT	Information Technology
ISO	International Standards Organization
NATO	North Atlantic Treaty Organization
OECD	Organisation for Economic Co-operation and Development
OSCE	Organization for Security and Co-operation in Europe
PPRR	Prevent, Prepare, Respond, Recover
PPT	People, Process, Technology
UN	United Nations

ANNEX II: Main Definitions

- **Crisis**

Unstable condition involving an impending abrupt or significant change that requires urgent attention and action to protect life, assets, property, or the environment. (ISO 22300:2021).

- **Crisis Management**

Holistic management process that identifies potential impacts that threaten an organization, and provides a framework for building resilience, with the capability for an effective response that safeguards the interests of the organization's key interested parties, reputation, brand, and value-creating activities, as well as effectively restoring operational capabilities. (ISO 22300:2021). Crisis management also involves management of preparedness, mitigation response, and continuity or recovery in the event of an incident, as well as management through training, rehearsals, and reviews, ensuring preparedness, response & updated continuity plans.

- **Business Continuity**

Capability of an organization to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption (ISO 22300:2021)

- **Business Continuity Plan**

Documented information that guides an organization to respond to a disruption and resume, recover and restore the delivery of products and services consistent with its business continuity objectives. (ISO 22300:2021)

- **Business Continuity Management System (BCMS)**

Part of the overall management system that establishes, implements, operates, monitors, reviews, maintains and improves business continuity (ISO 22301:2019)

- **Risk**

The effect of uncertainty on objectives (ISO 31000:2018), which is a deviation from the expected (positive or negative). Uncertain event that if occurs it creates disruption to business and operations at an organizational or national or international level.

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

- **Uncertainty**

A successful model and crisis management process is as good as its weakest link, one of which is the person putting it in action. Building consensus does not apply to crisis management. The role requires direct command and control capabilities, by a person who has the ability to handle extreme stress, has the ability to see things clearly, or one who is a good listener and is able to prioritize with sense-making capabilities, one who shows empathy and is able to take decisions in situations of complete uncertainty and chaos, and at the same time build trust and confidence with stakeholders. A state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood (ISO 22301:2019). When an unpredictable and unexpected event occurs.

- **Information Management**

Information management (IM) is the discipline that directs and supports the handling of information throughout its life-cycle ensuring it becomes the right information in the right form and of adequate quality to satisfy the demands of an organization.

From a business management perspective information management is the process of collection, storage, curation, dissemination, and archiving or disposition of different sources of information.

The three main elements of information management are: People, Process and Technology. Organizational efficiency can be achieved by balancing those three elements and optimizing the relationship between them.

- o People: Adequate number of skilled staff available for all activities required, for smooth business continuity during a major crisis event
- o Process: The updated roadmaps, plans, processes, and procedures in place for business continuity during a major crisis event.
- o Technology: Existing & backup technology available within your organization, to implement the business continuity plan effectively.

MASTER'S DEGREE PROGRAMME IN ENTERPRISE RISK MANAGEMENT

We will consider Crisis Information Management (CIM) in this respect, the notion of IM as explained above within the framework of a major external crisis affecting IGOs.

- **Intergovernmental Organizations (IGOs)**

According to Harvard Law School, IGO refer to an “entity created by treaty, involving two or more nations, to work in good faith, on issues of common interest”. In the absence of a treaty an IGO is not considered a legal international entity. Today IGOs play a significant role in international political systems and global governance. This dissertation is considering the IGOs formed by treaties, as they are “subject to international law and have the ability to enter into enforceable agreements among themselves or with states”.