# New approach to Risk & Crisis Management – Business, Financial, and Information Security

Mr. Danny Ha, Vice President – M&R (Hon.) of ICRM, FCRP, CRT, CISA, CISM, CISSP, CFE(c)
Dr. Freddie Lee, Chairman of the Institute of Crisis and Risk Management (ICRM)


居安思危，作爲卓越的管理人員，應該要警覺到將來可能發生的威脅或危機，作好準備去预防和面對。風險管理透過既定的程序，評估每個決策所帶來的影响，針討性地執行相應的行動和措施。[六西格瑪]是一個幫助企業實現質量目標的嚴格的過程，一種基於資料的決策方法，致力於不斷改善產品及服務，目的是提高質量，降低成本，使顧客滿意，減低風險及提高市場競爭力。本文將揉合［六西格瑪］的基礎，處理财務及資訊風險，讓管理人員了解風險管理的行動和措施。

## Introduction

In 21st century globalization content, there are known or unknown risks or crises that could cause immeasurable damage to an organization. Business executives must understand and develop the right strategies to mitigate possible risks and crises. This paper is designed to give an insight to crisis and risk management and its relevance to Six-Sigma, business, information security management and financial risk management.

## What is Quality?

Quality is one of the many aspects the survival and prospering of business. Continuous quality improvement enables a firm to reduce cost, increase productivity and market share, and ultimately benefit the society through job creation.

Some of the factors influencing the operation of a business are the business ethics, people quality and product/service quality. Regarding to the business ethics, organization required basically compliance with the law. An organization needs initiatives that is driven from within and guided by customer-focused quality and thus the customer satisfaction. As the people quality concern, individuals must be motivated to comply with highest ethical standards by a desire to do the right thing rather than by fear of sanctions. We should focus on people quality and how to reconcile the need to maintain a high product quality/service and the product/service deployment strategies.

In 21st century, long-term success of a business should be identified with the ability to maintain highly predictable outcome. We shall use a continuous improvements and lifelong learning approach to tackle the five issues of Technology, Financial, Management, Organization, and Business from now to 2010.

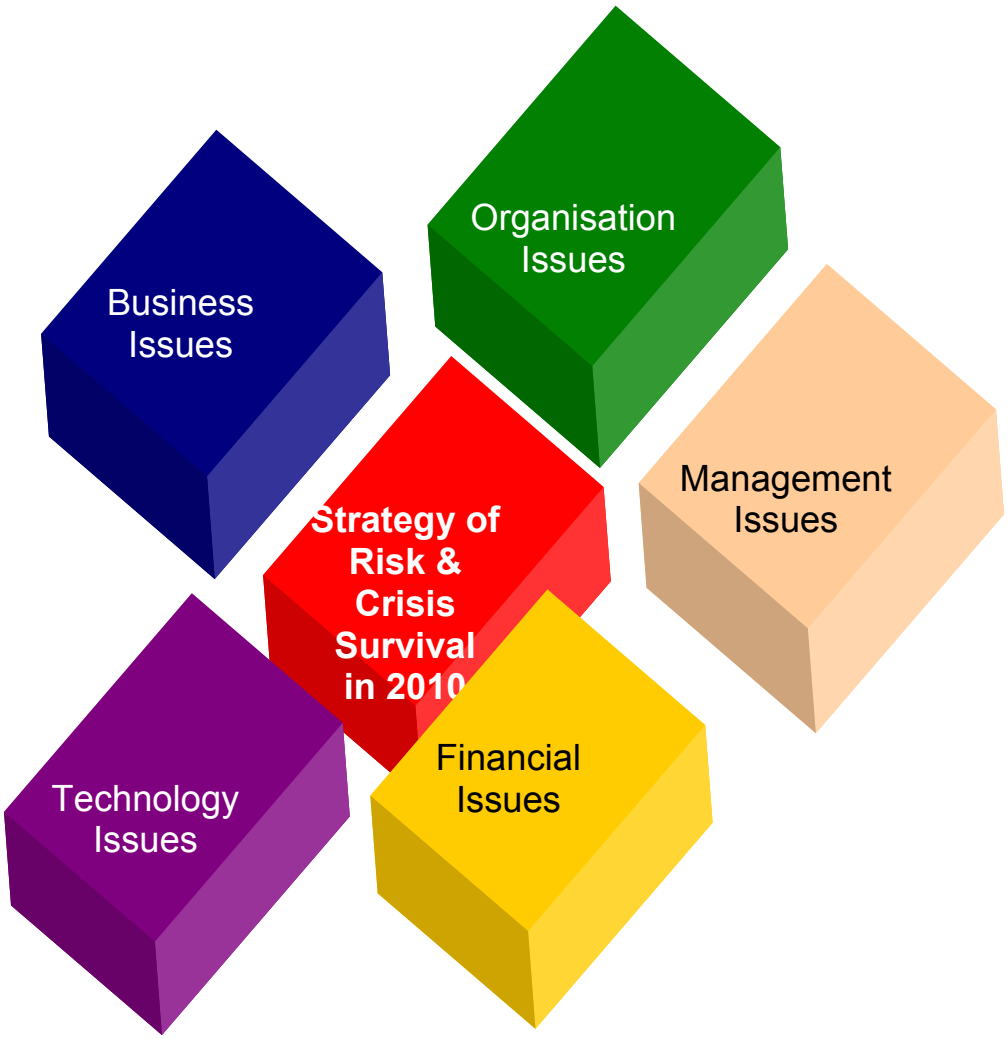


***Figure-1: Five critical business framework in 21st century***

## What is Standard?

There are a number of standards such as BS, UL, ISO, and Sigma. The quality management of ISO9000, BS5750 and EN29000 are some of popular standards. ISO9000 requirements prompted many organizations to create documented data collection procedures. However, these standards describe various items to be included in quality system, but it is quite difficult for an organization to integrate the different methodologies into the practical implementation. To be consistently profitable, the business must know how well its operations are running, what the major issues, risks or problem areas are, and which process variations need to be streamlined. We need a performance measurement system that can relate the operation performance to the financials. In practices, the organizations running the ISO and other systems mentioned-above may need to map their procedures to Six-Sigma context.

Six-Sigma is a fact-based or data-driven methodology. Decisions are made based on the data or rate of improvement. The data are collected during the project life, instead of

under normal operations conditions. Six-Sigma is a disciplined methodology for continuous improvement, applicable to manufacturing, service sectors, and retail industry which aims at keeping quality standard predictably high.

It should be noted at the Figure below, the cross-point of Cure-A and the vertical line of 'Critical Customer Requirement' is for 'Cost and Benefit Analysis (CBA)'. This is the main goal of Six-Sigma for which the real improvements are reflected in the improved overall bottom-line financial numbers through continuous process improvements.

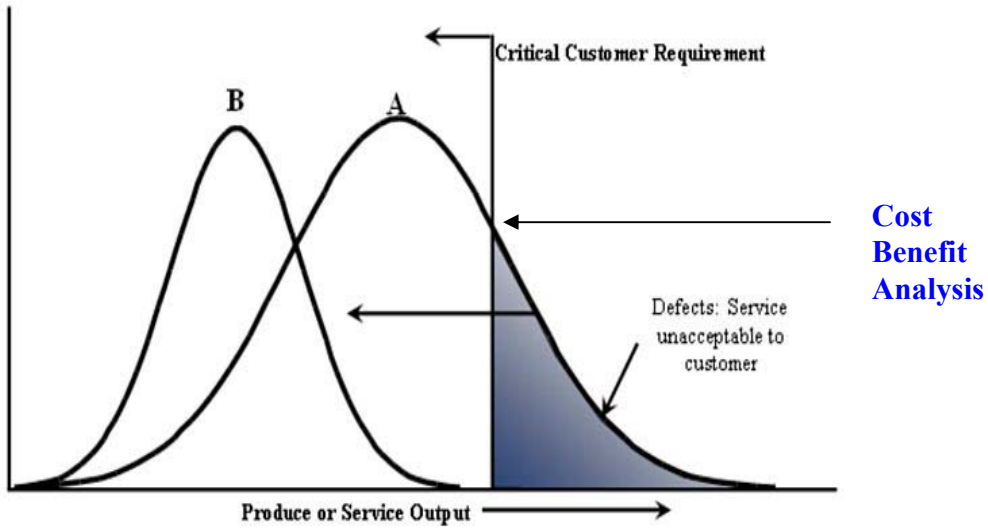


***Figure-2: Critical Customer Requirement***

Your customers may ask what sigma level are your products or services. The sigma level allows us to quantify our ability to provide services or produce products. Using the sigma level we could compare dissimilar goods or services. For example, 2-sigma means 69.2% of products or services meet customer requirements or 208,000 Defects per Million (DPM) whereas 6-sigma means 99.99966% of products or services meet customer requirements or 3.4 DPM. In application development project risk context, could a programmer write 1 million lines of code (LOC) with less than 3.4 LOC errors?

Among other things, the Six-Sigma methodology brings an effective structure to process management. Since the focus is on the customer's definition of quality, the Six-Sigma project demands identification of the business strategy and its key elements for success. In addition, it requires the identification and analysis of gaps that may lead to failure. In case of an administrative operation, the main factor affecting system performance is excessive human involvement. It is very difficult to develop robust measurement tools to quantify, control, and manage employees. Consequently, Six-Sigma can be deployed in any type of organization or nature of business and achieve success through process improvement and risk mapping. It can be easily integrated with other initiatives to enhance and build upon improvements that are already in place. Although Six Sigma is typically associated with medium to large enterprises, with proper and careful planning and follow-through it can be easily adapted to small to medium business.

## Integrated Decision Making

Decisions regarding project selections, incentives to sales or production units, resource allocation, and so on, must all be based on sound data analysis. Consider the project selections. As projects are deployed, decisions need to reflect the data. Sponsors or directors need to motivate the project team the project team to acquire sufficient data to justify decisions made at each stages of **DMAIC** (one of the associated methods with Six Sigma) by asking the right questions. For example, is the project defined for the correct problems? Does the project attack the root cause or just the symptom? Has the data been properly analyzed? Is the improvement plan sustainable? Business success will be more closely aligned with project success when management consistently integrates this way of thinking into their daily decisions. Rather than reacting to the daily crisis, management should understand the differences between common and special causes of variation, and react accordingly. The executives may encounter difficulties in making the right decision; however, the following guidelines are very useful for their considerations:

**Four Critical Risk Management Decision Making**

1. Accept No unnecessary risk
2. Accept necessary risk when only benefit outweigh than costs
3. Make risk decisions at the appropriate and affordable level
4. Crisis and risk management just as Critical Business Planning and Renewal Strategy

Most importantly, from the management point of view, the risk management is classified as problem solving while the crisis management is kind of decision making. From the technical and professional point of view, the risk management is prevention-focused while the crisis management is response-oriented.

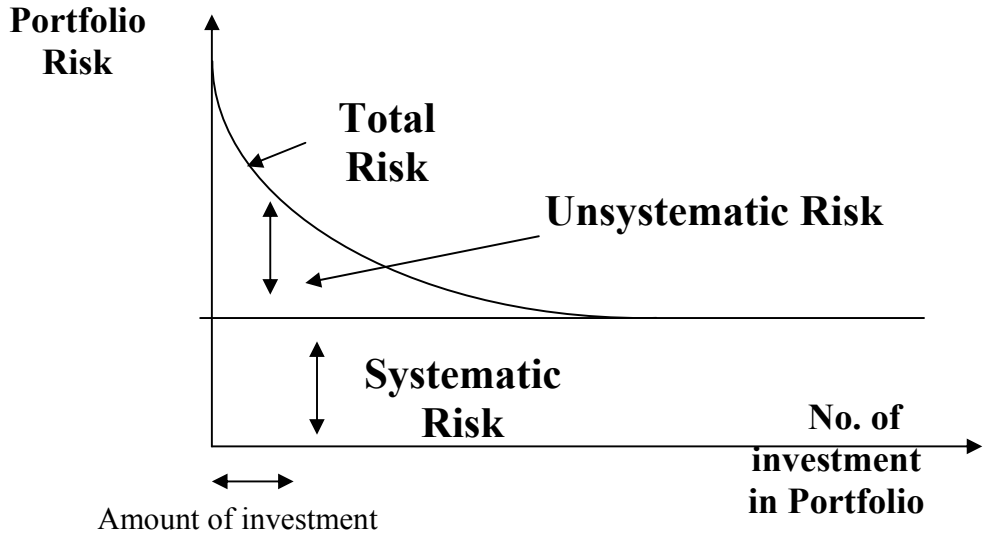


***Figure-3: Risk Diversification***

There is a wealth of data available to management for decision making. Six sigma projects can be used to define, collect, and synthesize the data necessary for project

decision making. Eg. Reliable customer data (internal perceptions and actual customer needs), data-mining, and benchmarking

## Application of Six-Sigma to minimize the financial risks

There are many types of financial risks. We should know how to identify the risks and take appropriate actions for risk prevention and response/recovery. The focus will be on the methods of identifying and measuring the impact of these exposures and the appropriate tools to hedge an organization's exposures. Starting from the root cause effect analysis tools for identification of critical issues in business or organization, to the use of FMEA operational method, Six-Sigma is the appropriate tool for achieving our requirements. To be effective, the financial risk management should include the following:

- ***Risk & return concepts***
- ***Risk & crisis opportunities***
- ***Risk exposures***
- ***Risk diversification & hedging***

***Figure-4: Categories of risks***


## Voice of the customer, business, employee, and external forces

For a clear process improvement direction, it is required to define the focus of the improvement plan. According to George Labovitz and Victor Rosansky, "The power of Alignment" (1997), the four areas are needed to focus are listed below.

1. Voice of the customer

   This is a measure of customer dissatisfaction. Critical customer requirements change over time. Gathering customer data should be through both formal (such

as carrying out a competitive benchmarking survey) and informal channels. It should also be openly confirmed with the customer to build trust relationship. It is critical to quality and customer.

2. Voice of the business
   Internal objectives, governance and critical requirements must be included in the plans for growth and improvement. It is critical to process financials.
3. Voice of the employee
   Employees must have the capabilities to execute the plan objectives. A well balanced plan must acknowledge both the current status of employee competencies and the objective target for new capabilities and cultural climate. It is critical to learning and improvement.
4. Voice of the external forces
   External forces, such as legal requirements, competitive pressures, and technology shifts, muse be adapted, included and measured. Intelligence on trends and pending changes must be evaluated for planning. It is critical to change response.

In risk management context, it is important to translate the above critical requirements into what must occur in your business. We should pay attention to creating balance across our business organization and operations to create a plan of related 'voice'. In all cases, we should also evaluate their related treats and opportunities.

For example, after a serious virus attack to your financial computer systems, we may have the following issues and areas of focus. Improvement plan must be taken to address the business crisis timely.

Voice of the customer
   Customers complained the business services due to virus attacked.
Voice of the business
   Serious reputation and financial loss due to the virus attacked.
Voice of the employee
   Latest virus signature had been deployed.
Voice of the environment
   SOX requirement must be complied with adequate internal control.

## Application of Six-Sigma to solve the problem of virus attack

As of the example in the session "Voice of the Customer", we could carry out a DMAIC improvement initiative that brought its quality standard from 3-sigma to 5- sigma or more. The company's serious virus attack to your computer systems, we may have the following issues and areas of focus**.** (Dr. Freddie P.W. Lee, Strategic Crisis and Risk Management)

Define
Located problems using process mapping and other tools and locked in the core problems that needed to be solved
Measure
Found out the opportunity of error of the present process flow and the main causes of error.

Analysis
Clarified the company's position and compared it with the benchmark so as to see how far the company was behind. Then the management decided the maximum extent of improvement to be undertaken
Improve
Implemented improvement solutions with suitable procedures
Control
Controlled the new process flow and measured outcome regularly.

In the "Define" and "Measure" phases, we could locate the core problems by mapping the existing procedure and found out the main causes of error.

Virus Signature Update Procedure

1. Receiving virus signature update from vendor through Internet, CDROM, encrypted delivery
2. Store virus signature on distribution server
3. Disseminate the virus signature using deployment tools
4. Check to ensure the virus signature has been received by every computer
5. Check the virus scanning history of every Anti-virus agent
6. Ensure alert message has been enabled for virus found

In information security management practices, we must evaluate and define the requirements for protecting financial information which are always exposing to virus attacks, cyber threats and internal hacking. Real-time financial data must be maintained with the CIA information security concepts in mind. DMAIC approach could be the appropriate method to prevent, detect and correct any problems that could damage the business operations.

Some of the improvement solutions were:

1. Propose to have dual-scanner for higher protection to mitigate the detection risk
2. Propose to have better anti-virus scanner to mitigate technology risk
3. Carry out testing procedures for the new received signatures to ensure no production system crash issues
4. Check the anti-virus scanner log regularly to see if the new deployed signature has been effectively run.
5. Prepare BCP and DRP before dissemination of virus signatures
6. Prepare Incident Response Procedure
7. Audit the updating procedures regularly
8. Institutionalize the above procedures onto the corporate information security policy.

Thank you. July 2005.

Contact: Mr. Danny Ha, iamokthankyou@gmail.com

*A paper for the 6th Info-Security Conference www.infosecurityproject.com*
*"The Latest Security Definition, Application and Technical Know-How"*
*Info-Security Handbook 2005*