Development of Risk Management Framework - Case Studies

Edly F. Ramly
Certification Director
EFR Certification Sdn Bhd, Malaysia
e.ramly@efrcertification

Mohd Soffian Osman
Senior Operation Manager,
Safety Management Academy Sdn Bhd, Malaysia
soffian@rafflesiagroup.com.my

Abstract

Action to address risk and opportunities is one of major requirements in Quality, Environmental and Occupational Health and Safety Management System (QMS) based on ISO9001:2015, ISO14001 and ISO45001:2018 standards. Each of organization that certified either to ISO9001:2015, ISO14001:2015 or ISO45001:2018 the organization shall embark the risk based thinking (RBT) in their organization. The objectives of this research are to determine issues in implementation of risk-based thinking (RBT) and recommended the applied RBT framework based on case studies in three organizations. The issues determine from the case studies included 1) To many and complicated RBT approaches; 2) Not integrated the RBT with strategic and operation; 3) Communication and awareness of RBT. Based on issues determined, each organization proposed several solutions to address the issues and the solutions are compiled as the effective RBT framework.

Keywords: Risk Assessment, Risk Management, Quality management system, Operation Management, ISO 9001:2015, ISO31000

1. Introduction

The latest revision of ISO9001 version 2015 which is the 5th edition of Quality Management System requirement include the principle of risk based thinking. The requirement include the action to address risk and opportunities. (ISO standard, 2015) . While Baldrige Business Excellence Framework 2017-2018 include the risk as part of "Focus on success" and "Managing for Innovation" to ensure the organization success now and in the future. However the ISO9001:2015As the standard does not explicitly indicated the used of specific tools or techniques for product or process risk assessment, the ISO 31000:2009 standard is intended to help organizations to embark the risk based thinking (Atan et al., 2017). Atan et al., (2017) indicated that ISO31000:2009 is a systematic and comprehensive manner diverse types of risk by offering a universal framework 'to assist the organization to integrate risk management into its overall management system. In 2018, ISO revised the guideline to clearly show the interrelation between risk management principle, risk management framework and risk management process (ISO, 2018). However, ISO does not include any example on how to adapt and implement the framework. Without clearly defined risk management, measurable tolerances the whole risk cycle and any risk framework is arguably at a halt (IRM, 2018). At the same time, several studies were conducted on risk management framework. Comprehensive literature review was conducted by Qazi et al. (2015). However the conceptual framework proposed was on supply chain management risk. Choo and Goh (2015), conducted study on adaptation of the ISO 31000:2009 enterprise risk management framework in a high-

tech organization using Six Sigma, Myšková and Doupalová (2015) study on approach to Risk Management Decision-Making in the Small Business and Atan et al (2017) study on operational risk as decision support tools. Most of risk management framework are used for decision support tools. Other common studies were conducted on specific industry such as supply chain (Heckmann, Comes, & Nickel, 2015; Wiengarten et al., 2016), and risk in operation (Reim et al., 2016). However there was limited study on development of risk management framework according to ISO9001:2015 requirements. This research intended to apply the ISO31000 to develop specific risk management framework to meet ISO9001:2015. At the same time, this research explores the issues and procedure in development of risk management framework and proposed the procedure to develop risk management framework.

2. Methodology

Dane (1990) asserts that it is through the action research that researchers are able to test the application against other research results. This way, researchers will be able to assist managers in deepening their understanding of the issue(s) in hands so that they can resolve the problem(s) confronting them. The major strategy for this research is action based case study, in order to explore the issues and develop the effective risk management framework. The steps in implementation of action research are depicted in figure 1. The case study protocol was developed to ensure consistency and reliability of the data collection process.

Process Flow	Process Description	Comments/ Remarks
Develop checklist and Semi Structure Protocol	Develop the case study -action based protocol	The protocol developed based on ISO9001:2015 and ISO31000 standard
Determine and invite the organization	Determine and invite the organization	Total 4 invitations and 3 organizations agreed to participate.
Conduct the action research	Conduct the action research	Apr 18- May 18
Disseminate results	Report the findings	Add memo to Atlas TI to organize and conduct cross case analysis to determine issues and development procedure arise from case study.
DIscussion	Discussion on procedure of development of "Risk Management Framework"	Improved and Refined risk management framework

Figure 1: Research Methodology - Action based case study

The case study protocol is developed through the standard of ISO 31000:2018 and ISO9001:2015. The principle, framework and process adopted from ISO31000 as shown in figure 2. The research adopted the sequential action

based case study according to the step proposed in ISO31001. The first steps of case study is to determine the organization context of organization, product or services and work process to produce/ deliver the product or services. The second phase is to determine the risk, risk analysis, risk evaluation and risk treatment. The final phase of research is to determine the issues and linkages between risk management process, framework and principles.

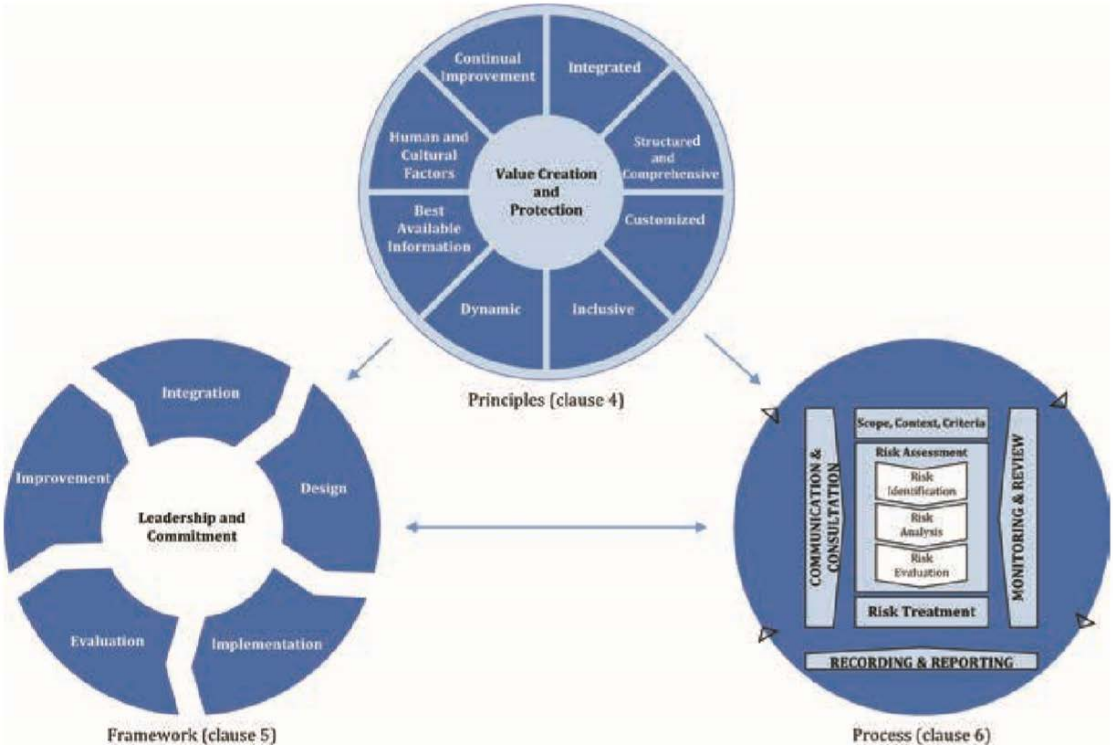

Figure 2: Relationships between the risk management principles, framework and process (ISO, 2018 pp. v)

3.0 Results

3.1 Profile of organizations

All organization participate in the action research are located in Malaysia and categorized under large organization from various types of industries, types of product and customer based. The organizations certified to ISO9001:2015 The organization details are shown in Table 1 (as part of non-disclosure agreement with the organization, the organization have been referred to as Case A to C).

Table 1: List of case organization

Case Organization	Type of product/ Services	Customer Based	Remarks
A	Services - Maintenance	Marine/ Oil and Gas	Local
B	Manufacturing - Electrical	Developers	Multinational
C	Hospital	Public	Private

3.2 Result from Case Study

The presentation of case study result is presented through cross case examination on each case to determine the inductive coding. Each case organization is going through case study protocol as followed:

- What is the current risk management framework,
- What are the issues on current risk management framework,
- What are the recommended solution to mitigate the issues on current risk management framework (Discussion).

The presentation of cross case examination and case study critical analysis is presented by each questions case study protocol. The use of cross case examination is used in order to sort out the existence and magnitude of similarity, causal effects of case study protocol.

3.2.1 Current risk management framework

All three case organizations current risk management framework and process have not aligned the three approaches according to ISO31000 guideline. Even though their approaches were not aligned with ISO31000 guideline, several elements are adopted in order to meet ISO9001:2015 requirement. Summary of organizations implementation of risk related the ISO9001:2015 requirements as shown in table 2.

Table 2: Organization approaches in implementing ISO9001:2015 risk requirements

Case Organization	Clause 4.1 Context of Organization	Clause 4.2 Interested Party	Clause 6.1 Action to address risk
A	Internal External Issues – Risk Register	Internal External Issues – Risk Register	Internal External Issues – Risk Register
B	COTO List	COTO List	Risk Register, Force field analysis
C	List in Quality Manual	List in Quality Manual	Risk Register

3.2.2 Issues on current risk management framework

To determine the issues on current risk management framework interview was conducted with organization management representatives. All the management representatives agreed that the issues included 1) To many and complicated RBT approaches; 2) Not integrated the RBT with strategic and operation; 3) Communication and awareness of RBT. Case A representatives indicated that the main challenge in risk management is to determine and describe the risk. She indicated that, there are too many risks to include in the risk register. While Case B representatives indicated the different trainers and consultant provide different method to develop the COTO list and Risk Register.

4.0 Discussions

All the organizations agreed that each organization shall have their risk management plan or risk management manual that described; 1) Scope and purposed of risk management framework, 2) Detail definition on the term used, 3) Detail steps that linking the context of organization to risk management process. Based on the six elements of risk management framework, the most important elements are designing, integration and implementation of risk management process. This section discusses detail description of common problems in design, integration and implementation of risk management framework.

4.1 Scope and purposed of risk management framework

Each of case organization determined the Context of Organization (COTO) in various method recommended by their consultant. However, when ask on what is the purpose and linkage of risk with COTO, each of organization was unable to explain. ISO31000:2018 provided detailed explanation in element 5.4.1 and 6.3 that the purpose COTO is to establish the scope, the context and criteria to customize the risk management. Hence COTO provide funneling process to determine the scope of risk management and determining the risk criteria as shown in figure 2.

Figure 2: COTO as funneling process

4.2 Detail definition on the term used

The most common confusion with the organization is defining issues and risk. Issues can be determined as risk and vice versa. Issue is referring to COTO as external/ internal environment in which the organization seeks to achieve its objectives. Issue normally act as key drivers or key result area and trends having impact on the objectives of the organization. Common category of issue used by the case organization can be according to four category of Balance Scorecard (BSC) which are: 1) Financial; 2) Customer; 3) Internal process effectiveness; 4) Learning and Growth.

The BSC category can be further derived the issues in term of objectives or key performance indicator. On the other side, risk is defined as "effect of uncertainty on objectives". An effect is a deviation from the expected can be positive and/or negative. The positive risk, commonly defined as opportunities. Objectives can have different aspects and categories i.e. BSC and can be applied at different levels.

Detail definition for commonly used term in risk management are described according to the steps of risk management process in next section.

4.3 Detail steps of risk management process

Each case organization recommended that each steps of risk management process shall be defined. At minimum the generic process shall be develop. After several round of discussion, the team agree that the risk management process flow as depicted in figure 3. The first and second steps have been discussed in earlier section. Next section discussed the step three to seven and proposed the effective risk management framework.

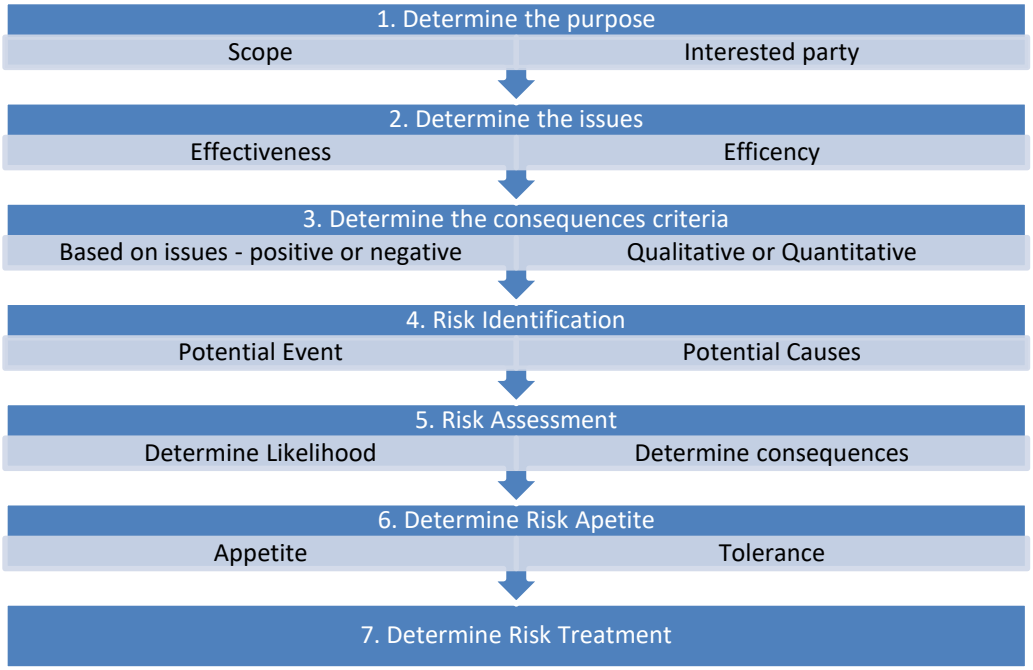

Figure 3: Recommended risk management process

4.3.1 Determine the consequences criteria

ISO31000:2018 does not provide the specific guideline on how to determine the consequences risk criteria. However, based on case studies, the consequences risk criteria can be determined through issues that have been determine in step 2. For example, the organization have determined organization reputation as main issues as part of financial or customer category under BSC, the consequences risk criteria can be determined either for positive or negative impacts. The detail description is required to support risk assessment either through qualitative or quantitative method. At minimum, the qualitative description shall be developed for Low and High, or Low Medium and High. All the case organization utilized the quantitative description through score 1-5. Each of score has the description on level of consequences or impact.

4.3.2 Risk Identification

The organization should consider using ISO31000 version 2009 for detail definition of risk. According to ISO31000:2009, risk description should be in terms of risk sources, potential events, their consequences and their likelihood. Risk source element which alone or in combination that potential to give rise to risk that may include the event and potential causes. Potential cause of risk is defined as how the risk could occur and should be described in terms of something that can be corrected or can be controlled. The organization should list, to the extent possible, every cause assignable to each of the risk. The causes should be described so that risk treatment can be aimed at those causes which are pertinent.

Each of case organization utilized different method to describe the risk. Case A organization have already separated the description of risk, risk causes and impacts. Case B organization only provide the single column to described the risk. However, this method may have potential missed out to described the potential cause of risk. While case C organization separated the risk description and risk causes.

4.3.3 Risk Assessment

The main purpose of risk assessment is to determine whether the risk level is acceptable according to risk appetite. Risk level commonly determine through combination of consequences and likelihood. The consequence is an outcome of an event that affecting objectives and consequence can be certain or uncertain and can have positive or negative direct or indirect effects on objectives. At the same time, consequences can be expressed qualitatively or quantitatively. Any consequence can escalate through cascading and cumulative effects. Finally, the term likelihood is defined as chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period). Hence, the likelihood will always refer to risk events/ potential event.

Based on case organizations, three methods were observed which are; 1) risk matrix, 2) risk priority number (RPN), and/or 3) force field analysis,. Risk matrix methodology can combine either qualitative or quantitative. The risk matrix utilized by case A and C organization. The risk matrix used by case A, utilized 5 x 5 matrix in which the likelihood used letter A to E and consequences used number 1 to 5. The risk level will determined by letter and number i.e. A1 trivial risk while E5 is the highest significant risk. While for case C organization, the organization utilized matrix that already multiply the score of consequences and likelihood which the lowest risk level is 1 and the highest is 25. This method quite similar with RPN method risk priority number. The different is the organization does not have the risk table of risk matrix. The risk matrix table example as shown in figure 4. The force field method only used by case B for the purpose of decision making in investment. The scoring of risk level used the formula sum of score in positive risk and minus sum of score of negative risk to determine the risk level.

Likelihood/ Severity	1	2	3	4	5
A	A1	A2	A3	A4	A5
B	B1	B2	B3	B4	B5
C	C1	C2	C3	C4	C5
D	D1	D2	D3	D4	D5
E	E1	E2	E3	E4	E5

Likelihood/ Severity	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

Figure 4: Example of risk matrix

4.3.4 Risk Appetite

Both ISO31000 standard version 2009 and 2018 does not provide any definition of risk appetite. At the same time, risk appetite will always mean different things to different people, a properly communicated, appropriate risk appetite definition and statement can actively help organizations achieve goals. Institute of risk management (IRM-UK) defined risk appetite as the amount of risk that one is prepared to accept, tolerate, or be exposed to at any point in time" (IRM, 2018).

Based on case studies, only case C organization defined the risk appetite since the organization is part of public listed group. While risk appetite is about the pursuit of risk, case C organization also add in risk tolerance is about what an organisation can actually cope with. Case B organization used the risk priority number (RPN) threshold as the risk tolerance and all risk that are more than 15 of RPN required improvement action and in between 5 to 14 to have a least monitoring of risk (at minimum through internal audit). The case A organization, used the same method of with case B organization but only determine in risk matrix through color. All the organization does not develop the risk appetite and risk tolerance for positive risk (opportunities).

4.3.5 Risk Treatment

ISO31000 version 2009 defined the risk treatment as process to modify risk. However the definition of risk treatment have been deleted and replace with risk control in ISO31000 version 2018. Risk control defined as measure that maintains and/or modifies risk. Controls include, but are not limited to, any process, policy, device, practice, or other conditions and/or actions which maintain and/or modify risk. The modify risk is consider residual risk. Residual risk is a risk that remains after all efforts have been made to mitigate or eliminate risks. After a risk assessment, a residual risk may be known but not completely controllable, or, it may not be known. In addition, ISO31000 (2009) recommend that risk treatment can involve 1) Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk; 2) taking or increasing risk in order to pursue an opportunity; 3) removing the risk source; 4) changing the likelihood; 5) changing the consequences; 6) sharing the risk with another party or parties (including contracts and risk financing); and 7) retaining the risk by informed decision. Risk treatments that deal with negative consequences are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention" and "risk reduction". All the case organizations did not determine the method to determine the risk treatment. Hence the method to determine risk treatment is recommended for future research.

4.4 Proposed Risk Management Framework

The ISO31000:2018 framework have been simplified by grouping the framework elements. The first element remains the same which is leadership and commitment. The second element combined the risk management process with design and integration of risk management process. The final element is combination of implementation, evaluation and improvement. The overall framework is shown in figure 5.

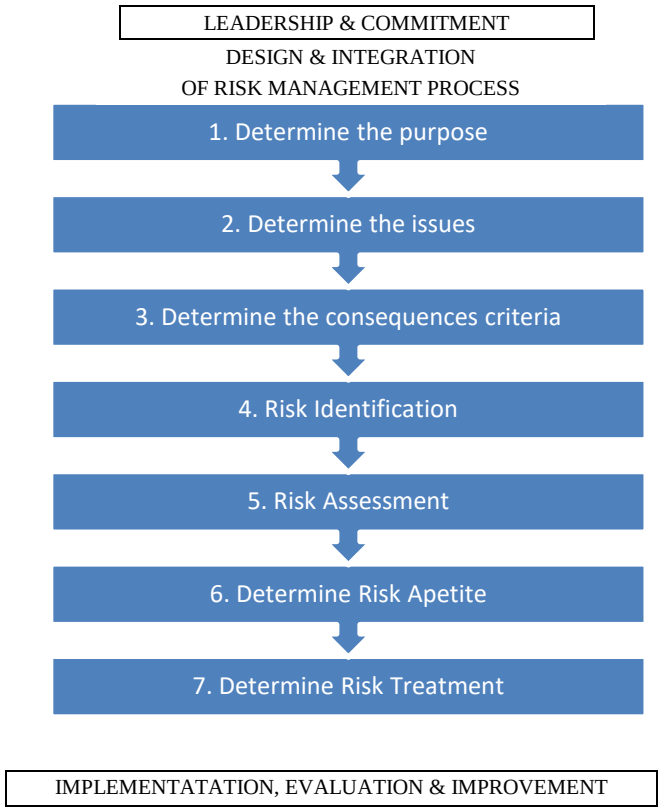

Figure 5: Improved Risk Management Framework

5.0 CONCLUSION AND FUTURE FOCUS

Both version of ISO31000 2009 and 2018 version have been developed, review and tested in case organizations. However, there are several issues that potentially face by the organizations that implement several management system such as ISO9001:2015, ISO14001:2015 and ISO45001:2018. The ISO31000 risk management framework have been refined and improved that include detail steps in risk management process. This will enables organization design, integration and implementation of risk management framework effectively.

The future research should focus on linking the framework with other risk process such as PFMEA and HIRAC. More case study is required on different context of organization, different industry and sector, difference business process and difference size of organization.

References

Atan, H., Ramly, E. F., Mohammad, M., & Yahya, M. S. (2017). A review of operational risk management decision support tool. *Proceedings of the International Conference on Industrial Engineering and Operations Management, Morrocco*.

Baldrige Performance Excellence Program. (2017). *2017–2018 Criteria for Performance Excellence*. Gaithersburg, MD: U.S. Department of Commerce, National Institute of Standards and Technology. http://www.nist.gov/baldrige.

Dane, Francis C. 1990. 120 *Research Methods*. Brooks/Cole Publishing Company Pacific Grove, CA.

Dunkle, David C. 2005. "Prioritizing Human Interface Design Issues for Range Safety Systems Using Human Factors Process FMEA." In *NASA Risk Management Conference*.

Heckmann, I., Comes, T., & Nickel, S. (2015). A critical review on supply chain risk – Definition and Measure. *Omega*, *52*, 119–132. https://doi.org/10.1016/j.omega.2014.10.004

International Organization for Standardization (ISO). (2015). *Quality management systems – Requirements* (5th ed.). (ISO9001:2015).

International Organization for Standardization (ISO). (2009). *Risk Management - Principles and Guidelines.*

International Organization for Standardization (ISO). (2018). *Risk Management - Guidelines.*

https://www.theirm.org/knowledge-and-resources/thought-leadership/risk-appetite-and-tolerance/

Qazi, A., Quigley, J., & Dickson, A. (2015). Supply Chain Risk Management : Systematic literature review and a conceptual framework for capturing interdependencies between risks. *Proceedings of the 2015 International Conference on Industrial Engineering and Operations Management.* Dubai, United Arab Emirates (UAE), March 3 – 5, 2015

Reim, W., Parida, V., & Sjödin, D. R. (2016). Risk management for product-service system operation. *International Journal of Operations & Production Management*, *36*(6), 665–686. https://doi.org/10.1108/IJOPM-10-2014-0498

Wiengarten, F., Humphreys, P., Gimenez, C., & Mcivor, R. (2016). Risk , risk management practices , and the success of supply chain integration. *International Journal of Production Economics*, *171*, 361–370. https://doi.org/10.1016/j.ijpe.2015.03.020

Biography

Edly F. Ramly is an Certification Director for EFR Certification. He is renowned coach, auditor, consultant and trainer. With his excellent technical expert and interpersonal skills, he has conducted various high impact trainings and workshop in the area of operation management, industrial engineering, management system including quality, environment and occupational health and safety, workplace improvement, variation and waste reduction, and practical problem solving techniques including statistical tools. Apart from being trained as Lead Auditor in various management system, he is also qualified auditor for Automotive Industry ISO/TS 16949. During his service with Pera Neville Clarke, he is also tutor for QMS lead auditor course. His industrial experience was in the automotive industry. During his stayed with the TRW Automotive, he was tasked with the responsibility of promoting and implementing Lean and Six-Sigma within the Organization. Due to his extensive exposure in Lean and Six-Sigma Management System, he was invited by Malaysia Productivity Corporation (MPC) and Asia Productivity Organization (APO) to conduct public training in the area of Six-Sigma implementation and Lean Implementation. In 2014, he been awarded as one of Malaysia Productivity Specialist by Malaysia Ministry of International Trade and Industry.

Mohd Soffian graduated from Universiti Malaysia Sabah (UMS) in Bachelor of Food Science & Nutrition with Honors. At the same time, he also holds an Executive Diploma in Occupational Safety & Health. He is a certified trainer and assessor by various agencies such as Ministry of Health Malaysia, Human Resource Development Fund Malaysia, American Heart Association, Rescue Medical International, Vocational Education & Training Australia, Australian Institute of Management & other related agencies in the field of occupational health & safety, food hygiene & safety and human development. He is also a certified lead auditor by IRCA & RABQSA for various management systems such as food safety, quality, environment and occupational health & safety. His research on hypertension has been chosen as one of the best undergraduate research & being awarded the NSM Undergraduate Award by Nutrition Society Malaysia in year 2005. He has more than 13 years of experience, with locally and internationally exposure.