

INTEGRATED ENTERPRISE RISK MANAGEMENT IN DIGITAL AND POST PANDEMIC COVID-19 ERA: LEVERAGING ON BUSINESS MODEL CANVAS FOR THE FUTURE OF MALAYSIAN ARMED FORCES

MUHAMMAD HARIS BIN ASMUNI ^{1*}, ABDUL RAHMAN BIN AHMAD DAHLAN¹

¹ Kulliyah of Information & Communication Technology, International Islamic University Malaysia

*Corresponding author: harisasmuni73@gmail.com

ABSTRACT: As stated in the Defence White Paper, Malaysia has planned to construct Malaysian Armed Forces (MAF) of the future, which will have five key thrusts: jointness, interoperability, technology driven, ability to operate in two theatres simultaneously, and mission oriented. It literally refers to Malaysia's status as a maritime nation and the government's dedication to the three pillars of the country's defence strategy: concentric deterrence, comprehensive defence, and credible cooperation. In addition, the report emphasised the importance of focusing on non-traditional security challenges such as terrorism, piracy, and marine security, as well as applying Industrial Revolution 4.0 (IR 4.0) technology to strengthen defence. The current state of digital transformation in the post-COVID-19 period has a significant impact on achieving the MAF's vision that has been outlined in the Defence White Paper. MAF's management should be in sync with the organization's strategic goals. To guarantee that the vision is realised, potential risks should be recognised, mitigated, reduced and/or eliminated. Integrated enterprise risk management (IERM) is a critical component of organisation's success, by assuring force preparedness in the face of any threats and challenges. This paper offers a possible IERM Business Model, using Business Model Canvas (BMC) framework, for MAF to consider, deliberate and adapt. The proposed MAF IERM business model is compliant with MS ISO 31000:2018 and ISO 27000 Information Security Management System (ISMS) in risk assessment, and as part of the digital transformation effort.

KEY WORDS: Malaysian Armed Forces, IR4.0 technology, Business Model, ISO 31000, ISO 27000 Information Security Management System, IERM

1. INTRODUCTION

According to The World Economic Forum, IR 4.0 technologies are continuing to revolutionise civilisation and warfare in dramatic, near-unprecedented ways. The development of "cyber-physical systems" that give humans and machines with whole new capabilities can be termed as the Fourth Industrial Revolution. The Internet of Things (IoT) is becoming increasingly popular as the world shrinks and new sensor and gadget technology becomes available. While fundamental developments in social and community formation pose governance issues, Big Data can pave the road for information dominance. International regimes must change

in order to meet this possible threat (OECD, 2017). Ideological conflict is expected to worsen. Policymakers at a government level must define and prioritize the investments that will yield the greatest returns and to ensure safety for the country. In whatever form, conflict in the future is unavoidable and the MAF must recognize these factors, adapt accordingly to overcome the ongoing and potential future threat to the nation. The current age of warfare is termed as the post nuclear age. The days of large battle wages are over, and warfare now focuses on projecting strength to troubled regions throughout the world and battling insurgents. Numbers of infantry deployed have shrunk further and development of very high technology infantry equipment is under way (Gearson, Berry, Devanny and Musgrave, 2020). Because mobility is so important, many of the troops are carried on helicopters or armoured vehicles. Artillery guns, unmanned aircraft, and cruise missiles all have long range and high accuracy fire support, with the emphasis on very accurate strikes and interdiction rather than sheer bulk of weaponry delivered on target. Air power is becoming increasingly unmanned. These are some of the issues confronting the MAF, particularly in the aftermath of the COVID-19 pandemic in the IR 4.0 age, which has a significant impact on digital transformation.

With the current development of post pandemic COVID-19 and the outbreak of digital transformation, the MAF need to have an integrated enterprise risk management system that can identify, mitigate and control potential risk. In addition, the recent IR 4.0 such as AI, IoT and cloud computing have changed defence technology lanscape with the development of smart and intelligence systems (Liang, 2018). IR 4.0 is one of the most important drivers of innovation in warfare tactics, production and automation. With this development, MAF is not only facing new risks, but also opening the window of opportunities.

2. PROBLEM STATEMENT

The phrase risk management is always used to allude to the survival, profit, and loss of an organisation. As a result, risk management is defined differently depending on one's assessment of the threat and the severity of the threat. Accountability is critical in the government sector that provides defence and security services, such as MAF. Taxpayers fund military troops and assets to safeguard citizens from internal and external threats, and to protect national interests and country's sovereignty. New risks may occur as a result of improved technology, which has been compounded by the outbreak of pandemic COVID-19 and a complex digital transformation during the era of IR 4.0, making integrated enterprise risk management (IERM) more problematic and potentially affecting strategic direction.

3. LITERATURE REVIEW

3.1 Definition of Integrated Enterprise Risk Management and Process

As the word risk is being defined based on threat perception, risk management is also defined in a different context. Risk management is part of a systematic decision-making process whereby individual or organisation identifies, mitigates and controls potential risk in order to avoid or minimise undesirable impact. In business or industrial sector, an effective risk management can avoid loss and

maximise profit, and at the same time, minimise unexpected problem (Srinivas, 2019).

According to Stoneburner, Goguen, Feringa and National Institute of Standards and Technology (2002), risk management is the process that allows Information Technology (IT) managers to balance the operational and economic cost of protective measures and achieve gains in mission capability by protecting the IT system and data that support their organization's mission.

Tucci (2021) in her article, "What is risk management and why is it important", defined risk management as a process of identifying, assessing and controlling threat to an organisation's capital and earnings. Risks stem from a variety of sources including financial uncertainties, legal liabilities, technology issues, strategic management errors, accidents and natural disasters.

Referring to International Organization for Standardization (ISO) 31000:2018, risk management process is described as in Fig. 1 below.

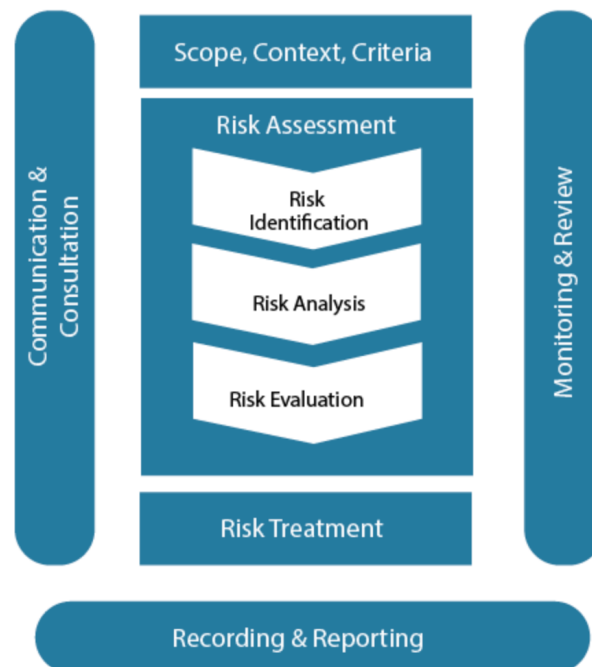


Fig. 1. ISO 31000 Diagram (Risk Management Process)

3.2 Defence White Paper Structure (DWP)

DWP portrays the government's firm and strong commitment to strengthen national defence. It represents the government's strategic point of view for the coming decade, set the direction for the defence sector and formulates a long-term strategy for defending national sovereignty and territorial integrity from any external threats.

This ten-year strategic direction and defence planning, DWP literally denotes Malaysia as a maritime nation and its government's commitment to pursuing the three pillars of defence strategy, namely concentric deterrence, comprehensive defence, and credible partnership. Besides, the paper also stresses that Malaysia needs to focus on non-traditional security issues like terrorism, piracy and maritime

security, cyber and transnational crimes, as well as apply modern technologies to solidify defence. The DWP is structured into three parts:

- a. Vision - Strategic Outlook.
- b. Strategy - Defence Strategy, The Future Force, People in Defence and International Defence Engagement.
- c. Implementation - Defence Science Technology and Industry and Reform, Governance and Funding.

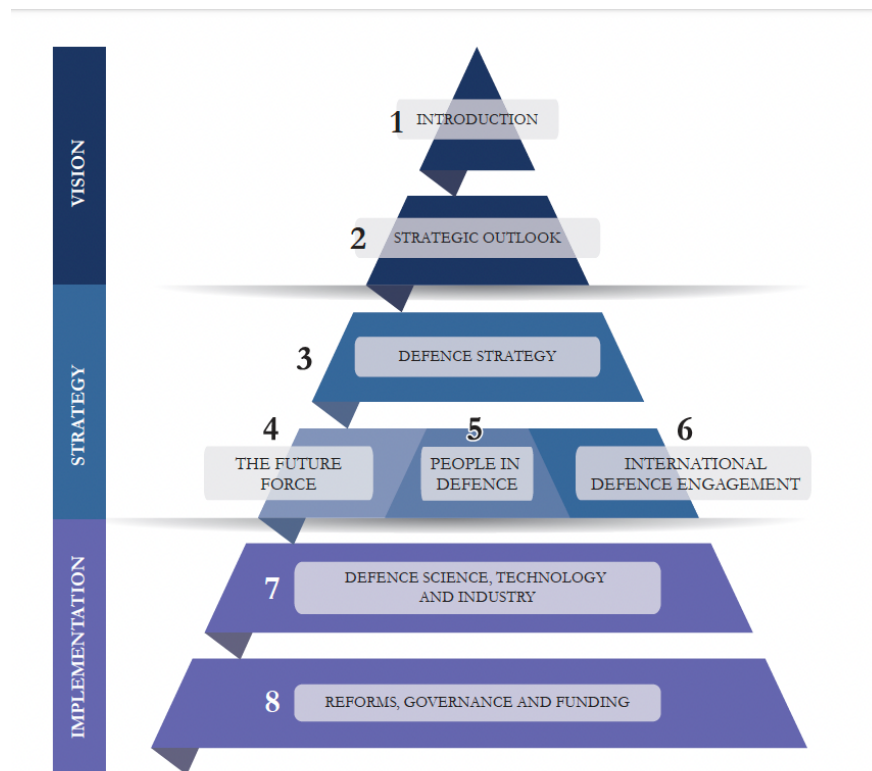


Fig. 2. Malaysian Defence White Paper (2020)

3.3 Risk Management Framework

The Risk Management Framework is based on the ISO 31000 standards risk management as described in Fig. 3 below:

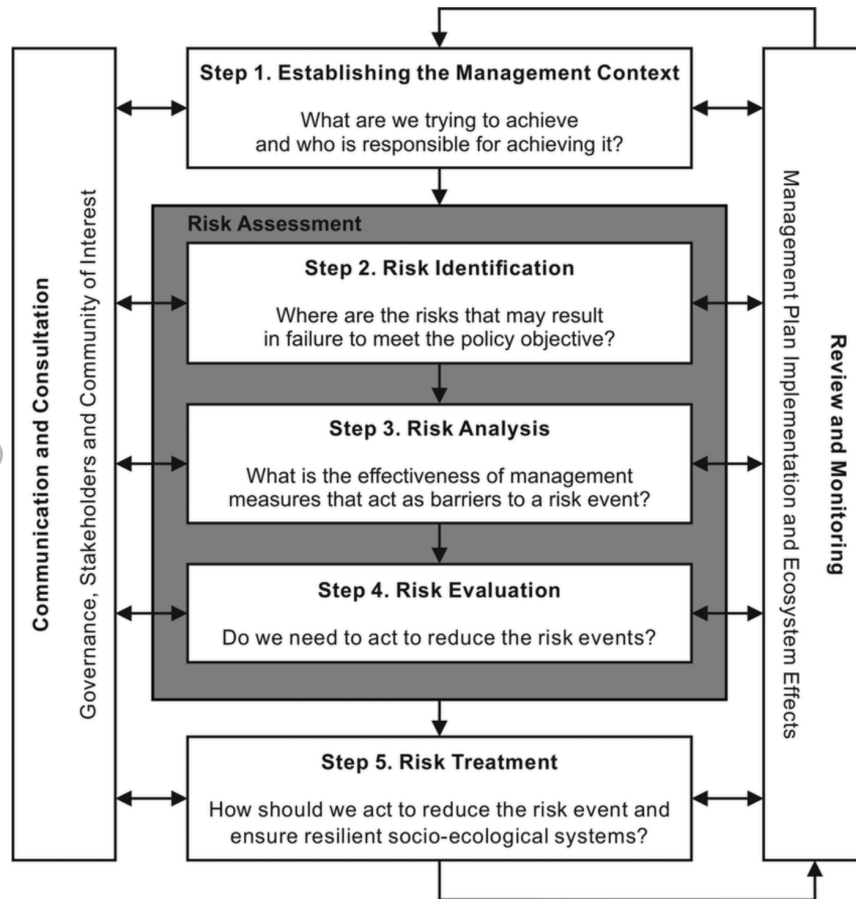


Fig. 3. ISO 31000 Risk Management Framework

3.4 US Army Risk Management Process

The US Army risk management approach appears to be simpler than the IERM risk management framework. The US Army uses risk management manual which was published from the Department of the Army Headquarters to help maintain combat power while ensuring mission accomplishment in current and future operations. Risk management applies to operations and to non-operational activities. Thus, risk management is defined as the process of identifying, assessing, and controlling risks arising from operational factors and making decisions that balance risk costs with mission benefits. Risk management is a deliberate process in which five-steps elements are shown in Fig. 4.

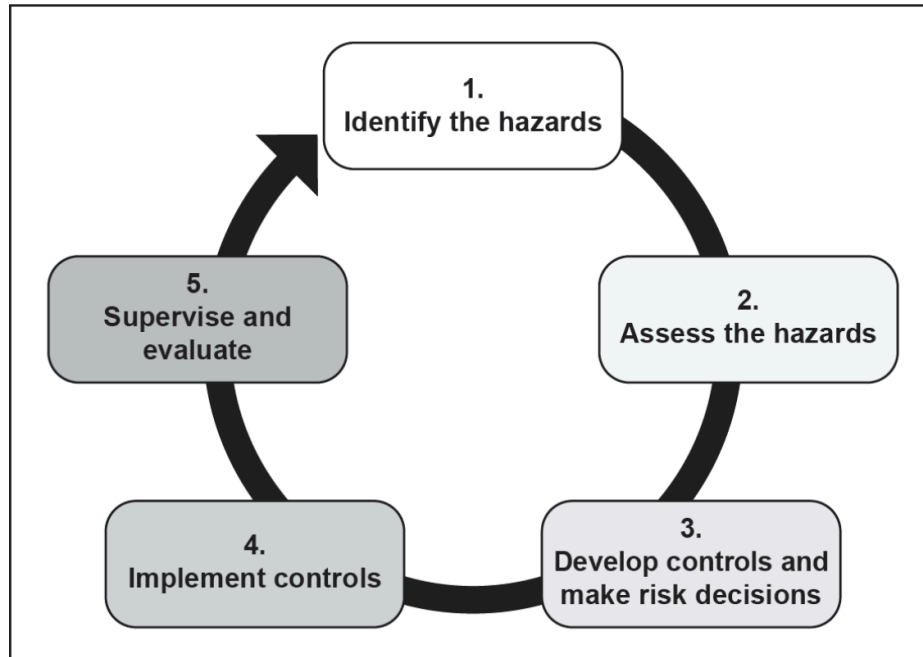


Fig. 4. Continuous Process of Managing Risk

3.5 Risk Assessment Matrix

US Army Risk Management process is used to evaluate the level of risks. These rules were developed utilizing the levels of risk described in the Army Risk Management process, Low, Moderate, High, and Extremely High. Each rule was calculated to reflect the risk level presented according to current Army regulations, doctrine, and policies.

Severity	Probability				
	Frequent	Likely	Occasional	Seldom	Unlikely
	A	B	C	D	E
Catastrophic	Extremely	High	High	Moderate	Moderate
Critical	High	High	Moderate	Moderate	Low
Moderate	High	Moderate	Moderate	Low	Low
Negligible	Moderate	Moderate	Low	Low	Low

Fig. 5. US Army Risk Assessment Matrix

4. METHODOLOGY

This study was based on a literature review, and it looked at the current risk

impact of the Defense White Paper established for future MAF, as a result of digital transformation in the aftermath of the COVID-19 pandemic. It was done to make sure MAF's strategic direction is still relevant in the post-pandemic, IR 4.0 and digital era. Interviews with similar military officials from related divisions were conducted to obtain a detailed picture of the division's important strategies, including risk management. Then, utilising the BMC framework, an initial MAF IERM Business Model was created, and later validated by interviewing relevant military officials from related divisions. The interviews were conducted to provide a clear scenario and understanding of MAF's essential strategies, identify risk factors, and recommend IERM business model options. This is to validate MAF IERM Business Model as a probable future model.

5. POSSIBLE FUTURE INTEGRATED ENTERPRISE RISK MANAGEMENT (IERM) MODEL FOR MALAYSIAN ARM FORCE

5.1 Establish an initial MAF IERM BMC

Business Model Canvas (BMC) is a relatively new paradigm to business modeling. The BMC framework is shown in Fig. 6. The nine blocks of BMC captures the business big picture and its logic (Osterwalder and Pigneur, 2010). There are numerous works on applying BMC to design and generate disruptive business strategies.

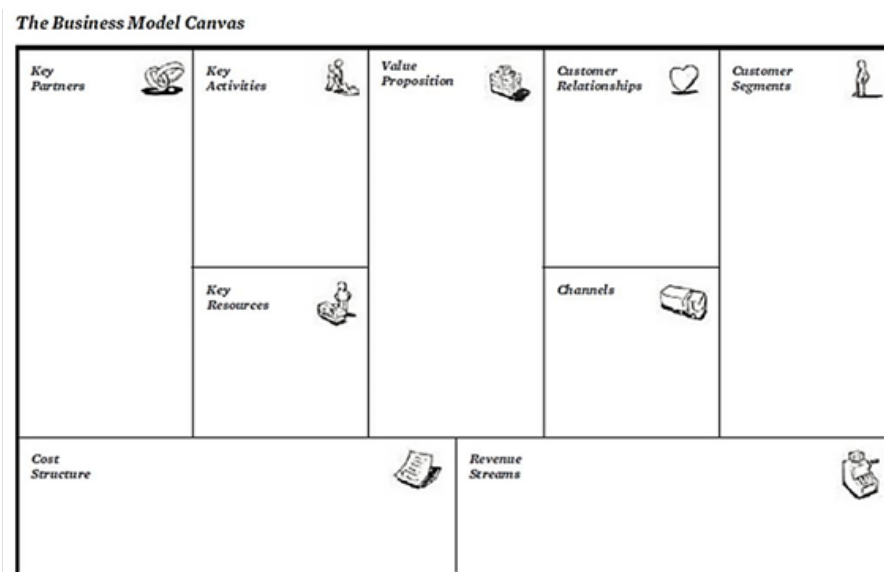


Fig. 6. Business Model Canvas by Osterwalder and Pigneur (2010)

In this conceptual paper, we explore the use of BMC as a tool to formulate and analyze, and establish the MAF IERM business model, relevant for digital transformation in the post pandemic COVID-19 era. The nine blocks of BMC capture the business big picture and its business logic. BMC allows for different approaches of doing business to be modelled in sufficient details, thus enabling us to design and test the business model before embarking on real-world implementation. Furthermore, BMC should enable us to understand how best MAF IERM business model to be formulated, analysed, prototyped, tested, and pivoted.

5.2 Validation process

We started by building BMC prototype based on our reading of the publicly available literatures. The focus was on examining current risk impact on Defence White Paper formulated for the future MAF due to digital transformation during post pandemic COVID-19. The prototype models were iteratively validated and fine-tuned by interviews with related military officers from related division to get a clear picture of its critical strategies including the risk management aspect.

5.3 Establish a possible MAF IERM BMC

The MAF may adopt or adapt the use of BMC to establish its Integrated Enterprise Risk Management (IERM), thus, facilitating the achievement of MAF's strategic goals and objectives. BMC identifies strategic risks, allowing for the mitigation of potential risks in the implementation of strategic plans. Fig. 7 depicts the MAF IERM Business Model, using the BMC framework. It is made up of 9 component blocks.

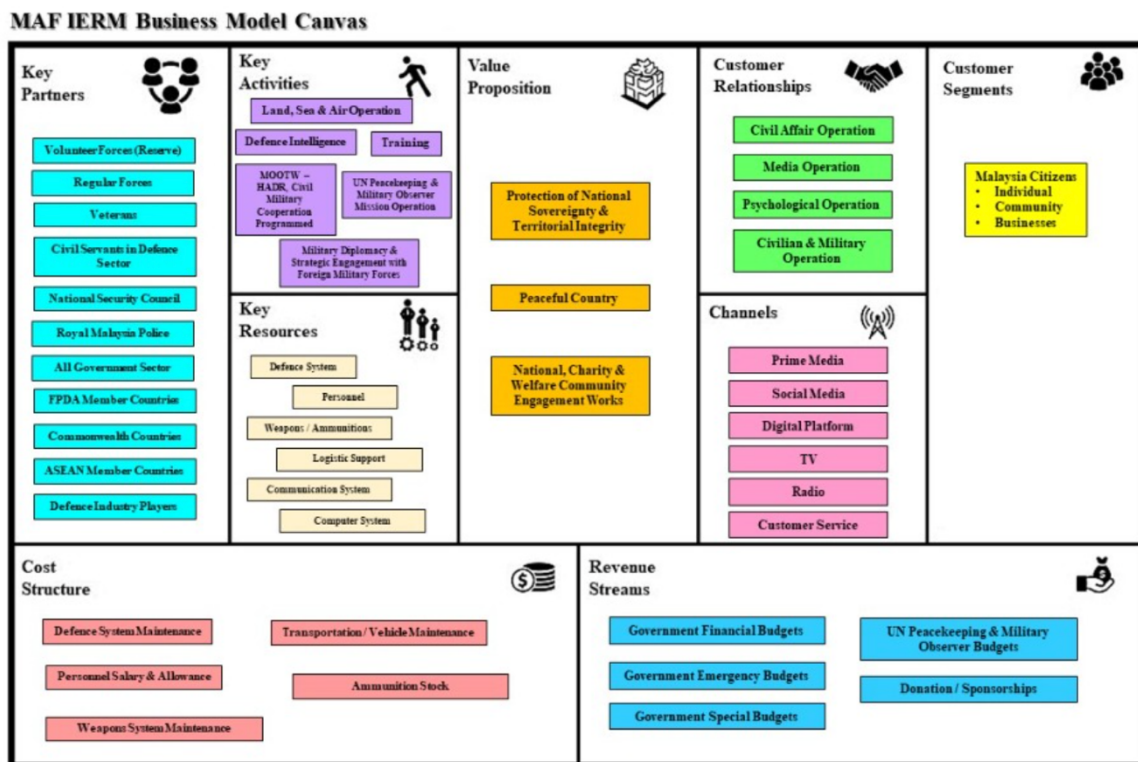


Fig. 7. The Use of BMC in mapping core success factors of MAF Strategic Direction Plan

5.3.1 Customer Segment

The Customer Segment (CS) in the MAF IERM business model is the Malaysian Citizens - Individual, Community, and Businesses. The purpose and objectives of the DWP are to embody the Government of Malaysia's aspiration in strengthening our national defence and formulating directions and strategic priorities for the nation's security. The key message in DWP is to achieve the Whole-of-Government and Whole-of-Society approaches that are central to national defence. National defence is a process requiring the active participation of

and by the people. The Government is committed to engaging the public on defence and other related matters. DWP offers an opportunity to reach out and inform the '*rakyat*', comprising of individual citizens, community, as well as all stakeholders including the business sectors, about the Government's present priorities and plans for bolstering Malaysia's defence.

Inactive participation from all the target audiences (Individuals, Communities, and Businesses) identifies as the risk to meet this objective. A few suggestions as mitigation action plans can be proposed. Firstly, MAF needs to specifically identify and systematically access the target audience. Each layer of society and different cultures place different priorities on specific needs. Secondly, to earn their support, it is necessary to understand their requirements as well as their sensitivities. MAF also can use Maslow's hierarchy of needs, as in Fig. 8, as an idea to attract and influence the target audience's emotions and their motivation (Maslow, 1943). Determining systematically their critical needs, short-term needs, and long-term needs may optimistically win their "hearts and minds". The effectiveness of these mitigation measures is highly dependent on the cooperation and compliance of all CS and members of society. The knowledge, attitudes, and practices people hold toward national security and well-being play an integral role in determining a society's readiness to accept behavioural change measures from authorities.

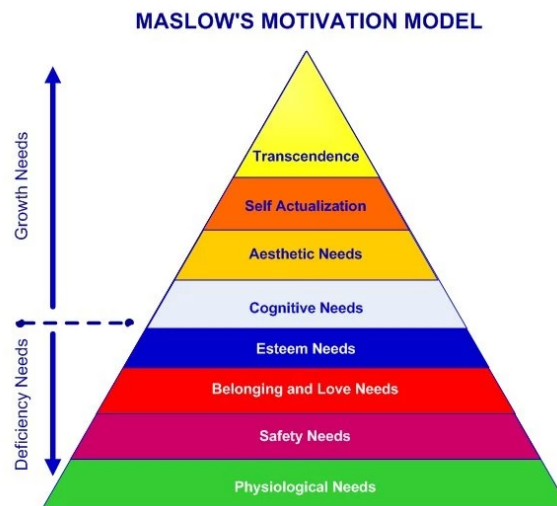


Fig. 8. Maslow's Hierarchy of Needs

5.3.2 Value Proposition

The Value Proposition (VP) is an important part of the MAF IERM business model towards achieving its strategic direction, goals, and objectives. The VP components in the MAF IERM BMC consist of the following:

- a. Protection of National Sovereignty & Territorial Integrity,
- b. Peaceful Country, and
- c. National, Charity & Welfare Community Engagement Works.

This VP remains a work in progress given the complexities inherent in measuring or describing defence's contribution to prosperity. The MAF, therefore, identified a need to develop a more coherent, complete and compelling

understanding of the totality of the 'Defence Value Proposition' to the Malaysians. The main risk in achieving this goal is a reputation that can lead to bad perspective that can tarnish the credibility and image of the MAF itself. The mitigation action plan to avoid this is by establishing a general inspectorate unit in each branch of the service. This unit is to ensure that every strategic plan is implemented. Another priority is any matters involving misconduct are investigated and appropriate action is taken. This VP can be achieved by maintaining personnel's moral and ethical integrity, sufficient logistic support and an appropriate training system.

5.3.3 Channel

Channel (CH) describes how the MAF communicate with and reach its Customer Segment in delivering the Value Proposition. The CH includes Prime Media, Social Media, Digital Platform, TV, Radio, and Customer Service. Due to post-pandemic COVID-19, mitigation is made by using new media such as social media and digital platforms to deliver the value proposition to Malaysian citizens. Enhancing the use of digital technology is critical in assuring the channel's effectiveness. It is critical to choose an appropriate theme to guarantee that the message reaches the Customer Segment.

5.3.4 Customer Relationships

Customer Relationship (CR) describes the type of relationships the MAF has with its various Customer Segment. The CR includes Civil Affair Operation, Media Operation, Psychological Operation, and Civilian & Military Operation. The current dynamics and conduct of armed conflict as well as the absence of effective mechanisms to mediate root causes of conflict and displacement have contributed to a global record high of people in need of protection, including displaced people. Relationship requires a strategic operational engagement, ensuring a protection continuum during flight and in situations where civilians are unable to move and seek safety. The MAF's involvement in Human Assistance and Disaster Relief (HADR), such as flood relief, is considered a Military Operation Other Than War (MOOTW) operation. It not only connects military troops with civilians, but also brings together corporate and private entities under one roof to achieve the same goal.

5.3.5 Revenue Streams

Revenue Streams (RS) describes the income and budget, benefits, outcomes, and impact generated for each of the Customer Segment. The Revenue Streams include Government Financial Budgets, Government Emergency Budgets, Government Special Budgets, UN Peacekeeping and Military Observer Budgets, and Donation and Sponsorship. Since the sources are from the taxpayers, political will and interference are required to secure the provision of Revenue Streams. Apart from the government's defence budget, which is dedicated to maintaining the welfare of military personnel and veterans, public donations and corporate sponsorship are another way for the government to cut its financial budget and so ensure the availability of Revenue Streams.

5.3.6 Key Resources

Key Resources (KR) describes the most important assets required to make MAF IERM business model work. The KR components include Defence System, Personal, Weapon and Ammunitions, Logistic Support, Communication System,

and Computer System. Strengthening the national defence industry and transferring technology through strategic partnerships with multinational defence businesses will improve local defence expertise and, in turn, assure the long-term availability of Key Resources.

5.3.7 Key Activities

Key Activities (KA) describes the most important course of action the MAF must do to make their IERM business model work. The Key Activities include:

- a. Land, Sea and Air Operation,
- b. Defence Intelligence,
- c. Training,
- d. MOOTW – HADR, Civil-Military Cooperation Programmed,
- e. UN Peacekeeping and Military Observer Mission Operation, and
- f. Military Diplomacy and Strategic Engagement with Foreign Military Forces.

Malaysia's Total Defence concept, launched in 1986, is a holistic approach that includes national vigilance, community solidarity, and unity in safeguarding national sovereignty and territorial integrity. With this idea of defence, the roles and responsibilities for protecting the country are not solely those of the military or other security organisations, but also include the entire population as a Customer Segment. This concept will be deemed an effective method of presenting the MAF's Value Proposition to people who are concerned about national security.

5.3.8 Key Partners

Key Partners (KP) describes the network and partners to optimize MAF IERM business model and to reduce risk or acquire resources. The KP include:

- a. Volunteer Forces (Reserve),
- b. Regular Forces,
- c. Veterans,
- d. Civil Servants in Defence Sector,
- e. National Security Council,
- f. Royal Malaysia Police,
- g. All Government Sector,
- h. FPDA Member Countries,
- i. ASEAN Member Countries, and
- j. Defence Industry Players.

These KPs are critical to the MAF's Value Proposition being realised and synergized. inter-agency collaboration, bilateral and multilateral international military diplomacy, and intelligence sharing are all vital components of the strategy for the country's ability to defend itself against any external threat. The veteran's duties are obviously synergistic, ensuring that the MAF's Value Propositions are met. As part of Customer Segment, they can completely employ their rich knowledge in diverse specialities while in service to bridge MAF with the public community.

5.3.9 Cost Structure

The Cost Structure describes all costs incurred to operate MAF IERM business model. The Cost Structure components include:

- a. Defence System Maintenance,
- b. Personal Salary & Allowance,
- c. Weapons System Maintenance,
- d. Transportation / Vehicle Maintenance, and
- e. Ammunition Stock.

The mitigation plan to ensure the synergy and cost-effectiveness of Cost Structure in delivering VPs to various CS is by making a cost-effective study based on the concept of five factors, namely TELOS (Technicality, Economical, Legal Operational and Security). All Cost Structures need to achieve minimum requirements and consideration based on TELOS factors to ensure the costs are synergy and cost-effective. Another mitigation plan that can be suggested is by ensuring all the Cost Structures have a proper Return of Investment (ROI) as a measurement in their strategic plan.

5. CONCLUSION

Risk management is defined in a different context based on threat perception. It is a systematic process of decision making to identify, mitigate and control potential risk to avoid or minimise undesirable impact. In the business or industrial sector, effective risk management can avoid losses. Also, it can maximise profit and at the same time minimise the unexpected problem. Practicing risk management process along with a good framework in accordance to the standard and clearly defined roles and responsibilities, prepares the company or organization to predict potential risk for future success. For the MAF, there are risks being mitigated and encountered rather than avoided for the national sovereignty and territorial integrity. The adaptation of BMC framework will help the MAF in formulating and developing an effective integrated risk management process; thus, enabling the achievement of its strategic goals, and objectives.

REFERENCES

- Busch, O. V. Reviewed by & Palmås, K. (2021). Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy, March 2021, Command Paper 403. by UK Cabinet Office, Design and Culture, 13(3), 361-366.
- Gearson, J., Berry, P., Devanny, J. & Musgrave, N. (2020). The Whole Force by Design: Optimising Defence to Meet Future CHallenges. London: Serco Institute.
- Institute of Standards and Technology. Gaithersburg. (n.d). MD: U.S. Dept. Of Commerce, National Institute of Standards and Technology. Retrieved from

https://www.armystudyguide.com/content/powerpoint/Safety_Presentations/risk-management-4.shtml

- Karels, C., McCormick, H., & Hodhod, R. (2015). Application of Fuzzy Expert Systems in Assessing Risk Management in The US Army: *International Journal of Computer Applications* 113 (6), 10-16
- Liang, T. N. (2018). The Fourth Industrial Revolution's Impact on Smaller Militaries: Boon or Bare?. Singapore: RSIS.
- Maslow, A. H. (1943). A theory of human motivation. *Psychological Review*, 50(4), 370–396.
- Ministry of Defence Malaysia. (2020). Defence White Paper.
- MS ISO 31000:2018 Risk Management – Principles and Guideline.
- OECD. (2017). OECD Digital Economy Outlook 2017. Paris: OECD Publishing
- Osterwalder, A. & Pigneur, Y. (2010). *Business Model Generations - A Handbook for Visionaries, Game Changers, and Challengers*. Hoboken, New Jersey: John Wiley & Sons, Inc.
- Srinivas, K. (2019). *Process of Risk Management*.
- Stoneburner, G., Goguen, A., Feringa, A., & NIST (U.S.). (2002). *Risk Management Guide For Information Technology Systems: Recommendations of The National*
- Tucci, L. (October, 2021). What is risk management and why is it important. Retrieved from <https://www.techtarget.com/searchsecurity/definition/What-is-risk-management-and-why-is-it-important>
- United Nations ESCAP. (2021). *Economic and Social Survey of Asia and the Pacific 2021: Towards post COVID 19 Resilient Economies*.
- Waidner, M. & Kasper, M. (2016). *Security in Industrie 4.0 - Challenges and Solutions for the Fourth Industrial Revolution*. 2016 Design, Automation & Test in Europe Conference & Exhibition. pp. 1303-1308.