

# Pragmatic adaptation of the ISO 31000:2009 enterprise risk management framework in a high-tech organization using Six Sigma

Bennie Seck-Yong Choo

*Cummins Inc., Singapore, Singapore, and*

Jenson Chong-Leng Goh

*School of Business, SIM University, Singapore, Singapore*

## Abstract

**Purpose** – This case study aims to present a viable solution to how organizations can adapt and customize the ISO 31000:2009 enterprise risk management framework to suits its needs and requirements.

**Design/methodology/approach** – Approach used for this case study is via adopting Six Sigma DMAIC (Define, Measure, Analyze, Improve and Control phases) methodology.

**Findings** – Key finding is the importance of stakeholders' feedbacks which are taken into consideration during the designing of the new customized enterprise risk management framework, integrated with all supporting processes, tools and resources.

**Originality/value** – The ISO 31000:2009 enterprise risk management framework dictates that it is not a one-size-fits-all. Rather, organizations who wish to adapt this framework need to customize accordingly, but there is no indication on how organizations can do it. This case study presents a viable solution to this challenge.

**Keywords** Six Sigma, DMAIC, Risk management, ISO 31000:2009 enterprise risk management framework

**Paper type** Case study

## 1. Introduction

In recent times, the inadequate management of enterprise risk management (ERM) practices by Toyota (Shechterle, 2010) and General Motors (Slezak, 2014) had resulted in several high-profile recalls of their vehicles. These events demonstrate the importance and challenges in developing and maintaining effective ERM practices in an organization. In today's global business environment, an organization is constantly facing heightened volatility from globalization, deregulations and increased competitions. This volatility has increased an organization's exposure to risks. A failure to proactively identify, assess, mitigate, report and monitor these risks may result in significant damage to an organization's reputation and revenues (Gorzen-Mitka, 2013; Hogan and Lodhia, 2011).

The traditional approach that many organizations take in risk management is a reactive one and does not take into consideration the dynamics of changes in its business



environment (Gorzen-Mitka, 2013). It often emphasizes on detecting and mitigating risks rather than preventing the occurrences of risk. Many organizations' risks, especially multi-national corporations, are also managed in a silo manner, where an individual business unit focuses on its own risks and the risks that cut across the entire organization are largely left unattended. Therefore, there is a growing need for an organization to take on ERM effectively to hold risks in check and protect itself from the volatility of its environment (Gorzen-Mitka, 2013).

The ISO 31000:2009 ERM framework was developed by a group of international technical experts to address the challenge of a lack of frameworks and principles in the area of ERM. The framework provides a conceptual approach to develop comprehensive ERM practices in an organization (Gjerdrum and Salen, 2010). Practitioners were expected to "adapt and not adopt" the ISO 31000:2009 ERM framework according to their organizations' risk management needs (Frigo and Anderson, 2014). However, the ISO 31000:2009 ERM framework has been criticized as being overly abstract and is confusing in many of its terms and definitions in ERM by both practitioners and researchers (Gorzen-Mitka, 2013; Leitch, 2010). The industry's drive toward ERM is also being "viewed as a still developing process" (Frigo and Anderson, 2014). This makes adaptation of the ISO 31000:2009 ERM framework a challenge for most organizations.

In this case study, we attempt to present a possible solution to this challenge. We will demonstrate how the Six Sigma DMAIC (Define, Measure, Analyze, Improve and Control) approach is being used to help a business unit of a large high-tech organization adapt the ISO 31000:2009 ERM framework successfully. We believe our paper will answer to the call by practitioners and researchers to shed more insights into the ways to enact effective ERM practices in an organization (Frigo and Anderson, 2014; Knight, 2010). We also believe our approach, while will require some forms of contextualization, can serve readily as a guide for practitioners when adapting the ISO 31000:2009 ERM framework into their organizations. We think this is of significant contribution to both the researcher's and practitioner's world.

## 2. Case background

The case organization that we had selected is a Fortune 500 company, headquartered in the USA. The organization was founded in 1919 and pioneered the development of diesel engines and promoted diesel fuel as a reliable source of power. The organization has a global presence in more than 190 countries and territories. As at end of 2013, the organization has around 48,000 employees employed at its various worldwide entities and has an annual revenue of around US\$17 billion. Today, the organization is a recognized market leader in the diesel engine industry. The organization develops, designs, manufactures and services engines and related technologies in six continents.

Due to the large cultural changes that are required in an organization during an ERM initiative, the literature recommends to first start an ERM initiative within a business unit before proliferating it to the rest of the organization (Frigo and Anderson, 2014). Therefore, one of the business units within this organization is selected to apply our Six Sigma DMAIC approach to ERM.

The selected business unit within this organization is the distribution arm of the organization. The business unit drives a comprehensive global distribution strategy and channel management through more than 120 global distributors, as shown in Figure 1. Through this extensive distribution network, well-trained personnel sell and

distribute the organization’s products, related services and customer-tailored solutions such as maintenance contracts, engineering services and customized integrated products to its valued customers. Capitalizing on its synergies in products and services, the business unit constantly provides outstanding worldwide customer and product technical support to all its valued customers. In 2013, the business unit achieved an annual revenue of US\$3.7 billion, which was 20 per cent of the organization’s total annual revenue. Market volatility due to globalization and heightened competition have increased the business unit’s exposure to risks. A failure by the business unit to effectively address and mitigate these risks would lead to an adverse impact to the organization’s revenue and reputation (Hogan and Lodhia, 2011). Therefore, we think that this business unit should be at the forefront in the implementation of ERM within the organization.

The business unit has started to reflect on the importance of ERM as part of its business continuity strategy to address the volatility in its business competitive environment. The senior management of the business unit believes that ERM is an extremely important endeavor to safeguard the business unit’s continual profitability and reputation (Hogan and Lodhia, 2011). The senior management wants to take the opportunity to raise the risk awareness level across the business unit comprehensively to assess on their risk exposure more effectively.

3. Literature review

ISO 31000:2009 ERM framework was developed by The International Organization on Standardization (ISO) in 2009, as illustrated in the document found here ([www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en](http://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en)) and noted as Figure 1.

ISO 31000:2009 ERM framework sets out the principles, a framework and a process for the management of enterprise risk that is applicable to any type of organization. It does not mandate a one-size-fits-all approach but rather emphasizes that ERM must be tailored to each particular organization’s specific needs and structure (Muzzy, 2008; Knight, 2010). However, while the ISO 31000:2009 ERM framework provides good directions on how to enact effective ERM practices, there are some challenges within the framework (Leitch, 2010).

First, the diagrams presented in the ISO 31000:2009 ERM framework are confusing. The diagrams, Principles (Clause 3), Framework (Clause 4) and Process (Clause 5), feature a number of boxes and arrows, but there is no explanation on what those boxes and arrows represent, making it impossible to deduce their meaning (Gorzen-Mitka, 2013). Second, the ISO 31000:2009 ERM framework is generic to all organizations (Frigo

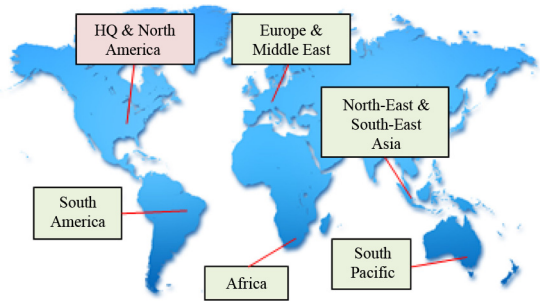


Figure 1.  
Regional offices of  
the business unit

and Anderson, 2011), as noted under Clause 3, Principle (b), which states that risk management is an integral part of organizational processes. It does not shed light on how organizations can adapt it to suit their specific requirements incorporated into their business model (Leitch, 2010), as noted under Clause 3, Principle (g), which states that ERM must be tailored to an organization. Without a clear understanding on how organizations can customize the ISO 31000:2009 ERM framework to suit their specific requirements, the drive to implement effective ERM practices within organizations is hindered (Leitch, 2010). This is a missed opportunity because, as advocated above, ERM is becoming an essential and important endeavor for an organization in today's volatility business environment.

In our view, the key to a pragmatic and rigorous adaptation of the ISO 31000:2009 for ERM into an organization lies in its implementation methodology (Purdy, 2010). The methodology must not only be a rigorous one, but somewhat pragmatic to implement. Hence, we undertook an effort to compare and contrast the advantages and disadvantages of several commonly used implementation methodologies, as shown in Table I, before concluding on the use of Six Sigma.

Justified by Clause 3, Principle (h) and (k) in the ISO 31000:2009 ERM framework, we concluded that the Six Sigma DMAIC approach is a more ideal methodology for

Process improvement tool	Key advantage	Key disadvantage
Plan-Do-Act-Check	The method emphasizes on continuously assessing the process of enterprise risk management and gaps and lapses in the process can readily be identified systematically and can be corrected early	The method is often oversimplified and does not take into consideration the voices from the customers. This is particularly not ideal for enterprise risk management implementation, as such implementation often requires the buy-ins of all key stakeholders
Kaizen	The method is centered in addressing what needs to be changed with the process of enterprise risk management so that gaps and lapses do not reoccur	The method requires the entire organization and all its members to be constantly on a lookout for potential areas that can be improved. It is often a bottom-up approach with support from senior management. Ideal when a proven enterprise risk management methodology is already in place
Six Sigma DMAIC	The method is customer-driven (as it emphasizes the use of voices from business and customers to identify risk management needs). The method aimed to drive out "defects" (in relation to risk management) by an iterative process of controlling the variation of the enterprise risk management process	The method requires specialized skills in the area of statistical analysis. The method may be viewed as more top-down but with inputs from the grounds

**Table I.**  
Key advantage and disadvantage of commonly applied process improvement tools

organizations to adopt in customizing the framework than the other two, namely, Plan-Do-Act-Check and Kaizen.

This case study attempts to fill these gaps as highlighted in the literature by applying the Six Sigma DMAIC approach on the ISO 31000:2009 ERM framework's adaptation process in the business unit. The method will have an emphasis in taking both human and cultural factors into consideration during the ISO 31000:9009 ERM customization process. It will also strive to reduce the variation in the business unit's current business process to achieve excellence in integrating risk management as an integral part of the business unit's organizational processes.

#### **4. Six Sigma DMAIC process**

##### *4.1 Define phase*

Risk management is defined as the identification, assessment and prioritization of risks, followed by coordinated and economical application of resources to minimize, monitor and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities. The underlying principles of risk management allow every entity, whether for-profit or not, to realize its true value for its stakeholders and the value is created, preserved or eroded by management decisions in all activities, from setting strategy to operating the enterprise day-to-day. Risk management supports value creation by enabling management to deal effectively with potential future events that create uncertainty and respond in a manner that reduces the likelihood of downside outcomes and increases the upside.

The selected business unit's intent is to improve on its current management capability through establishing a comprehensive and integrated risk management program framework, with supporting processes and tools. The business unit believes that by doing so, they are able to improve on the business unit's image to its internal and external stakeholders.

This case study would entail working with a dedicated team, consisting of the business unit worldwide entities and functional leaders, and corporate's ERM group to review on the business unit's current risk assessment processes and tools, identify best practices for integration into a comprehensive and integrated ERM framework for the selected business unit.

Based on a number of interviews with the senior management of the selected business unit within the organization, we have noted that the development of effective ERM practices has been highlighted as one of the key business unit's critical projects that is aligned with the overall organization's strategy. Therefore, we took this opportunity to solicit the business unit's senior management support to allow us to adapt the ISO 31000:2009 ERM framework across its business unit. Their approvals were obtained and we proceeded to the next phase of the Six Sigma approach.

##### *4.2 Measure phase*

To understand the complexity in developing an effective risk management framework, it is essential to first determine the effectiveness of the current risk assessment practices in the selected business unit. We carried out a process mapping exercise to develop the AS-IS process map[1] of the selected business unit's existing risk management practices. A total of 48 key business stakeholders in the selected business unit were chosen to

participate in a comprehensive survey to uncover the existing gaps in the business unit's current risk management practices. This is an important process, as it addresses the need to take both the human and cultural factors into consideration when establishing the ISO 31000:2009 ERM framework. These gaps form the "Voices of the Business" in the measure phase. The profiles of the 48 key business stakeholders are shown in [Table II](#).

The four key existing gaps in the business unit's current risk management practices are:

- (1) *No resource*: There is no available risk management tool which had been developed to conduct effective risk assessment for the business unit's respective entity and/or function so as to determine its risk profile. Moreover, there is no dedicated person assigned to take ownership for risk management within the business unit.
- (2) *Non-structured framework*: Current risk assessment framework which is adopted by the business unit is not from any known industry well-accepted risk management model and is loosely connected between all stakeholders, in particular between internal audit, finance and management. Moreover, there is no clear authority and accountability.
- (3) *Internal audit*: Current risk management practiced by the business unit takes on a silo approach, as only internal audit is involved in assessing each entity and/or function risk profile, particularly with matters concerning business finances only.
- (4) *Once a year*: Current risk management practiced by the business unit takes on a reactive standpoint, as risk profiling is only conducted when an unfortunate event occurred which caused a negative impact on the business revenue and/or company image.

Moreover, review on the business unit risk profile is only conducted once per year and it is usually conducted at the end of each work year. Thus, the business unit might not be

Classification of stakeholders' job position	Representation (%)
Senior management	31
Mid-senior management	33
Middle management	36
<i>Regions where stakeholders are located at</i>	
North America	35
South America	10
Europe and Middle East	15
Northeast and Southeast Asia	30
South Pacific	10
<i>Business profile which stakeholders belongs to</i>	
Corporate-level functional groups	45
Regional - and local-level business entities	55

**Table II.**  
Key stakeholders'  
profiles

able to react effectively to its ever-changing business risk profile. See Pareto chart of current state of risk management practices of business unit in [Figure 2](#).

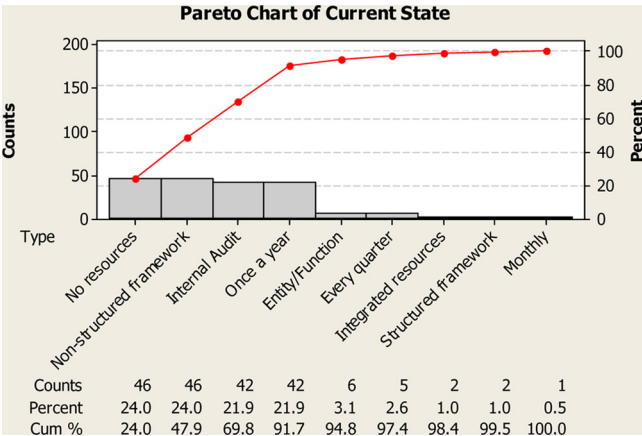
From the assessment conducted on the business unit's current risk assessment practice, we concluded that it is neither comprehensive in structure nor integrated with supporting processes, tools and resources. As a result, the business unit might be constantly challenged and exposed to substantial risks due to its adoption of a silo approach in assessing its risk profile and taking on a reactive standpoint in terms of its manner and frequency in conducting its risk assessment. Hence, there is a need for the business unit to establish a comprehensive risk management framework that integrates all necessary processes, resources and tools to better improve on its risk management capabilities.

4.3 Analyze phase

To uncover what are the critical factors in the development of an ERM framework for the business unit, a survey was conducted to obtain qualitative feedback from the identified 48 business stakeholders. We have applied the Kawashita Jiro (KJ) analysis[2] on this feedback to systematically organize the feedback collected according to a set of themes. The objective of the KJ analysis is to determine those critical factors from the stakeholders' provided inputs to be taken into consideration when developing the proposed risk management framework for the business unit.

We find the KJ analysis particularly useful in our situation because:

- the issues that surround a problem (i.e. ERM) are large and complex;
- the information relevant to the problem appears in unorganized thoughts and ideas within the business unit's stakeholders;
- a breakthrough from the traditional ways of implementing risk management is needed;
- team consensus is essential to ensure the success of the initiative; and
- data are in a non-numeric form, which renders numeric or statistical techniques useless.



**Figure 2.**  
Pareto chart of  
current risk  
management  
practices in unit

Our analysis revealed four critical factors and they are:

- (1) *Infrastructure*: The need to have a well-structured infrastructure that ensures the effectiveness in risk management by having the right systems, processes and tools to ensure effective and efficient risk management.
- (2) *Resources*: The need to have a team of capable cross-functional employees who can serve in various risk management roles to help the business unit realize its risk management vision and project goal.
- (3) *Management commitment*: The need to have risk management as a part of, and not separate from, the business unit work practices and processes, and embedded into the entity and/or function's strategic plan and goal objectives.
- (4) *Governance*: The need to have a set of control measures and policies to ensure continuity and effectiveness of risk management practices across all the business unit's entities and functions.

The four factors form the requirements for the improvement phase and they are summarized in [Figure 3](#).

#### 4.4 Improve phase

In the improve phase, we considered that the proposed risk management framework must be able to allow the business unit to manage those risks that could have a negative impact on its ability to achieve its organizational objectives. This will allow the business unit to make well-informed, risk-aware decisions that are aligned to its overall business and operational strategy. Therefore, the proposed risk management framework must be dynamic, iterative and responsive to changes and explicitly address uncertainties. It should also be able to protect the business unit's ability to accelerate its global business values and enable growth. As such, the proposed risk management framework must be promoted throughout the business unit to create awareness on the nature and consequences of risky behavior and how to avoid them. Through this effort, everyone within the business unit at every level will be encouraged to discuss risks openly and take ownership and responsibility for managing it. Last but not least, the proposed risk management framework must be in sync with evolving legal and regulatory compliance development.

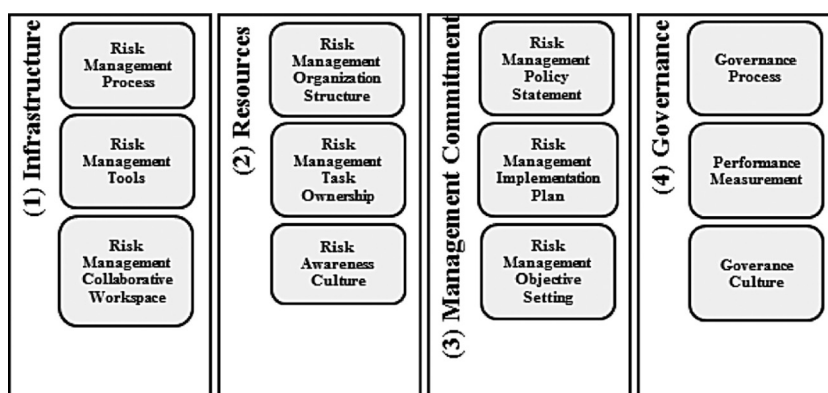


Figure 3.  
Requirements from  
Kawashita Jiro (KJ)  
analysis[3]

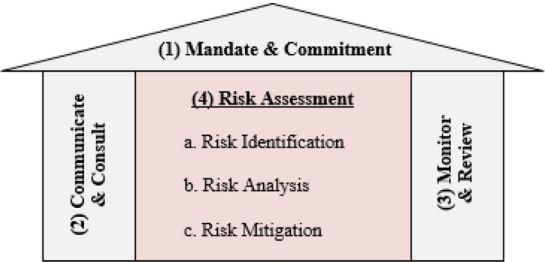
The development criteria for the proposed risk management framework involves reviewing on the current risk management models that range from informal qualitative models to sophisticated quantitative models, depending on the need and culture of the organization. Therefore, one size does not fit all. Moreover, a critical consideration is that the proposed risk management model must include processes to identify, assess, mitigate, report, monitor and communicate identified critical risks which might be and/or affecting the business unit, establishes people roles and responsibilities, and system requirements to facilitate communication flow.

As such, we customized the ISO 31000:2009 risk management framework according to the data collected in the measure and analyze phases, as shown in [Figure 4](#).

The collected stakeholders' views were then translated into KJ Images[4] and aligned accordingly to each of the structural blocks of the customized framework. Some examples are shown in [Table III](#). This is done to identify the recommended actions needed to effectively integrate the customized framework into the business unit's management control system. The importance of each structural block is:

- *Mandate and commitment*: The mandate and commitment structural block ensures that a strong and sustained commitment by all levels of management, particularly the senior management team, is essential to ensure the successful introduction and implementation of a risk management process and to ensure its sustainable effectiveness.
- *Communicate and consult*: The communicate and consult structural block ensures that effective communication and consultation is essential to those accountable for implementing the risk management process and all key stakeholders understand the basis on which decisions are made, and the reasons why particular actions are taken.
- *Monitor and review*: The monitor and review structural block ensures that ongoing monitoring and review is paramount to ensure that risk management process remains to be effective and up-to-date.
- *Risk assessment*: The risk assessment structural block is the fundamental building block in establishing a clearly developed risk management framework through a comprehensive process which involves risk identification, risk analysis and risk mitigation.

A solution design session with the project core team was conducted to identify the recommended action plan for each of the structural blocks in the new customized risk management framework. The recommended action plan is closely aligned to the



**Figure 4.**  
Customized risk  
management  
framework

		ISO 31000:2009 enterprise risk management	
<hr/>			
<i>Mandate and commitment</i>			
KJ Image	Embedded into the business unit's work practices and processes	<hr/> <b>373</b> <hr/>	
Stakeholders' views	Senior leaders to takes ownership and responsibility on risk management activities Senior leaders to set the tone on the level of risk management activities within the business unit		
<i>Communicate and consult</i>			
KJ Image	A risk awareness culture across all levels within the business unit		
Stakeholders' views	Risk assessment and reporting should form part of management report To create a common collaborative workspace for risk information sharing		
<i>Monitor and review</i>			
KJ Image	A set of control measures to ensure continuity and effectiveness		
Stakeholders' views	To establish a centralized monitoring system on all identified risks and its current status To set the rules of the game clearly and upfront through policies and procedures		
<i>Risk assessment</i>			
KJ Image	Develop understanding of the risk for better decision-making	<b>Table III.</b> Alignment of stakeholders' feedbacks	
Stakeholders' views	To establish a toolkit that is user-friendly and non-complicated for actual applications Each business entity and functional group to establish its own risk appetite and tolerance		

received stakeholders' feedbacks which had identified the critical gaps for improvement actions. The recommended action plan was presented to the senior management for approval. The approved recommended action plan for each of the structural blocks of the new customized risk management framework is as shown in [Table IV](#).

Various ideas from the project core team which were based from the received stakeholders' feedbacks were consolidated in the development of the new customized risk management framework's tools and resources. A total of ten templates and media platform were eventually consolidated into a comprehensive risk management tool kit. For each structural block of the new customized risk management framework, appropriate tools are developed and assigned respectively (see [Table V](#) for details on the name and application of each tool).

Risk assessment is the fundamental building block in addressing those risk events which may impair the success of the business unit. It comprises a comprehensive process which includes risk identification, risk analysis and risk mitigation. The corresponding risk assessment tool that was developed by the core project team for the business unit's business entities and functions is shown in [Figure 5](#).

In the risk identification stage, it is important that a comprehensive identification of all potential risks is conducted and not overlooked. A risk that is not positively identified at this stage will not be included in later analysis and that might result in dire consequences. Some of the risks, which are crucial to the business unit, identified by the

**Table IV.**  
Recommended  
actions

Structural block	Action plan
Mandate and commitment	Creates a leadership statement that establishes the risk management mandate Establishes a reporting structure and allocates appropriate resources accordingly Communicates risk management benefits to all stakeholders Risk management objectives are aligned with organization's and business unit's strategic goals Leadership team to takes ownership on risk management activities
Communicate and consult	Creates communication mechanisms between all stakeholders Establishes Wiki page for collaboration through social media platforms
Monitor and review	Treats as a living document as new methods and tools to manage risks are developed Embeds in managerial activity and guards against superficial approach Establishes regular capability checks through risk compliance readiness review
Risk assessment	Creates a toolkit and allocates appropriate tools accordingly Creates a roadmap to be taken for each identified risk indicator rating

**Table V.**  
Risk management  
toolkit

Tool no.	Tool name	Tool explanation
A	Risk catalog	Potential areas of risk within the organization
B	Risk prioritization scale	Quantitative method to assign likelihood and impact ratings to the associated risks
C	Risk indicator scale	The level of risk present, taking into account the impact and likelihood of the risk event
D	Risk map	Graphical representation on where risks stood in terms of its likelihood and impact
E	Risk assessment template	A comprehensive tool to facilitate the identification, analysis and mitigation of risks
F	Risk project update template	Monthly updates on risk-specific project progress
G	Risk compliance readiness template	Measures risk management performance against key indicators
H	Global risk register	Inventory of all identified risks within the organization
I	Wiki page	Collaborative workspace to share and store information
J	Risk governance structure	Employees with defined roles and responsibilities to govern the organization's risk management programs

project core team are strategic risks, technology risks, financial risks, human resources risks, legal/compliance risks and operational risks.

In the risk analysis stage, we seek to ensure the development of an understanding of the causes of each identified risk that is identified in the risk identification stage. This also includes their positive and negative consequences, and the likelihood that those

Entity / Functional Risk Assessment					Review Date
Entity Information					
Entity / Function				Risk Owner	
Location Address				Region	
Risk Identification					
Risk Description				Risk Category Please Select	
Risk Consequence				Others	
Risk Analysis				Risk Map	
Current State		Previous State		Target	
Impact	Please Select	Impact	Please Select	Impact	Please Select
Likelihood	Please Select	Likelihood	Please Select	Likelihood	Please Select
Direction	Please Select	Direction	Please Select	Risk Indicator	★VALUE!
Velocity	Please Select	Velocity	Please Select	Select the Star Marker on the left and paste it on the Risk Map on the right to reflect the Current State of Risk Level of the identified risk.	
Risk Indicator	★VALUE!	Risk Indicator	★VALUE!		
Key Risk Drivers					
Risk Evaluation					
Risk Level				Please Select	Evaluation Date
Treatment Required				Please Select	Evaluation By
Risk Treatment					
Treatment Type				Please Select	Due Date
Effectiveness				Please Select	Ownership

Figure 5.  
Risk assessment  
template

consequences might occur. Figure 6 shows a recommended roadmap which the business unit can undertake for each identified risk indicator rating that is developed by the project core team.

Finally, in the risk mitigation stage, risks are prioritized accordingly for the appropriate actions to be taken, depending on the business unit's risk appetite. There are a total of four commonly applied risk mitigation options as recommended by the project core team. The four common risk mitigation options include:

- (1) *Avoidance*: Exiting from the activity that gives rise to the risk.
- (2) *Transfer*: Transferring the risk to another entity and/or function.
- (3) *Acceptance*: Accepts the risk by doing nothing.
- (4) *Treatment*: Treat the risk to an acceptable level which is based on the business unit's risk appetite at that point of time.

#### 4.5 Control phase

As part of the control phase, it is essential that the requirements from KJ analysis and the recommended improvement action plan be documented. A monthly periodic review was also instituted in this phase. The purpose is to review if the proposed initiative is progressing as planned, and if there is a need for any further improvement to be made to address any new or changing landscape that the business unit is operating in. A Wiki page as shown in Figure 7 was created, which serves as a collaborative workspace to encourage all employees at different levels of the business to discuss risks openly without any fear of punishment. The business unit's risk management program has been treated as a living document which is periodically reviewed for new updates and latest developments from the industry's best practices. A control plan was then


Figure 6.  
Roadmap for each  
identified risk  
indicator rating

Risk Indicator	Suggested Actions	Suggested Timing	Attention by for Continued Toleration of Risk Indicator
81	Where the risk indicator score is not as low as reasonably possible, take action to reduce the level of risk to 27	Short-term, normally within 1 month	Leadership Team
27	Take action to reduce the level of risk to less than 27 or receive authority to continue	Medium-term, normally within 3 months	Global Risk Management Steering Committee
9	Take action to reduce the level of risk to less than 9 or receive authority to continue	Normally within 6 months	Global Risk Leader
3	Tolerable risk, with lower priority unless circumstances change, but still require attention within business	Ongoing control as part of a management system	Entity / Functional Leader
1	Tolerable risk, with lower priority unless circumstances change, but still require attention within business	Ongoing control as part of a management system	Entity / Functional Leader

Overview  Restricted  
Tags: [compliance](#), [risk](#)

**Forums**

[Start a Topic](#)




**Input Solicitation for the Proposed DBU Risk Management framework (due September 15, 2013)**

Last post by [Wesley E Wheeldon](#) | Sep 16, 2013 | replies (2)

[View All](#)

**Bookmarks**




Share Web resources with your community.

[Add Your First Bookmark](#)

**Files**


[Share Files](#)



**Comprehensive Risk Management.pdf**

Shared by [Thiru Sethuraman](#) on August 29, 2013 | 6 downloads


☆ 0



**Choosing the Right Risk Management Framework.pdf**

Shared by [Thiru Sethuraman](#) on August 29, 2013

☆ 0



**A Road Map to Risk Management.pdf**

Shared by [Thiru Sethuraman](#) on August 29, 2013 | 2 downloads

☆ 0

Figure 7.  
Wiki page as  
collaborative  
workspace

developed to ensure the continual capability of the business unit’s risk management program and also to assist in tracking and correcting the performance of the new customized risk management framework, with process owners identified for each of the process steps involved.

5. Lessons learnt

In general, this case study shows the importance of implementing a comprehensive and effective ERM within an organization. Given the volatile business environments and the complex business processes, organizations are facing difficulties that limit them from identifying, assessing, mitigating, reviewing and monitoring those risks that might

result in an adverse effect on the organization's financial performance and reputation (Byrnes *et al.*, 2012). As a result, the organization's ability to implement an ERM program in an effective manner becomes particularly significant for the reason that it allows the organizations to be more aware, reduces uncertainty and, most importantly, to make more accurate decisions, which lowers the organization's risk exposure (Kaiser, 2005).

This case study also demonstrated that despite the emergence of the ISO 31000:2009 ERM framework, many organizations today still struggle to get the framework to be implemented as its core business process. As the ISO is not a one-size-fits-all framework, organizations need to adapt and customize accordingly to suit their own respective organization's needs and requirements (Knight, 2010). The challenge today is how organizations can customize the ISO 31000:2009 ERM framework? This case study posited that the Six Sigma DMAIC methodology can provide a possible solution to this challenge.

This case study presents how the use and application of Six Sigma DMAIC methodology may allow the ISO 31000:2009 ERM framework to be effectively adapted into a business unit of a large global organization by:

- taking stakeholders' feedbacks in consideration during the designing and customizing of the ERM framework;
- custom-fit the proposed solutions according to the stakeholders' feedbacks without compromising on the rigors of adapting comprehensive and effective ERM practices; and
- developing a risk awareness culture through proper process design and integrating appropriate tools and resources into the new customized ERM framework.

In this case study, a comprehensive list of ERM tools which are aligned with the received stakeholders' feedbacks into each structural block of the new customized ERM framework is developed. Refer to Table VI for the alignment of each of the assigned tools to each guideline and principle which are customized from stakeholders' feedbacks, and the structural blocks of the new customized ERM framework.

Six Sigma DMAIC methodology is a powerful methodology that, we believe, can help an organization first establish a sound and effective risk management process within a business unit and then subsequently extend it across the entire organization. The

No.	Structural block	Guidelines and principles (customized from stakeholders' feedbacks)	Assigned tools
1	Mandate and commitment	Embeds into the business unit's work processes and practices	Tool J
2	Communicate and consult	Creates a risk awareness culture across all levels within the business unit	Tools E and F and Tools H-J
3	Monitor and review	Establishes a set of control measures to ensure continuity and effectiveness	Tools E-H
4	Risk assessment	Develop an understanding of the risk for better decision-making	Tools A-F

**Table VI.**  
Customized risk  
management  
framework

process variation control techniques in Six Sigma are highly iterative in nature and provide a basis where a pragmatic adaptation approach of the ISO 31000:2009 framework can be achieved. In our case, we have shown how the use of Six Sigma allows a business unit of an organization to adapt and develop an effective and customized risk management framework that took contextual information into consideration. Refer to [Table VII](#) for the effectiveness of the customized framework in mitigating the existing challenges that are present in the standard ISO 31000:2009 ERM framework.

Our study focuses only on a business unit within a large high-tech organization. For the risk management practices to be proliferated to the entire organization, we propose two proliferation strategies that are based on our existing Six Sigma approach, as shown in [Table VIII](#).

In this case study, Option 2 was selected and implemented by the organization, as each of its business unit shares similar operating environment, customers and business needs and requirements. The implementation of the customized ISO 31000:2009 ERM framework had enabled the senior management team to deal effectively on any future uncertainties in support of its annual growth strategy. This is evident in the quarterly growth in revenue of the organization since the implementation of the ERM practices (from Quarter 4, 2013 to Quarter 4, 2014), as shown in [Figure 8](#).

Business stakeholders play a critical role in the implementation of any ERM project ([Frigo and Anderson, 2014](#)). Because the development of the new customized ERM framework in this case study is driven from the feedbacks that are received from key business stakeholders, this case study has demonstrated that the Six Sigma DMAIC methodology can be a viable and effective approach to solicit strong buy-ins from them, especially from the senior management. With the clarification of the ERM processes, the implementation of appropriate ERM tools and resources and the strong support received from the senior management of the business unit, this case study reflects the positive strong ability to establish the necessary risk awareness culture across all levels within the business unit. The new customized ERM framework has also enabled the business unit to:

- proactively address its risks and opportunities and create value for both its internal and external stakeholders;

**Table VII.**  
Mitigation of existing  
challenges

No.	Standard ISO 31000:2009 framework	Customized ISO 31000:2009 framework	Variation addressed (Y/N)
1	Confusing diagrams, with no explanation on what those boxes and arrows mean	Simple in-house-designed framework which can be easily understood by all	Y
2	Generic to all organizations and requires customization to suit its own needs and requirements	Voice of the business is conducted to take human and cultural factors into consideration during the adaptation process	Y
3	It does not shed light on how organization can adapt and incorporate the standard as an integral business process	Our Six Sigma DMAIC methodology provides a pragmatic approach on how to integrate risk management practices into a business unit and eventually proliferate it across the organization	Y

No.	Proliferation strategies	Ideal business context consideration	Issues
1	Replicate the same Six Sigma approach to customize risk management practices one business unit at a time	This strategy is ideal when the business units within an organization function very different from each other. For example, in a conglomerate business, the business environment, customers and requirements would be very different across its business units. The result may be each business unit will have vastly different risk management practices from each other	Nonetheless, where appropriate, the implementing business unit can take several shortcuts to reduce the implementation efforts. For example, they can consider what has been already uncovered within the first business unit and then determine if it is also applicable to them. Some form of consolidations of risk management practices can also be done at enterprise level once all the business units have successfully adapted and implemented their risk management framework, especially if there are some common risk components. Because of the bottom-up nature of this approach, the risk management practices are likely going to be very pragmatic, customized and relevant to each business unit's operating environment
2	Using what has been developed within the first business unit as starting point, the organization can form a cross-business units' team to develop an enterprise-wide risk management framework that will be adopted across the entire organization	This is a highly effective approach when the organization's business units share largely similar customers, needs and requirements and operate in the same business environment. For example, in our case organization, the core business is diesel engine that is shared across all business units and hence this technique is highly suitable for it	This is more of a top-down approach. However, supported with successful implementation within a business unit, an organization should be able to readily convince the rest of the business units to follow what has been uncovered. The lessons learned in one business unit can also be readily shared to leapfrog the process of creating an enterprise risk management approach that all business units can conform to. Furthermore, the tools developed within one business unit are generic enough for it to be easily adapted for use at enterprise level

**Table VIII.**  
Proliferation  
strategies

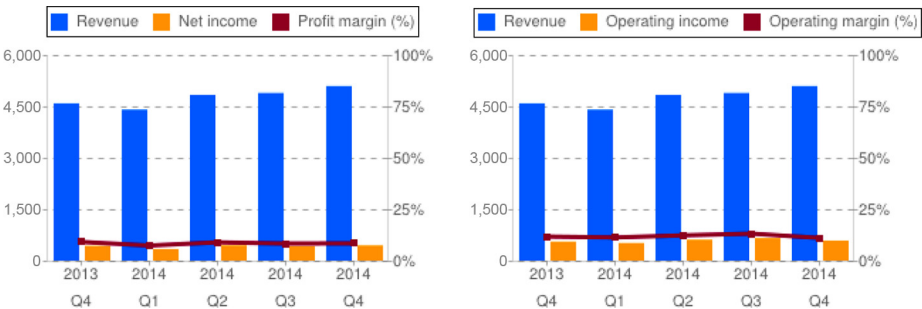
- analyze the business unit’s strategic, operational and functional risks effectively that the business unit might be exposed to in today’s volatile business environments that the business unit is operating in globally; and
- ensure the necessary compliance with all the applicable laws and regulations that the business unit is operating in worldwide (Khanin and Mahto, 2012).

The successful implementation of the new customized ERM framework for this business unit in a large global organization presents to the practitioners’ world that the framework can serve as a viable roadmap on how to adapt ISO 31000:2009 ERM according to an organization’s risk management needs and requirements through adopting the Six Sigma DMAIC methodology. Hence, we believe our paper can provide significant contributions to the practitioners’ world.

However, some of the key limitations of our case study are as follows:

- The initial efforts in engaging the business stakeholders are fundamental in the adaptation process. This is a step that we do not think can be removed. While the approach is expected to be high in efforts at the start of the process as a large number of key stakeholders’ feedbacks are required to be gathered to identify the human and cultural factors that affect ERM, we believe that this process step is a one-off event. The efforts invested in this area can be readily “reused”, as the organization adopts one of our “proliferation” strategies to develop its ERM framework.
- Organizations who wish to adopt the Six Sigma DMAIC methodology in designing their customized ERM framework will likely have very different risk management requirements, especially during the measure and analyze phases. While the risk management requirements may be different, the Six Sigma DMAIC methodology still remains to be a highly viable and rigorous approach for organizations who wish to customize their own ERM framework. The appropriate tools and resources which are developed in this case study for each of the structural blocks of the business unit’s new customized risk management framework can be readily replicated and reused by any organizations who wish to adapt the ISO 31000:2009 ERM framework.
- The organizations needs to be able to correctly identify the most appropriate proliferation strategies, as illustrated in Table VII, so as to ensure an effective and sustainable integration of the customized risk management framework across the entire organization. The organization needs to recognize that further

**Figure 8.**  
Quarterly financial  
results of the  
organization



customization might be required when replicating to other business units within the organization, as each could have variations in their business profiles, needs and requirements. The organization should not force fit any customized ERM framework which works well in a particular business unit into other business units by assuming that as it works well for one, it should also work well for the others too.

## 6. Conclusion

By implementing an effective and comprehensive risk management program; with all supporting processes, tools and resources, the business unit is able identify, assess and prioritize all its identified risks. Then, it is followed by coordinated and economical application of necessary resources to minimize, monitor and control the probability and/or impact of unfortunate events or to maximize the realization of the business unit's business opportunities.

The underlying principles of adapting an effective and comprehensive risk management program allow the business unit to realize its true value to both its internal and external stakeholders. And, the value is created, preserved or eroded by the business unit's senior management decisions in all activities, from setting its annual business growth strategy to operating the business unit's various worldwide entities and functions day-to-day.

Risk management supports value creation by enabling the business unit's senior management team to deal effectively with any potential future events that may create uncertainty for the business unit and to respond in a manner that reduces the likelihood of the downside and increases the upside of the business unit's financial performance and reputational image.

In today's dynamic business environment, adapting an effective and comprehensive risk management program will also enable the business unit to minimize on its risk exposure to any adverse financial performance and business result. Therefore, risk management involves every employee within the business unit, across all different levels, entities and functions.

## Notes

1. AS-IS process map is the current state of the process in the organization.
2. Kawashita Jiro (KJ) analysis is a project management tool that allows large number of qualitative ideas from brainstorming sessions to be collected and sorted into a set of themes. The themes can then be reviewed and analyzed for similar patterns. Efforts can be directed at each identified theme that is relevant and highly salient in accordance to the topic of interest, in this case enterprise risk management.
3. Requirements from Kawashita Jiro (KJ) analysis is the functionality in answering to each of the theme questions of the current process being reviewed.
4. KJ Image seeks to document and distill powerful qualitative voices describing the existing gaps which are present in the current process being reviewed.

## References

- Byrnes, S.E., Williams, C., Kamat, S. and Gopalakrishnan, S. (2012), "Making the case for an enterprise risk management program", *Journal of Equipment Lease Financing*, Vol. 30 No. 2, pp. 1-10.

- Frigo, M.L. and Anderson, R.J. (2011), "Strategic risk management: a foundation for improving enterprise risk management and governance", *The Journal of Corporate Accounting & Finance*, Vol. 22 No. 3, pp. 81-88.
- Frigo, M.L. and Anderson, R.J. (2014), "Risk management frameworks: adapt, don't adopt", *Strategic Finance*, Vol. 96 No. 1, pp. 47-52.
- Gjerdrum, D. and Salen, W.L. (2010), "The new ERM gold standard: ISO 31000:2009", *Professional Safety*, Vol. 55 No. 8, pp. 43-44.
- Gorzen-Mitka, I. (2013), "Risk management as challenge to today's enterprises", *Problems of Management in the 21st Century*, Vol. 22 No. 1, pp. 4-5.
- Hogan, J. and Lodhia, S. (2011), "Sustainability reporting and reputation risk management: an Australian case study", *International Journal of Accounting and Information Management*, Vol. 19 No. 3, pp. 267-287.
- Kaiser, M. (2005), "Comprehensive risk management", *Chain Store Age*, Vol. 81 No. 9, pp. 2-4.
- Khanin, D. and Mahto, R.V. (2012), "Regulatory risk borderline legality, fraud and financial restatement", *International Journal of Accounting and Information Management*, Vol. 20 No. 4, pp. 377-394.
- Knight, K.W. (2010), "AS/NZS ISO 31000:2009 – the new standard for managing risk", *Keeping Good Companies*, Vol. 62 No. 2, pp. 68-89.
- Leitch, M. (2010), "ISO 31000:2009 – the new international standard on risk management", *Risk Analysis*, Vol. 30 No. 6, pp. 997-992.
- Muzzy, L. (2008), "Approaching enterprise risk management", *Financial Executive*, Vol. 24 No. 8, pp. 59-61.
- Purdy, G. (2010), "ISO 31000:2009 – setting a new standard for risk management", *Risk Analysis*, Vol. 30 No. 6, pp. 881-886.
- Shecterle, R. (2010), "Toyota supply chain lacked risk management oversight", available at: <http://atrisk.net/toyota-supply-chain-lacked-risk-management-oversight/> (accessed 15 December 2014).
- Slezak, S. (2014), "GM's risk management failures provide lessons for other firms", available at: <http://globalriskinsights.com/2014/03/26/gms-risk-management-failures-provide-example-for-other-firms/> (accessed 15 December 2014).

#### **Corresponding author**

Bennie Seck-Yong Choo can be contacted at: [bennie.choo@cummins.com](mailto:bennie.choo@cummins.com)

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.