

BALI
ERM
2016

WHITEPAPER

Managing Risks in the Digital Era

BALI INTERNATIONAL CONFERENCE
ON ENTERPRISE RISK MANAGEMENT
2016

8 - 9 DECEMBER 2016

FOREWORDS

The 6th BaliERM International Conference themed 'Managing Risks and Opportunities in Digital Era' was held at Sofitel - Nusa Dua in Bali on 8-9 December 2016. Bali, the home of many major international conferences amid pleasant surroundings, was a delightful place for the conference with a vibrant cultural rich learning environment. Around 300 participants, of whom more than 100 board members, had many fruitful discussions and exchanges to the success of the conference. Participants from more than 15 countries made the conference truly international in scope.

16 sessions were presented over the span of two days formed the heart of the conference and provided ample opportunity for discussions which were delivered through some plenary sessions as well as through the three tracks of classroom coaching clinics. More than 30 presenters and participants shared and exchanged their knowledge and experiences.

BaliERM 2016 was organized under the association with our reputable Indonesian partner CRMS (Center for Risk Management Studies) Indonesia. With the collaboration of the International Finance Corporation - World Bank, experienced speakers from all over the world, and the very dynamic interaction throughout the program, we believe that all the insights and learning points generated from BaliERM 2016 should be shared to a much wider audience.

This volume of proceedings may provide an opportunity for readers to gain some insights and foresight as a helping tool to embrace the challenges, risks, and opportunities in the digital era.

We do hope you enjoy the reading and look forward to welcoming you at the next BaliERM2017 scheduled on 7-8 December 2017.

With Warm Regards,



Dr. Antonius Alijoyo, ERMCP, CERG
Chairman, Enterprise Risk Management Academy



TABLE OF CONTENT

4.....	Ethical Governance
11.....	The Importance of ISO 31000 to Increase the National Quality Assurance
16.....	Building Intellectual Risk Culture in the Digital Era
29.....	Managing Compliance and Risks in Digital Business Environment
41.....	Managing Risks in High Impact Mega Project Infrastructure
49.....	Risk Management in Family Business
56.....	Climate Change Risk Management
70.....	The Use of SNI ISO 31000 Risk Management Standard to Embrace Digital Challenges and Opportunities
81.....	Enterprise Legal Risk Management – Digital Environment
94.....	The New Face of Financial Risk Management in the Next Decade
102.....	The Journey of Risk Management Implementation in State-Owned Enterprises
112.....	International Perspective: GRC towards Economic Value Addition
116.....	The New Face of Strategic Risk Management in the Next Decade
121.....	Children of the Future - Renewable Energy Risk Management
134.....	Cyber Risk Management

ETHICAL GOVERNANCE

(Keynote)



BALI
ERM
2016

Ethical Governance

Presented by:

Prof. Dr. Ilya Avianti, S.E, M.Si, Ak, CPA

Board of Commissioner and Chair of Audit Board
Otoritas Jasa Keuangan

Hosted by:

Dr. Antonius Alijoyo, ERMCP, CERG

Chairman of Enterprise Risk Management Academy

The development of information and communication technology encourages the creation of a new chapter in human life, which is known as the digital era. In this digital era, the human behavior is constantly changing. These changes are driven by technological development on information and transaction systems; for example: new concepts, such as e-commerce (e.g. Tokopedia, Amazon, etc.) are arising. Other than e-commerce, another concept of sharing economy based on digital and financial technology has also arisen.

According to Mrs. Ilya, sharing economy emphasizes on a concept of a socio-economic system which has a concept of sharing and collaborating. Meanwhile, financial technology has the role of conventional financial institutions, payment, and transfers as well as lending and financing, by emphasizing the utilization of communication and information technologies. In financial technology, physical interactions are no longer required.

As a concept, financial technology is expected to be able to help stimulates the economic condition of a country or overall global economy. However, the rapid development of financial technology is not balanced with adequate regulatory developments.

According to Mrs. Ilya, when the government makes a regulation, it will pay attention to all aspects. The government needs to make sure that the new regulations that will be issued, will not hinder the business process. This situation makes the regulation relatively slow to be able to be issued. Moreover, this situation led to the occurrence of fraud cases in financial technology.

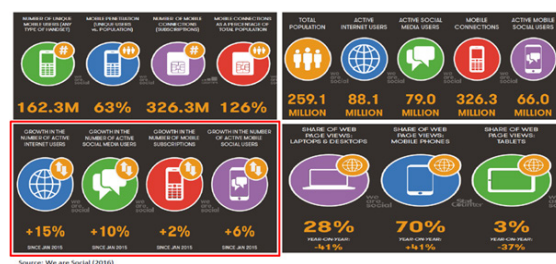


Figure 1. Technology Usage in Indonesia

Currently, the development of information and communication technology in Indonesia is very rapid. Based on the data obtained by the FSA in January 2016 (shown in Figure 1), Indonesia has more than 259 million people. Meanwhile, the number of mobile connection subscribers in Indonesia is around 326.3 million. These numbers show that every Indonesian people may have more than one mobile phone.

The number of mobile penetration in Indonesia is currently at 63% with 2% growth rate of

mobile subscription. Internet users in Indonesia grow at 15%. Indonesia is one of the most active countries in the world in terms of social media with 79 million social media users. This number means that around 30% of the total population in Indonesia owned social media account.

Additionally, the growth of social media users in Indonesia is 10%, with the growth of around 6% for the mobile social media users.

The high number of digital media usage in Indonesia is being realized by the public sector. This situation makes public sector aware that they have to carry out digital transformation. This digital transformation was conducted by providing public services based on digital systems.

These innovations can be seen as the commitment from the public sector in order to improve government services to the citizen. For example, Indonesia Financial Service Authority (OJK) has an online portal to provide updated information to all stakeholders.

Another public institution in Indonesia that has implemented an online system is the Directorate General of Taxation, which is known as Dirjen Pajak in Indonesia. Dirjen Pajak provides services to the public through e-billing, e-filing, and e-faktur.

According to Mrs. Ilya, utilization of technology by the public sector is expected to improve the quality and quantity of public services to the citizen.

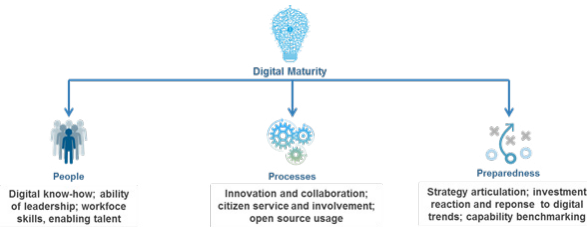


Figure 2. Digital Maturity

Digital transformation can be seen as a commitment to improve services from the government to the citizen. These efforts can also increase transparency between government and stakeholders. However, according to Mrs. Ilya, it is still a long journey for digital transformation to reach digital maturity.

Digital maturity means that digital transformation can bring positive impact to achieve all of the objectives. To achieve digital maturity, it must be supported by three aspects: people, processes, and preparedness (see Figure 2).

People aspect is related to human resources (the skills and leaderships). While in the processes aspect, innovation and collaboration are needed in order to achieve digital maturity. This collaboration includes the engagement of the citizen. In preparedness aspect, in order to achieve maturity level, better strategy articulation and quick response to the changes in digital trend are needed. To support this aspect, benchmarking is necessary to determine success and failure factors.

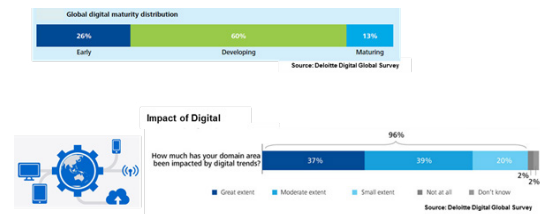


Figure 3. Impact of Digital on Public Sector

According to a survey (see Figure 3) conducted by Deloitte with 12,000 respondents in 70 countries, 96% respondent stated that the digital era has given improvement to the performance of public sector.

According to Mrs. Ilya, this survey result shows that the public sector cannot be ignorant to the digital era. Instead, public sector should take an advantage from the digital era to generate a positive value.

Based on the survey, the maturity level of public sector is mostly located in the developing stage (by 60%), 26% are in the early stage, and only about 13% are at the mature stage.

Characteristic of a digitally maturing organization				
	EARLY	DEVELOPING	MATURING	
Strategy	Aimed at cost reduction	Aimed at improving customer experience and decision making	Aimed at fundamental transformation of processes	
Leadership	Lacks awareness and skills	Digitally aware	Digitally sophisticated	
Workforce development	Insufficient investment	Moderate investment	Adequate investment	
User focus	Absent	Gaining traction	"Central" to digital transformation	
Culture	Risk averse, disintegrated	Risk tolerant, accommodates innovation and collaboration	Risk receptive, fosters innovation and collaboration	

Top Barriers by Maturity			
	EARLY	DEVELOPING	MATURING
Lack of overall strategy	Lack of overall strategy	Too many competing priorities	Too many competing priorities
Lack of understanding	Lack of understanding	Insufficient funding	Insufficient funding
Lack of entrepreneurial spirit, willingness to take risks	Lack of entrepreneurial spirit, willingness to take risks	Security concerns	Security concerns
Too many competing priorities	Too many competing priorities	Lack of organizational agility	Insufficient technical skills
Lack of organizational agility	Lack of organizational agility	Lack of an overall strategy	Lack of organizational agility

Figure 4. Digital Maturity Steps

Characteristics are being used to assess the level of digital maturity. These characteristics include strategy, leadership, workforce development, user focus, and culture (see Figure 4). If these five characteristics are not met, digital maturity could not be achieved.

Therefore, according to Mrs. Ilya, there are some questions that could become a reference in order to fulfill the five aspects. These questions are:

1. For Strategy

Do we have a clear and coherent digital strategy that addresses the key elements of digital transformation?

2. For User Focus

How can citizens and service users be a part of our digital transformation?

3. For Culture

What have we done to strengthen our organization's innovative and collaborative culture?

4. For Leadership and Workforce Skills

Have we looked at our talent pool and planned where our skills will come from?

At each stage of maturity level (early, developing, and maturing), the barriers that have to be faced would be different. In the early stages, the fundamental aspect that becomes the barrier is a lack of overall strategy.

The strategy is a component that supports the readiness of digital maturity level. According to Mrs. Ilya, errors in selecting digital transformation strategy happened when the strategy only focus on the provision of the latest technology while ignoring the readiness of human resources skill.

According to Mrs. Ilya, if the hardware is based on new technology but the human skill is not updated, there would be a gap between hardware and the skill of users. Hence, development of human resources is important in order to avoid the lack of understanding.

Human factor plays an important role in digital transformation because it relates to the way of thinking and decision-making. On human factor, leadership and skills become the driver for digital transformation.

Leaders who have sufficient digital skills can make changes for the employee skills as well. According to the Deloitte survey, leaders who have sufficient digital skills can increase the chances of success in implementing a digital transformation by three times. However, the development also needs to be fully supported by the organization.

Risk Management, Ethics, and Governance in the Digital Era

In the digital era, the environment is rapidly and continually changing. Changes in an environment should be anticipated because changes are related to uncertainty.

The element of uncertainty will affect the achievement of objectives for an organization. Thus, risk management is required to anticipate the changes that occur in the digital era. With risk management, an organization could be well prepared to anticipate environmental changes, which happening very fast.

Development of risk management in the private sector is relatively fast compared to public sector. The private sector has begun to realize the importance of risk management in protecting and creating values. Meanwhile, public sector awareness for risk management is relatively low (as an illustration, the FSA (OJK) and ministry of finance are the public institution in Indonesia that implements risk management).

In fact, the role of the public sector is very critical. When the public sector failed to anticipate risks and have negative impacts to their organization, not only the public sector itself is affected but it will also affect the private sector. Therefore, the success of the private sector cannot be separated from the success of the public sector.

The advancement of technology in the digital era has bypassed time and nation boundaries problem. This situation leads to a rapidly changing environment.

Sometimes, changes are not quickly balanced by a quick and precise response from the government. Regulations made by the government tend to be reactive and slow. According to Mrs. Ilya, a shift of paradigm in management of an organization from rule-based to the principles-based to support aspects of governance is needed.

Governance aspect plays an important role in organization's sustainability. On Good Corporate Governance (GCG) principles, ethics

aspects are mentioned. However, according to Mrs. Ilya, GCG is usually only being seen to support administrative aspect.

On the other hand, ethics is very important in implementing GCG when the rules are not available yet. Ethics can guide a person or organization to do a good thing because ethics is associated with norms or value system in a person or organization. In other words, people will tend to avoid doing negative things; they will be ashamed if they do those things or if they make mistakes.

Therefore, ethics should be realized as a necessity and conviction and not merely as an administrative purpose. Mrs. Ilya also stated that Ethical Principles (starting from Planning, Implementation, to the Management Accountability and Evaluation) must exist in order to achieve sustainability.

*Written by: **Yusuf Munawar***

CONCLUSION

The digital era comes with many benefits, as long as an organization is ready to take advantage of digital development. Public sector can take an advantage in this digital era by carrying out the digital transformation. With this transformation, the public sector could improve the quality and quantity of public services.

In the digital transformation, human factors (especially leadership and skills) play an important role in order to achieve digital maturity. Besides all of the benefits, the rapid changes in the digital era might lead to negative impact if not managed properly. Hence, risk management and ethics have important role in governance. Ethics plays a crucial role when regulation is not formed yet.

STANDARDS BUILD TRUST:

The Importance of SNI: ISO 31000

Risk Management Standard

to Increase the National Quality Assurance



BALI
ERM
2016

Standards Build Trust:

The Importance of SNI: ISO 31000 Risk Management Standard
to Increase the National Quality Assurance

Presented by:

Prof. Bambang Prasetya, Ph.D.

Chair of National Standardization Body Indonesia

Hosted by:

Prof. D. S. Priyarsono, Ph.D., CERG

Chairman of Academic Advisory Board CRMS Indonesia

Uncertainties, risks, and opportunities are natural, critical, and must be embraced by every nation. If nations did not do it, they might lose their national competitive advantage because they will not be ready to deal with the downside or upside risks. Therefore, nations need to build their national risk management capacity and capability systematically.

Building risk management capacity and capability at the national level requires the existence of a national standard. By having a standard, the nation (privates and public sectors) will be able to develop its risk management capability and capacity structurally.

Perceiving this phenomenon, Enterprise Risk Management Academy (ERMA) invited an experienced practitioner, Prof. Bambang Prasetya Ph.D., to share his knowledge and thoughts about the importance of SNI: ISO 31000 risk management standard which could be used to increase the national quality assurance.

Mr. Bambang is the chair of National Standardization Body Indonesia (BSN Indonesia) and the chair of National Accreditation Committee Indonesia (KAN Indonesia). Looking at his roles, ERMA believes that his experience sharing will be useful to the participants of BaliERM 2016. Hence, below are the summary taken from his presentations during BaliERM 2016.

Every year on October 14th, an initiative from the World Standards Cooperation (WSC), as a member of the IEC, ISO, and ITU, celebrates World Standards Day. It is a way of paying tribute to the collaborative efforts of the thousands of experts worldwide who dedicate their time and expertise to the development of international standards.

The theme for World Standards Day 2016 is "Standards Build Trust". Standards connect us with reliable modes of communication, codes of practice, and trusted frameworks for cooperation.

International standards speak to the diversity of our interconnected world, introducing uniformity at the interfaces where we need to be certain that we are speaking on the same terms. For example, we trust that electrical equipment will be safe to use and function as expected if it conforms to the international standards for safety, quality, and compatibility with related electro-technical infrastructure.

The different standards reflect the different motivations and technical focus of their developers and are appropriate for different organizations and situations. Standards and guidelines – which typically are voluntary – are not regulations.

Standards are published as a formal document that can establish criteria, methods, processes, and practices. It provides value when they foster common understanding reflecting collective wisdom while creating efficiencies and better results for the organizations who are using them.

Without international standards, there would be no confidence in the global supply chain of goods and services that most of us readily take for granted. When we scan our well-stocked store shelves or call upon a service provider, we trust – and expect – that the products or services they provide will meet our expectations. That thing happened because behind the trust, there are standards and conformity assessment ensuring the reliability.

The everyday life we know would not work without standards. From tech gadgets to office and household items, to services in the global economy, including risk management, everything got standards. Risk management standards set out a specific set of strategic processes which started with the overall aspirations and objectives of an organization, and intended to help to identify risks and promote the mitigation of risks through best practice.

In benefiting organizations, risk management standards generally recommend risk criteria, methods, processes, and practices. It helps organizations to implement strategies which are tried and tested, and proven to work.

Risk management itself plays an important role in facing uncertainties due to the increasing number of unpredictable bio-geodynamic, such as environment-ecological global warming, global economic challenges, natural disasters,

social dynamic and lifestyle, issues related to terrorism, and the impacts of social media-ICT (Information and Communication Technologies).

In order to reduce risks, we can use the implementation of standards to the product development process. The process of implementing and developing technical standards based on the consensus of different parties is called as standardization. Standardization can help not only to maximize compatibility, interoperability, safety, repeatability, and quality, but also to minimize the uncertainties and risks.

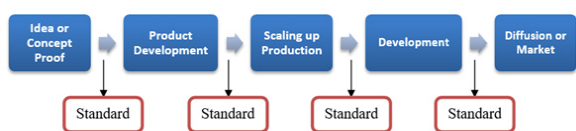


Figure 1. Role of Standard to Reduce Risk

In Indonesia, we already have SNI (Indonesian National Standard) ISO 31000 as our national risk management standard. SNI ISO 31000 provides principles and guidelines on risk management. The principles and guidelines are generic and not developed for any specific industry or sector.

SNI ISO 31000 can also be applied throughout the whole organization and to a wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services, and assets. Moreover, it can be applied to any type of risks, whatever its nature, whether it has positive or negative consequences.

Nevertheless, although SNI ISO 31000 provides generic guidelines, it is not intended to promote uniformity of risk management across organizations. The design and implementation

of risk management plans and frameworks will need to adjust to the organization’s particular objectives, context, structure, and operations.

There are 11 principles in risk management SNI ISO 31000, which are:

1. Create and protects value
2. Is an integral part or organizational processes
3. Part of decision making
4. Explicitly addresses uncertainty
5. Is systematic, structured and timely
6. Is based on the best available information
7. Is tailored
8. Takes human and cultural factors into account
9. Is transparent and inclusive
10. Is dynamic, iterative and responsive to change
11. Facilities continual improvement and enhancement of the organization

These principles should be applied to the risk management framework and also to the risk management process because risk management principles are the foundation of risk management when implementing and operating the risk management arrangement.

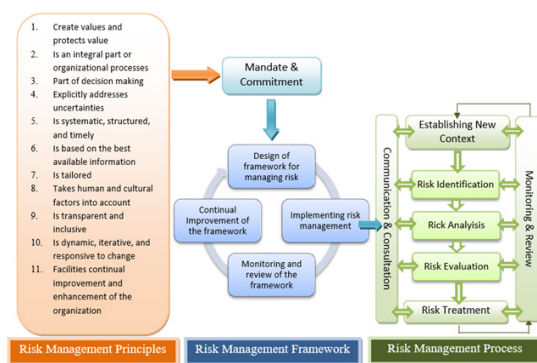


Figure 2. SNI ISO 31000 Risk Management – Principles and Guidelines

Written by: **Aldi Ardilo**

CONCLUSION

International standards play an important role in building trust since they are necessary to ensure safety, dependability, and interoperability. Reliability and trust are fundamental components of any process, business, or service because the standards and conformity assessment stand behind them.

Also, a standard has a significant positive impact on reducing risks. SNI ISO 31000 is one of the tools to manage uninvited risk. Additionally, as the Indonesia risk management standard, SNI ISO 31000 will become a contributing pillar in building national risk resilience, by helping the nation to create values (economic value, social value, and environmental value) in order to satisfy stakeholders' interests.

Furthermore, it also can be used to protect value when facing uncertainties due to the increasing of bio-geodynamics. Lastly, the implementation of SNI ISO 31000 should be in line with the implementation of other management systems.

BUILDING INTELLECTUAL
RISK CULTURE
IN THE DIGITAL ERA



BALI
ERM
2016

Building Intellectual Risk Culture in the Digital Era

Presented by:

Dr. Guido Gianasso

Professor of Nanyang Business School Singapore;
Management Consultant Honorary Consul of Romania
in Geneva

Chairil Tarunajaya

Partner of Risk Consulting Services PwC SEAC & Indonesia

Hosted by:

Prof. D. S. Priyarsono, Ph.D., CERG

Member of National Technical Committee SNI: ISO31000 BSN;
Chairman of Academic Advisory Board CRMS Indonesia

Nowadays, we live in the digital era that changes most of human behaviour in doing many things, such as the way people do their daily activities, buy something, interact with others, etc. It also influences the behaviour of customers in the market as well as the employees in the organizations.

Due to this situation, organizations cannot just do nothing and hope for the changes to suddenly happen by itself. Instead, they should do something to be able to adapt to the changes.

In this session, Dr. Guido presented about the changes of human behaviours, whilst Mr. Tarunajaya talked about how the world changes due to the digital era via the surveys done by PwC. Other than those two topics, both of them also discussed risk and digital culture.

Part 1

Dr. Guido Gianasso

Professor of Nanyang Business School Singapore and Management Consultant
Honorary Consul of Romania in Geneva

The role of risk management is to ensure the achievement of corporate strategic objectives. However, the human factor in risk management must not be forgotten. Human factors are the factors that influence the behaviour of people and the work environment. Hence, organizations should understand the human factors in order to minimize the errors that can be caused by them which are known as human errors.

Individual behaviours are determined by their own mental program. Mr. Gianasso mentioned that according to Hofstede and Hofstede (2005), there are three levels in Human Mental Programming, including human nature, culture, and personality.

Human nature and personality are inherited and universal, whilst, culture is obtained through learning in the environment and usually specific for groups (work environment, clan environment, and country environment).

Regarding personality, every person will have a different personality. This personality will determine how an individual act in the environment. Moreover, personality has five big traits, which are:

1. Extraversion / introversion
2. Openness to experience
3. Conscientiousness
4. Agreeableness
5. Emotional stability (neuroticism)

In terms of risk management, these personality traits will affect an individual's risk tolerance.

For example:

1. Higher Extraversion is associated with higher risk tolerance (Pan and Statman, 2009). Extraverts' need of stimulation is likely to result in an increased desire for sensation seeking (Eysenck, 1973) which is a strong predictor of risk tolerance (Harlow and Brown, 1990).
2. Higher scores on openness to experience are associated with having a high-risk tolerance (Hunter and Kemp, 2004). That is because people with higher scores on openness to experience are more tolerant to uncertainty and change (McCrae and Costa, 1997), more adventurous and imaginative, and more active to search for new experience and seek out risks (Kowert, 1997).
3. Higher conscientiousness is associated with having a lower risk tolerance (Pan and Statman, 2009). This is because people with high conscientiousness need conformity and control (Hogan and Ones, 1997); have less tolerant of uncertainty, change, and innovation (Nicholson et al., 2005); and have hasty, impulsive, careless, and impatient characteristics that make them more likely to want to take risks (Kowert, 1997).
4. Higher scores on agreeability is associated with having a lower risk tolerance. Most highly agreeable individuals fear the harm that could come to others through their own risky behaviour (Kowert, 1997).

5. High scores on neuroticism are related to having lower risk tolerance (Nicholson et al., 2005). That is because people with high scores on neuroticism are less resilient (Nicholson et al., 2005), focus more on threat (Eysenck, 1992), usually interpret ambiguous stimuli as more threatening (MacCleod & Cohen, 1993), and have a high fear of failure (Elliot and McGregor, 1999).

From the big five traits that have been mentioned before, there are 3 types of risk managers, which are technicians, drivers, and evangelist (see Figure 1). Each type has a unique behaviour which can be strength or weakness and opportunity or threat in certain conditions.

The Traditionalists	The New Breed
'TECHNICIANS' <i>Reactive introverts – over 60%</i> <ul style="list-style-type: none"> Analytical Logical Planners Naturally cautious Attention to detail Sticks to facts/follows rules Ignores emotionally charged arguments Serious and responsible Suspicious of others Brief and to-the-point 	'DRIVERS' <i>Proactive introverts – less than 10%</i> <ul style="list-style-type: none"> Very pragmatic Produces results ahead of expectations Focused and determined Prefers results to facts Demanding, not always reasonable Impatient, no time for lots of detail The end justifies the means 'EVANGELISTS' <i>Proactive Extroverts – over 30%</i> <ul style="list-style-type: none"> Inspiring leaders Very optimistic Diplomatic and persuasive Verbose and prone to exaggerate Over familiar Can appear to lack gravitas

Figure 1. Three Types of Risk Managers

Reactive introverts have more population (60%) than the proactive extroverts (40%). Reactive introverts can be said to be a problem because reactive introverts are usually not “persuasive commenters”. They often lack of delivery or communication skills required to gain acceptance or overcome resistance.

On the other hand, proactive introverts or “drivers” represent individuals determined to see a project brought to a successful conclusion; while proactive extroverts or “evangelists” possess more social skills and charm.

Other than personality and human nature, culture also has a role in human behaviour. To know more about culture, these are some concepts of culture by some gurus:

• Hofstede G.H. (1980): “the collective programming of the mind which distinguishes the members of one human group from another.”

• Tylor E. (1871): “that complex whole which includes knowledge, beliefs, art, moral, laws, customs and any other capabilities and habits acquired by man as a member of society.”

• Kroeber A.L and Kluckhohn C. (1952): “transmitted patterns of values, ideas and other symbolic systems that shape behaviour.”

Culture could be divided into many layers. For example national, regional, gender, generation, social class, industry, company, profession, and so on. All of these are influencing the way we think, proceed, and behave.

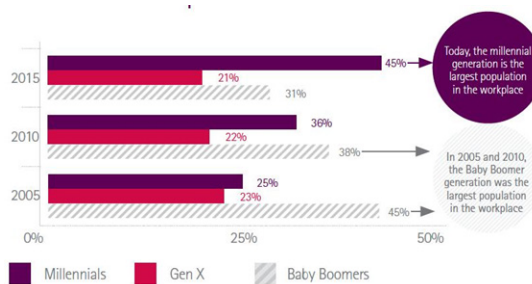


Figure 2. Generation in the Workplace

Generation is one of the many layers of cultures. In each workplace, there must be a majority of generation per a certain time. Figure 2 shows the majority of generation in 2005, 2010, and 2015.

In 2005 and 2010, the Baby Boomers generation was the largest population in the workplace. But in 2015, the Millennial generation is the largest population in the workplace. There is a different culture in the workplace when the Baby Boomers are the largest population.

Baby Boomers are identical with work-centric, independent, goal-oriented, competitive, and self-actualization. Whereas generation Y is identical to tech-savvy, family-centric, achievement-oriented, team-oriented, craves attention, and prone to job-hopping.

The differences in every generation will make different cultures. For example, some people definitely feel the difference in leadership style of their leader when the leader came from the different generation.

Other layer of culture besides generation culture is national culture. Some facts about national culture are:

1. 70% of cross-national business ventures fail due to cultural clashes
2. Only 14% of the Fortune 500 CEOs come from a country which is different from the country of their company's HQs.

According to theory by G. Hofstede, there are 5 dimensions of national cultures as follow:

1. Power distance index (PDI):

The power distance index is defined as "the extent to which the less powerful members of

organizations and institutions (like the family) accept and expect that power is distributed unequally." In this dimension, inequality and power are perceived from the followers, or the lower level. A higher degree of the index indicates that hierarchy is clearly established and executed in society, without doubt or reason. A lower degree of the Index signifies that people question authority and attempt to distribute power.

2. Individualism vs. collectivism (IDV):

This index explores the "degree to which people in a society are integrated into groups". Individualistic societies have loose ties that often only relate an individual to his/her immediate family. They emphasize the "I" versus the "WE." Its counterpart, collectivism, describes a society in which tightly-integrated relationships tie extended families and others into in-groups. These in-groups are laced with undoubted loyalty and support each other when a conflict arises with another in-group. The high side of this dimension called individualism and the low side called collectivism.

3. Uncertainty avoidance index (UAI):

This dimension describes how well people can cope with anxiety. People who are in the societies with a high score of Uncertainty Avoidance tend to make their life as predictable and controllable as possible. If they find that they cannot control their own lives, they may be tempted to stop trying. A lower degree of this index shows more acceptances of differing thoughts/ideas. Society tends to impose fewer regulations, ambiguity is more accustomed to, and the environment is more free-flowing.

4. Masculinity vs. femininity (MAS):

In this dimension, masculinity is defined as "a preference in society for achievement, heroism, assertiveness and material rewards

for success.” Its counterpart represents “a preference for cooperation, modesty, caring for the weak and quality of life.” Women in the respective societies tend to display different values. In feminine societies, they share modest and caring views equally with men. In more masculine societies, women are more emphatic and competitive, but notably less emphatic than men. In other words, they still recognize a gap between male and female values. This dimension is frequently viewed as taboo in highly masculine societies.

5. Long-term orientation vs. short-term orientation (LTO):

This dimension associates the connection of the past with the current and future actions/challenges. A lower degree of this index (short-term) indicates that traditions are honoured and kept, while steadfastness is valued. Societies with a high degree of this index (long-term) views adaptation and circumstantial, pragmatic problem-solving as a necessity. A poor country that is short-term oriented usually has little to no economic development, while long-term oriented countries continue to develop to a point.

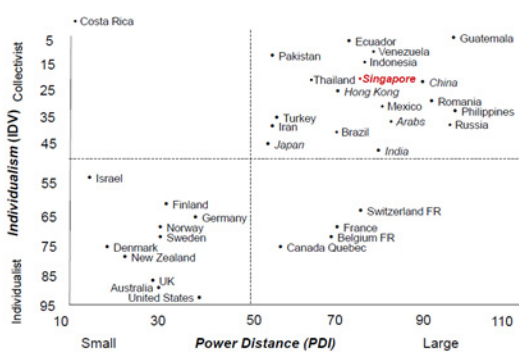


Figure 3. Scores of Each Country in PDI and IDV Dimensions

From figure 3, you can see that Indonesia located in Large PDI and Collectivist. It means that Indonesia has a clear hierarchy and tightly-integrated relationships.

On the other side, countries which have small power distance and individualism mean that their people strive to equalize the distribution of power and demand justification for inequalities of power. Also, most of them have loose relationships.

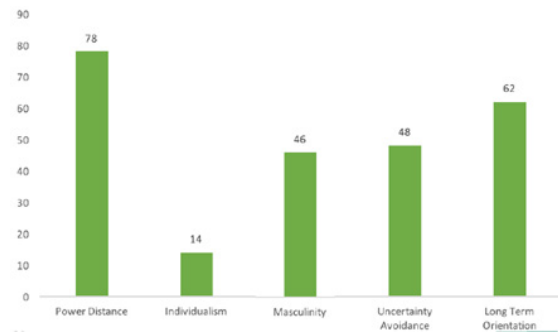


Figure 4. The Scores of Indonesia in 5 Dimensions

Figure 4 shows how high the scores each dimension of national cultures in Indonesia. Also, those scores influence how organization approaches the risk assessment methodologies.

Most risk assessment methodologies include five steps such as: (1) defining context; (2) risk identification; (3) risk assessment; (4) risk response; and (5) risk reporting and monitoring.

1. Defining context

For example:

a. Business objectives are long-term or short-term. In Japan, most business objectives are cast at a minimum of five-year increments whereas U.S. corporations have a shorter-term horizon (quarterly reporting commitments).

b. When dealing with cultures with a high UAI score, risk managers should concentrate on the short-term risks. The audience have a cultural tendency to value less uncertainty and this will be accommodated by taking a longer view of business activities, goals, objectives, and strategies.

c. For the United States and other cultures with a low UAI score, risk managers should focus the assessment of risks on the long-term viability of the firm's business objectives and strategies to compensate for the cultural predisposition to shorter-term results.

2. Risk identification

For example:

a. For high UAI and PDI cultures, a high acceptance of authority is a key value. Consequently, group discussions would be quite difficult to conduct if there are people of power in the session. Any form of anonymous voting or sharing of information is ideal. Furthermore, since internal or company-specific risks often grow out of strategic and operating decisions made by managers, the interviewer should consider this when identifying risk assessment participants, including both top-down and bottom-up risk identification.

b. In low UAI and high PDI cultures, a low acceptance of authority is a common trait. These cultures appreciate open debate. Therefore, all three risk identification methods can offer constructive results.

3. Risk assessment

For example:

a. Cultures with a high UAI and low IDV score rely heavily on employee integrity. The trust factor goes both ways: the employee and employer trust each other to do the right thing without having to resort to controls to safeguard assets. The idea of "saving face" to avoid the humiliation or embarrassment of disrupting harmony among the group helps to reinforce this shared bond of trust.

Risk managers should concentrate the risk assessment process on identifying inherent risks and spend less time trying to identify controls, precisely because the best control may be a cultural one.

b. For the United States and other cultures with a low UAI and high IDV score, controls are more necessary.

4. Risk response

For example:

a. Cultures with high UAI score have a lower residual risk appetite, preferring to manage the uncertainty more conservatively, unlike the lower UAI cultures that celebrate ambiguity and are more susceptible to take on or accept increased risks.

b. When dealing with high UAI cultures, companies should expand the idea of risk management. For example, companies could use risk management to provide a competitive advantage instead of thinking of it as a compulsory measure to protect against only catastrophic and other general risks, which are covered by insurance policies.

c. Cultures with a low UAI score generally dislike rigid rules and laws. Policies and procedures are required, but your quest to reduce risks may be better served by keeping the attention focused on the specific risks and less on implementing new rules and regulations.

5. Risk reporting and monitoring

Creative methods of risk reporting and monitoring should be incorporated depending on the culture's UAI and PDI score. Embedding

risk management may be an excellent complement to a centralized risk management approach if it is implemented effectively.

Part 2

Chairil Tarunajaya

Partner of Risk Consulting Services
PwC SEAC & Indonesia

Recently, people are in the tendency of changing their habits. For example: at a music concert in 2005, most people only listen to the music and exclamation-appeal with their friends. Meanwhile in 2016, people always take a picture or record the music concert in their smartphones. In the span of 11 years, you can see the differences on what people do.

In the tendency of sharing information, people share what they are doing and where they are. The changes will always be there. It can be opportunities or threats depending on the readiness of organizations.

Organizations should be ready to face the changes. If you are ready, the change will be an opportunity. Otherwise, if you are not ready, the change will be a threat.

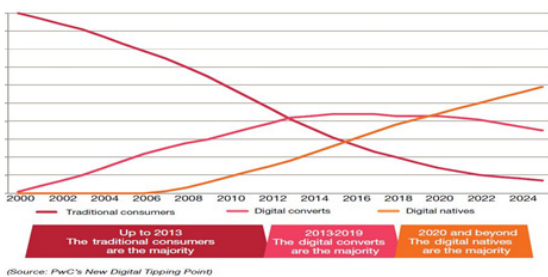


Figure 1. Dominating Customer/Demographic in Each Era

Previously, Mr. Chairil Tarunajaya has discussed the changing behaviours of people, but evidently, it also impacted the behaviour

of customers in the market and employees in the workplace. Among these people, there is a group of people (customers and employees) who are more tech-savvy than any other demographics, which is called the digital natives. Digital natives are consumers and employees born into a culture of digital technology.

Figure 1 is the result from PwC’s survey. Figure 1 shows the majority demographic of customers from 2000 until 2024. In 2000 until 2013, the traditional customers are the majority demographic. In 2013-2019, the digital converts are the majority demographic. In 2020 and beyond the digital natives are the majority demographic.

So, from now, many organizations have been changing their behaviours. They change to be more digital, not only because the majority demographic is the digital natives, but also the requisition of competition.

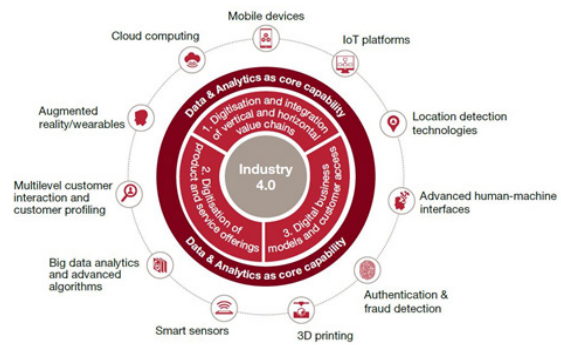


Figure 2. The Now Trending Topic of Digitals

The PwC’s 2016 Global Industry 4.0 Survey tries to capture the now trending topic of digital. From the figure 2, you can see the mobile devices, Internet of Things (IoT) platforms, big data analytics and advanced algorithms, cloud computing, and others are the trending topic of digital now.

In the discussion about digital, there are some areas that were affected by digital because of changing the digital new trend such as:

1. Vertical and horizontal integration value chains;
2. Product and service offerings; and
3. Digital business model and customer access.

On the other hand, data analytics become a core capability that organization must do in managing cyber risk.

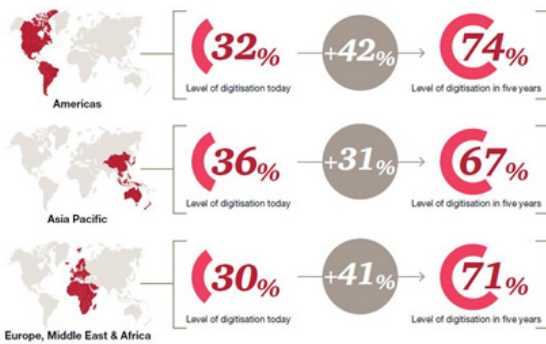


Figure 3. Level of Digitization Companies for the Next Five Years in Each Region

Now is the era when the data can be transferred to many people in many devices. The process of converting information into a digital form with suitable electronics devices is called digitization. A lot of companies are expecting to dramatically increase their digitization over the next five years.

Figure 3 shows the digitization over the next 5 years across regions. The level of digitization today means that in their regions, the company's overall have converted their information into digital forms as much as 32%, 36%, and 30%.

By the next 5 years, America who has 32% level of digitization today will be increased by 42% ; Asia Pacific will be increased by 31%; and Europe, Middle East, and Africa will be increased by 41%.

In the next 5 years, companies around the world will convert their information into digital forms up to 74%, 67%, and 71% which means most of their information will be in the digital form.

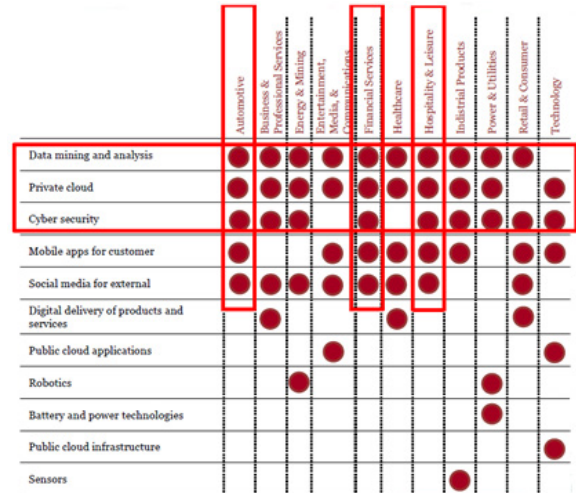


Figure 4. The Highest Strategic Importance of Technologies

In other surveys, PwC tried to capture which of the technologies in the figure 4 will be the highest strategic importance of the organizations over the next 3 to 5 years. Data mining, private cloud, and cyber security are the top 3 technologies that affect the strategic of organization. Automotive, financial services, and hospitality & leisure are the industries that most affected the highest strategic importance of digital.



Lack of digital culture and training



Note: Included as one of three possible responses

Figure 5. The Biggest Challenges Building Digital Operations Capabilities

To make changes towards digitization, the company faces the biggest challenge especially the lack of digital culture and training. PwC's survey indicated 50% of the respondents still concerned about the lack of digital culture and training in their organizations.

PwC's survey also shows the biggest challenges or inhibitors for building digital operations capabilities in the organization. Lack of clear digital operations vision and support/leadership from top management, unclear economic benefit and digital investments, and high financial investment requirements are the top 3 biggest challenges that organizations must face. The other biggest challenges can be found at the figure 5.



Figure 6. The Technologies to Address Threats and Create Value

Many companies or organizations try to address the threats of digitization by using technologies. Figure 6 shows the data about how many companies using those technologies to address threats and create value. 63% of companies are running the IT function in the cloud, 62% of companies are using managed security service for cyber security, 53% of companies are using open-source software, and so on.



Figure 7. Cyber Security Risk

Many companies may fail in their security because they are still using the same old strategy to make them unable to be breached.

However, the priority today is not about how to make an organization unbreachable, but how can one detects and defends it.

PwC shared 6 things about cyber security risk (as shown in figure 7). Figure 7 shows that: (1) You cannot secure everything, which means you must set the right priorities; (2) You should talk about before the breaches occurred, not after it happened; (3) If you are transferring your risks, it does not mean all of you risks are transferred. You cannot assume that you have no risks if you transfer your risks to other parties such as insurance or outsource companies.

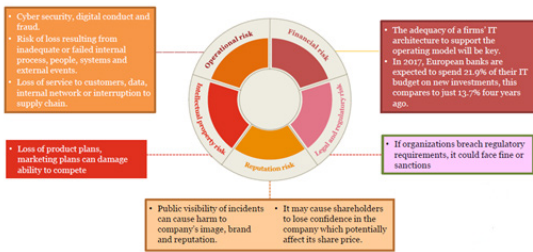


Figure 8. Impact of Cyber Threats

On the other hand, cyber threats can lead to a wide variety of risks. For example, cyber-attacks can cause reputation risk. When incidents happen, it can harm a company's image, brand, reputation, and also share price.

Other example is operational risk; just imagine if you are a stock exchange company. When a server is hacked at the prime trading time, can the daily operations still running as usual? It's just some cases from cyber threats and there are many more impact arising from cyber threats such as in figure 8.



Figure 9. Establishing Effective Risk Culture

The lack of digital culture is the one of the biggest challenges that organizations must face. Organizations need the digital culture to apply many of strategy that needs digital technologies. On the other hand, when you are running your business, there are also risks inherent to every activity of your business. Therefore, you cannot only apply the digital culture in many strategies.

Organizations need risk culture as well. Risk culture can be driving your awareness to be more careful in every decision-making and make you more successful in risk management implementation. If you are going to apply the effective risk culture, there are some requirements such as 6 multidiscipline approaches / building blocks (see figure 9).

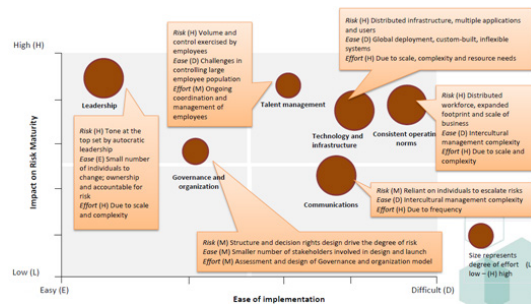


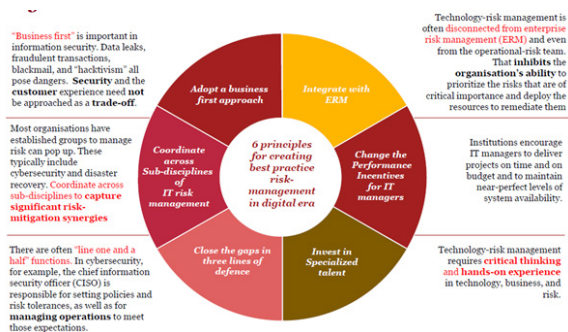
Figure 10. Building Blocks in the Implementation and Risk Maturity

Figure 10 shows the easy way to boost an organization's risk maturity based on previous 6 building blocks. Vertical axis describes how high each building blocks impact on risk maturity, the higher it is, the higher the impact. Horizontal axis describes how difficult each building blocks to implement in an organization, the further to the right, the more difficult it is to implement.

The result says that leadership is the building blocks which are easy to implement and have the higher impact on risk maturity. However, this is also a problematic matter for a lot of organizations because some of their leaders are still in the age of digital converts, not digital natives.

Adopting a "business first" approach means the organizations need to make sure, whether they understand what is the most valuable assets in their organization or not. Most of organizations think that valuable assets are not only about fix asset anymore, it is about the customer data and their privacy.

In other cases, technology-risk management is often disconnected both of ERM and operational-risk team. Investing in specialized talents means technology-risk management requires critical thinking and hands-on experience in technology, business, and risk. People who does not have specialized talents should not be invested otherwise it will become a waste of money.



Written by: **Fransiskus Bobby Wijaya**

Figure 11. Principles for Creating Best Practice Risk Management in the Digital Era

There are 6 principles (see figure 11) for creating risk management best practices in the digital era. Adopt a "business first" approach, coordinates across sub-disciplines of IT risk management, closes the gaps in three lines of defence, invests in specialized talents, changes the performance incentives for IT managers, and integrates with ERM (Enterprise Risk Management).

CONCLUSION

Human factors are the individual, group, and organizational factors which influence the behaviour of people and the work environment in a way which can affect achievement of objectives. Meanwhile, culture is obtained from environmental learning. Hence, culture can be created or affected by human factors.

Human behaviours always change over time as the technology advances. According to PwC's surveys, majority of the demographic changed from digital converts to digital natives. To apply many things about digital, you need digital culture to comply with your organization.

Additionally, you should remember that risks are always inherent in every step on your decisions. In managing risks, human factors play important roles as well. Nevertheless, culture is important on risk management because it influences the effectiveness of managing risk in organizations. While on the other hand, human factors could be the biggest challenge to build risk culture.

MANAGING COMPLIANCE AND RISKS IN DIGITAL BUSINESS ENVIRONMENT



BALI
ERM
2016

Managing Compliance and Risks in Digital Business Environment

Presented by:

Gordon Song

Head of Group Risk & Internal Audit Lazada Singapore

Ly Xuan Thu

Senior Expert Risk Management at IFC World Bank Vietnam

Hosted by:

Alan Simmonds

Key Contributor to COBIT 5 ISACA,
Board Member of ERMA, United Kingdom

This session talked about managing compliance and risks in the emerging digital business environment. In this session, the presentation were divided into two parts.

The first presentation was explained by Mr. Gordon Song, Head of Group Risk & Internal Audit Lazada Singapore. Mr. Gordon Song mainly talked about managing technology risks in the digital business environment.

The second part was explained by Mrs. Ly Xuan Thu, Senior Expert Risk Management at IFC World Bank Vietnam. Mrs. Ly Xuan Thu shared her view on the topic of managing the compliance risks in this emerging digital business environment.

Part 1 Gordon Song

Head of Group Risk & Internal Audit
Lazada Singapore

In this digital era, technology has become more and more important. As we all know, almost everybody is online nowadays. Thus, managing technology risks in this era becomes more challenging for every industry, especially for the ones that are running on the particular digital-based business area. As one of digital-based business industries, e-commerce businesses have to face technology risk as one of its biggest challenges.

Lazada is one of the subsidiaries of Alibaba Group that runs in the e-commerce industry. Alibaba Group is one of the largest e-commerce companies in the world. Lazada, as the subsidiaries of Alibaba Group, is also considered as one of biggest e-commerce retailers in South East Asia.



Figure 1. Lazada Ecosystem

In running their business, Lazada aims to become the online destination site across South East Asia for buyers and sellers. In South East Asia, Lazada reaches \$1.1 billion annual GMV and has approximately 8 million customers. There are also around 30,500 active seller partners cooperating with Lazada.

Figure 1 shows the Lazada business ecosystem explained by Mr. Gordon Song. Lazada regularly connect with their partners (buyers and sellers) through some platforms that make transactions become easier.

From the figure, we can also see that Lazada has its own logistics enabler, payment solutions, scalable seller solutions, and assortment and category strategy. Lazada provides a one stop end-to-end shopping and selling platform for both buyers and sellers.

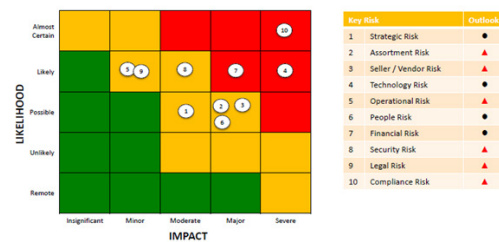


Figure 2. Lazada Risk Profile

Doing business in such tech sector, Lazada obviously has to face a lot of risks. Figure 2 shows us the top 10 risks in the risk profile of Lazada. From the figure, it can be seen that not all of the risks that Lazada face is about the technology risk.

Technology and security risk only represent 2 risks that Lazada has. Thus, the tech companies actually do not only face the technology-related risks, but there are also some other risks that need to be considered. As shown in the picture, compliance risk is the biggest risk that should be faced by the company.

Compliance risk is related to the regulation of the e-commerce industry, which every e-commerce companies should comply to.

The other top risks in tech companies are the technology and security risk itself. From figure 2, it can also be seen that financial risk has scored high.

According to the AON's global risk management survey, 3 of top 20 risks that companies face are closely related to technology. Those three risks are business interruption, computer crime/hacking, and technology/system failure. Besides that, many of the rest of those top risks are also caused by technology risk (e.g. supply chain failure) or direct consequences (e.g. damage to reputation).

In this session, Mr. Gordon Song also showed the 2015 Global Cyber Impact Report (Ponemon Institute) which says that 37% of surveyed companies have had significant security breaches in the last one year, averaging US \$2.1 million. Nine out of 10 respondents have validated the assessment that cyber risk is still not fully understood. From this report, it can be seen that technology risk has not been handled well by many companies.

Considering those technology risks, the main question would be "is technology risk a cancer or heart attack?" This terminology represents that whether technology risks are hidden and gradually endanger a company or are causing instant death for the company.

According to Mr. Gordon Song, technology risk can actually be both, either a cancer or a heart attack. If companies don't invest in some infrastructures in order to manage the technology risk, it would become a cancer for that company. It will be hidden and the company won't realize it until it comes up and bring fatal impacts for the company.

Furthermore, in several cases, technology risk can cause an instant death for the company. The sudden and great impact of that technology risk could make the company down instantly. Thus, every companies should be aware of these two technology risk characteristics and be prepared for it.

In this session, Mr. Gordon Song also shared Lazada's top 5 technology risk drivers, which include big data, mobile and social media, cloud computing, cyber security, and the internet of things (IoT). Explanations of each driver are as follow:

1. Big data

Every day, Lazada manages a huge number of transactions. Approximately, Lazada got 5 million visits every single day. From that statement, it can be seen how big the data that has to be handled by Lazada every day.

Nevertheless, the terminology of "big" data can be relative for each industry or the size of company. Small companies can say that 1000 transactions is a big issue, but bigger companies will have different perspectives.

Big data is something that companies should handle and manage in order to ensure that their business can run well, especially for the company that runs its business in the digital platform like Lazada. Furthermore, big data can be a big problem if it is not managed effectively.

So, what is the consideration of risk among big data? The first matter is about how the companies store the data. There are a lot of facilities that companies can use to store the data. The company should make decision about what kind of storage that companies want to use. The choice, for example, comes up from whether they want to store in cloud or in-house.

Each decision has its own risk that should be taken. Data stored in cloud has a bigger threat regarding the security and the confidentiality issue. Also, investing on in-house data storage has to be well calculated from the cost perspective.

The second issue is the access to data. It's about the security and privacy. In the good hand, data can absolutely help the entire process of organization and also be used in making strategic planning. However, imagine if the data fall into the wrong hand. Security breach is one of the main problems of big data, as it will obviously bring great impact to the companies.

The third issue is about skillset. Skillset talks about the capability of company to use their data. In some cases, skillset also determines the infrastructure that has to be owned by a company. For example, companies with low-skills employees do not need to have a too complicated infrastructure. All of these capabilities will help people in the company to use the big data in their company's infrastructure.

The last issue is to ensure data quality and usefulness. The company should determine what kind of data that they needed. Also, the company should decide how to get those data with the expected quality. This can be considered in determining how much investment do the companies need.

2. Mobile and social media

Using mobile and social media improperly is actually very costly for companies. Every company should have a proper strategy to face these threats. 'Bring Your Own Device' is one way to prevent data losses and encourage more privacy in a company.

However, we still have to consider about the efficiency and business need in order to make BYOD policy. Regarding mobile and social media issues, the biggest threat comes from the employees' devices. They can be used by the outsider/hacker to penetrate the company's network. Thus, every employee in the company should know about this issue and act carefully.

The next point is about community management. Sometimes, the boundary between private and official affairs in social media is blurred. Some employees sometimes post a private statement under the name of the company. This can be harmful and costly for the company.

Considering all of these things, the question here is: how to regulate/audit social media? Is it ethical for us to make such policy, or is it better if we just let it flow since it is called as "social"?

3. Cloud computing

Cloud computing offers a lot of benefit, especially to reduce cost. However, there are several considerations regarding cloud computing.

The first one is about control and ownership of historical data. How much control and ownership do companies own over the big data, especially when the data are needed to access the data for audit, comply, or legal reasons?

The second thing is about the dependency to cloud service provider. Too much dependency in a cloud service provider will obviously endanger the company. The third thing that companies should consider is about contractual and terms of using that cloud service.

4. Cyber security and data privacy

In managing technology risk, every company has to be concerned with cyber security trends and regulations. Cyber world evolves rapidly, so that companies should keep their pace with criminals and the lawmakers so that they can be more prepared in managing the technology issues.

Regarding this issue, people often become the 'weakest link' in managing technology risk. They maybe have not realized the danger of technology risk, while it's actually very harmful for the organization.

There is also an option of 'outsourcing' security operations and surveillance. However, companies should consider the risks (e.g. data privacy or dependency of the company) that might arise from taking this option.

5. Internet of Things

Internet of Things (IoT) refers to the connection of the devices (other than usual device like smartphone or computer) to the Internet. IoT can be defined as a network of internet-connected objects which are able to collect and exchange data using embedded sensors.

With this highly connected and accessible nature, cyber security issues become more and more important. Cyber security can be more vulnerable than ever because everything now can be connected to the internet.

The whole world that is entirely connected brings consequences to the privacy matters. There seems to be no more privacy nowadays due to the internet. The indefinite data storage (everything from credit information to intimate personal details) also brings an indefinite privacy impact.

Besides that, legal and ethical conundrums across IoT of all industries also increase liability exposure to business. This is the real fact that we should face and consider in our business environment.

In the last section of the session, Mr. Gordon Song explained some lessons that can be learned about managing technology risk. Those lessons are:

1. Technology as a 'culture'

Forming technology as the culture of the company can be a challenging task. However, considering the rapid developing digital era, this culture should be created in a company. One key of creating this culture is by making the same tone from the top. Leadership is the easiest way to implement the technology as a culture in the company.

2. Involve business stakeholders

Technology is not only for IT folks; it is not only driven by the IT department. Technology issues can also affect other stakeholders. Thus, the involvement of business stakeholders should be considered.

3. Quality and security by design

A company should design the quality and security of the technology in order to make sure that the company deals with the problem with the right infrastructure. It is better to get it right from the beginning. Therefore, companies should make the right design from the beginning and try not to be surprised when encountering any technology issues in the ongoing business process.

4. Outsourcing

In making outsourcing decision, a company should make a comprehensive evaluation and involve the right stakeholders. Outsourcing

decision is highly driven by cost. The issue regarding data privacy and dependency to the service provider should also be considered.

5. Resiliency

The company should always be prepared for failure. Managing technology risk is not about when or how the company gets hit, it is about how prepared the company is to face the technology risk and bear the effect of the events.

Part 2

Ly Xuan Thu

Senior Expert Risk Management at IFC World Bank Vietnam

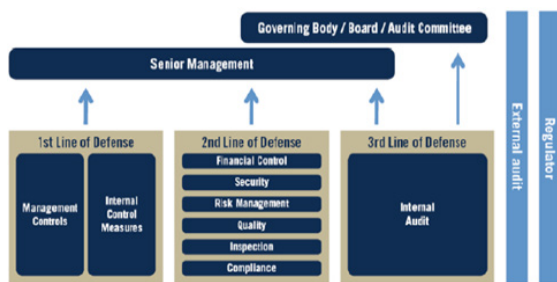
In this session, Mrs. Ly Xuan Thu started by explaining the three lines of defense concept. After that, she continued to explain the interrelation between ERM and compliance.

In the last part, this session talked about the future of ERM and compliance that may happen in this developing digital era.

The first line of defense consists of people that face the risks directly. These people are also called as the risk owner. In the second line, risk managers or risk department take into account. Compliance department are also included in this second line of defense. The third line of defense is done by the internal auditor.

The first line of defense is the responsibility of the operation management. As mentioned above, the first line will be done by the risk owners/managers in the operation activities. The second line of defense is implemented in order to create the risk control and compliance. People in the second line usually have a limited independency and should report primarily to the management.

Finally, the third line of defense talks about the risk assurance. It is the responsibility of the Internal Audit that has the greater independency than the second line of defense. People in the third line of defense should report to the governing body.



Adapted from ECII/EFERMA Guidance on the 8th EU Company Law Directive, article 41

Figure 1. The Three Lines of Defense Model

The three lines of defense seem to be important in managing risks in the digital era. Figure 1 shows the three lines of defense model.

	Responsibility	Function	Key activities
Board CEO Senior Management Provide oversight of the 3 lines of defense	First line of defense	Strategy, performance and risk management	Business units, countries and support units. Identification and management of risk in the business
	Second line of defense	Policy and monitoring	Corporate oversight and control functions. Framework, risk oversight and reporting
	Third line of defense	Independence assurance	Group audit. Independent challenge and review of adequacy and effectiveness of processes and controls

Figure 2. The Three Lines of Defense Model in DBS

In this session, Mrs. Ly Xuan Thu explained the example of implementation of the three lines of defense model by showing the DBS Bank Corporate Governance. Figure 2 shows the DBS corporate governance that implements the three lines of defense.

It can be seen from this picture that the first line of defense (which is performed by risk owners) have the responsibility in developing some business strategies and also perform risk identification. As the risk owner, these people should know the most about the risks faced by the company.

The second line of defense, which is performed by the risk management and compliance, have the responsibility of making risk management policy and monitoring. Considering that, these people have the key activities to oversight the risk and to report to the management.

The third line of defense in DBS is performed by internal auditor that is responsible for independence assurance. The people in this third line of defense have the key activities to perform the review of adequacy and effectiveness of processes and controls.

After explaining the three lines of defense concept, Mrs. Ly Xuan Thu continued to explain about the interrelation between ERM and compliance. Compliance department in a company is included in the second line of defense. This department also declared as the owner of compliance risks.

One of the most important functions of compliance department, which related to the ERM, is to perform the compliance risk assessment. The company should ensure that everyone in compliance function can collaborate and work effectively in forming compliance risk assessment.

Furthermore, compliance function communicates the compliance risk assessment result with risk managers and gets their inputs. Ultimately, the final result will be incorporated into corporate risk profile.

Besides compliance function, ERM function also takes a role in the second line of defense, especially as the facilitator of the risk management process implementation (holistic approach).

ERM function is not the risk owner of every risks faced by the company; instead, it is the risk facilitator or risk owner of the risk management implemented by the company. This function also combines risk assessment result from various risk owners and develops a corporate risk profile by using developed risk categories.

ERM uses a compliance risk assessment performed by compliance department in order to develop a corporate risk profile. Compliance risk assessment is actually one of some risk assessments that company performs. Nevertheless, this assessment will be important for a company in developing their risk profile as a whole. Compliance function is the part of ERM in one company.

ERM and compliance function seem to take more important role in a company recently. Based on EY sources, spending for risk management has increased significantly in the last decade due to the expansion of regulatory compliance requirements.

The number of risk functions has also increased to keep up with these compliance requirements (73% of companies have seven or more separate risk functions). This increase of risk functions without a clear task and responsibility might bring inefficiency to the company (e.g. redundancy).

The coverage and focus of those risk functions has become increasingly difficult to manage. As the result, the companies want to improve risk coverage while balancing cost and value.



Figure 3. Considerations for Balancing Risk, Cost, and Value

Figure 3 shows the considerations for company to balance their risk, cost, and value. Those questions shown up in the figure will help us to perform the efficient risk management based on cost benefit consideration. This is important for the company so that ERM can become a function that will create value for the company instead of becoming a costly department with no value creation at all.

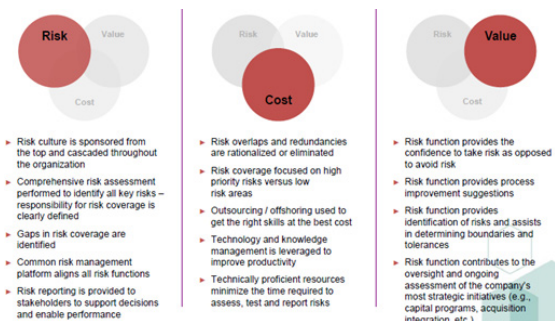


Figure 4. Leading Practice for Balancing Risk, Cost, and Value

In this presentation, Mrs. Ly Xuan Thu also explained about the leading practice of balancing risk, cost, and value. This leading practice can be used by a company as the guideline to see whether the implementation of risk management has been done efficiently or not.

Figure 4 shows the leading practice of balancing risk, cost, and value. In the leading practice, the risk culture should be sponsored from the top and cascaded throughout the organization.

The company should also perform a comprehensive risk assessment to identify all key risks. Considering the cost side, company could leverage the technology and knowledge management to improve the productivity.

Besides that, the risk overlaps and redundancies should be eliminated. As risk management should create value for the organization, the risk function should provide the confidence to take risk as opposed to avoid risk. Risk function should also provide the identification of risks and assist in determining boundaries and tolerances.

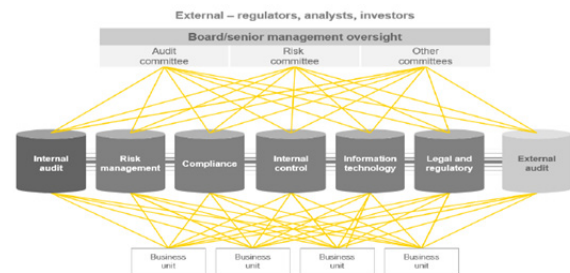


Figure 5. The Current State of Risk Management

Talking about the future of risk, Mrs. Ly Xuan Thu compared the current state of risk governance with the future conditions. Figure 5 explains the current state of risk governance. Each board/senior management oversight (audit committee, risk committee, and other committees) has a link to every function in the company. Also, every function in the company is linked to every business unit in that company.

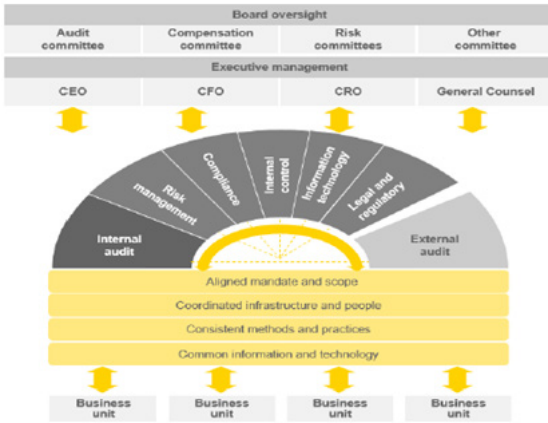


Figure 6. The Future of Risk Governance

While figure 5 shows us the current state, figure 6 shows the future of risk governance that company may implement. On figure 6, we can see that board oversight is not directly connected to the functions of the company.

There are executive management (CEO, CFO, CRO, and general counsel) between the board oversight and the functions. There also some notes that company should consider in linking each function to each business units.

Every company should be able to achieve the effective and efficient ERM in their ongoing business. Figure 7 shows the example of the diagnostic form that can be used to assess the maturity level of ERM implemented in the company.

ERM Maturity level can be measured in some focus area, such as risk governance; strategic risk management; business level risk management; mandate and scope; infrastructure and people; methods and practice; and information and technology.

Each focus area should undergo the phases from the basic phase to the leading phase. Every company that has achieved the leading phases will be able to implement the ERM effectively and efficiently. In the end, all of these achievements will result in improved business performance of the company.

In managing risks in the digital era, a company should also consider the vision of compliance that should be achieved in the future as it could bring better performance for the company. The compliance function is the risk owner of the compliance risk who has to perform the compliance risk assessment.

Other than that, compliance function should also review the risk assessment result done by the first line of defense. Facing the digital world, compliance function seems to be involved as the strategic partner in the nowadays world where many new regulations are arising.

Focus area	Basic	Evolving	Established	Advanced	Leading
Risk governance	Risk management efforts are ad-hoc and risk functions report independently	-	-	-	Risk culture is sponsored from the top and cascades throughout the organization to coordinate risk efforts and enable value creation
Strategic risk management	Non-business risk awareness and objectives	-	-	-	Risk management fully integrated into business planning and performance management with value, cost and risk considerations aligned to objectives
Business level risk management	Ad-hoc risk assessment and monitoring	-	-	-	Risk assessment, monitoring and measurement embedded into ongoing management processes with risk adjusted performance metrics
Mandate and scope	Risk function objectives are stand alone and may not be aligned to business objectives	-	-	-	Risk functions aligned and coordinated to effectively cover risk, enable value creation and support cost reduction
Infrastructure and people	Capabilities of risk functions do not support key risk areas or focus on improvement activities	-	-	-	Risk functions are enabled to offer improved services and are integral to value creation and cost reduction efforts
Methods and practices	Focus is primarily on financial and compliance risks - emerging methods to address risks	-	-	-	Comprehensive risk management approach by finding - consistent method for ongoing identification, assessment, monitoring and measurement of risk
Information and technology	Risk functions use basic technology with limited efficiency and leverage	-	-	-	Risk functions use enabling technologies to create leverage and apply information management and data analytics techniques to drive efficiency and value

Figure 7. Risk Maturity Self Diagnostic

Regarding the structure and reporting line, head of compliance reports to General Counsel or CRO. Head of Compliance also reports directly to the board or board committee. Regarding the compliance in the future, companies are suggested to establish executive risk and compliance committee to deal with daily risks and compliance issues led by the CEO as a chairman of the committee.

At the highest level, the strategic vision of compliance should be defined and set by the board in formal terms of reference. The role of compliance should also take the lead in identifying and managing the significant regulatory compliance risks to which the business is exposed. That role can be seen in these activities:

- Designing and supporting a regulatory risk framework for the business
- Supporting and challenging business line management regarding the completeness and accuracy of compliance risk management activities, including identification and measurement
- Providing advice to business units on regulatory obligations and the creation and implementation of regulatory compliant policies and procedures
- Monitoring the organization's compliance with relevant laws, regulations, and internal risk policies
- Reporting on compliance matters that warrant the attention of senior executives.

*Written by: **Reynaldi Hartanto***

CONCLUSION

The rapid changes and development in this digital era seem to create more challenging risks into our business environment. Technology risk is one of the biggest risks that arise in this developing digital era. Thus, managing this technology risk becomes more and more important these days.

Companies should consider many factors regarding technology issues, such as the data privacy, cyber security, cloud computing, mobile, and social media. They should also be more careful in using the IT infrastructure.

The development of digital era also makes new regulations arise. This could create new requirements for the companies to be complied with. Thus, managing compliance risks also become an important issue that should be considered in this digital era.

ERM and compliance function are actually strongly related. The compliance function especially needs to collaborate effectively with ERM in providing the compliance risk assessment for creating the right risk profile of the company. Bringing the right risk governance structure will also help the organization to comply and achieve their strategic objectives.

MANAGING RISKS IN HIGH IMPACT MEGA PROJECT INFRASTRUCTURE:

A Multidimensional Risk Management in
Modern Era



BALI
ERM
2016

Managing Risks in High Impact Mega Project Infrastructure: A Multidimensional Risk Management in Modern Era

Presented by:

Dr. David Hancock

Deputy Director of Construction in Cabinet Office Major
Projects Authority United Kingdom

Hosted by:

Hotbonar Sinaga, CERG

Former CEO of Jamsostek (Social Insurance of Workers);
Industry Expert Advisory Board Member of CRMS Indonesia

Project management and change management are the tools to support the implementation of changes. When the United Kingdom decided to leave the EU, there were many changes happening in the UK which also affect PLC (Public Limited Company). Therefore, projects have an important role in this transition period.

The roles of projects are: Major vehicle for delivery of policy objectives; Drive efficiency by reducing spend; Enable successful change management; and introducing structure, governance and best practice.

In the UK, every project that has been working out is based on Government Major Projects Portfolio (GMPP). The GMPP consists of the largest, most innovative and highest risk projects and programs in the government. The GMPP is a selection of Major Programmes and Projects that are being

assured by The Major Projects Authority (MPA) which is now known as IPA (Infrastructure & Projects Authority).

IPA is a central authority to achieve firmer control of Government's Major Projects both at the individual and the portfolio level. It aims to significantly improve the success rate of Major Projects across the Central Government.

The objective of selecting the projects is to deliver the right projects to achieve policy intent and strategic benefit. These projects vary from high cost to high politically sensitivity and are all highly complex. Their objectives are diverse and can range from the building of new submarines, readiness for pandemic diseases, to the transformation of the delivery of welfare benefits.

As those projects are high cost and highly important, the IPA publish an annual report which last published on 7 July 2016. The report is published as per Chief Officer Business Plan and Civil Service Reform Plan, which also includes combined GMPP, RAG (Red, Amber, Green) and whole life cost, MPA (Major Project Authority) progresses and examples.

The projects that have been chosen need to be prioritized and delivered properly. There are 5 key priorities that need to be done:

1. Challenge, assure, and support

Continue to provide 'challenge' function to departments in the UK through timely and insightful assurance ahead of approval points but also offer bespoke, specialist support and advice to help maintain project delivery momentum.

2. Create project based controls through alignment

Collaborate with Cabinet Office and HM Treasury (Her Majesty's Treasury) to develop better alignment, so that funding approvals, assurance and milestone checkpoints are completed as smoothly as possible.

3. Strategic prioritization

Facilitate and embed a process that supports senior departmental decision making on project portfolios, based on resourcing, constraints, risks and interdependencies.

4. Building long term capability

Ensure all departmental project teams have the talent, skills, and capability needed to successfully deliver projects, enrolling project leaders onto the MPLA (Major Projects Leadership Academy) and Project Leadership Programme.

5. Building the profession

Define the structure of the profession, including departmental 'head of profession' role, to encourage the creation of Project Leaders, with personal project delivery accountability balanced with greater autonomy to decide how best to deliver.

UK Projects Development

On 30 September 2015, the GMPP contained 143 major projects representing a £405 billion investment over the next 25 years that will improve the UK's infrastructure, transform public services and safeguard national security. The government is also carrying out thousands of other projects, and the improvements that the IPA is working to introduce with the departments will have benefits well beyond the GMPP.

Major projects on the GMPP are those where the project needs HM Treasury approval, either because the proposed budget exceeds a department's delegated authority level or because the project is novel, contentious, potentially sets a precedent or requires primary legislation.

These projects vary greatly in size and scope as illustrated by the case studies in this report which describe the Thames Tideway Tunnel (DEFRA), the National Proton Beam Therapy Service Development Programme (Department of Health), and Cross rail (Department for Transport).

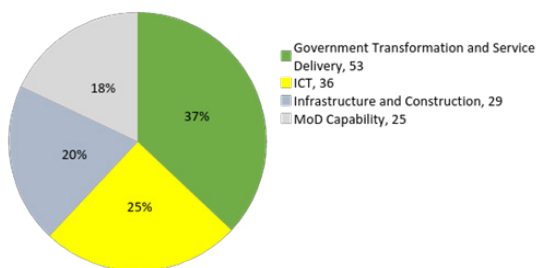


Figure 1. Number of Projects by Category

There are four types of project in the portfolio (see Figure 1):

1. Government transformation and service delivery projects are the largest single category of projects by number in the portfolio. They can be the most difficult to get right due to their complex and often challenging nature. Transformation projects are often unique and therefore do not benefit from lessons learnt to the same extent. An example of a transformation project is the Department for Work & Pensions' (DWP) New State Pension Project to implement the Pensions Act 2014 by introducing a simple flat-rated state pension.

2. ICT projects aim to restructure legacy IT contracts and introduce flexible IT systems more aligned to the future. These projects make up 25% of the total number of projects on the GMPP but less than 5% of its whole life cost. One example is the Columbus Programs, through which HMRC is replacing the government's largest IT contract.

3. Infrastructure and construction projects include improving and maintaining the UK's transport, energy, sewage and water systems, and constructions of new public buildings. These high-investment projects are vital to the nation's economic development and prosperity. Although they make up just 20% of projects by number, they represent the largest share of whole life cost at 43%, and also have the largest median project cost at £1.9bn. An example is the Department for Transport's (DFT) £15bn Crossrail Programme, which will start delivering a new rail capacity to London in 2017 which is scheduled to complete at the end of 2018.

4. Defense capability projects are vital to the effective operation of the Armed Forces. This is the smallest category in terms of number of individual projects but second highest in terms of whole life cost, representing a significant investment to maintain our national security. An example is the Air Seeker Programme to provide the Royal Air Force with three specialist surveillance aircraft that use advanced sensor technology to gather data and intelligence to support forces in the air and on the ground. The second aircraft was delivered ahead of schedule and the program is on track to complete by the end of 2017.

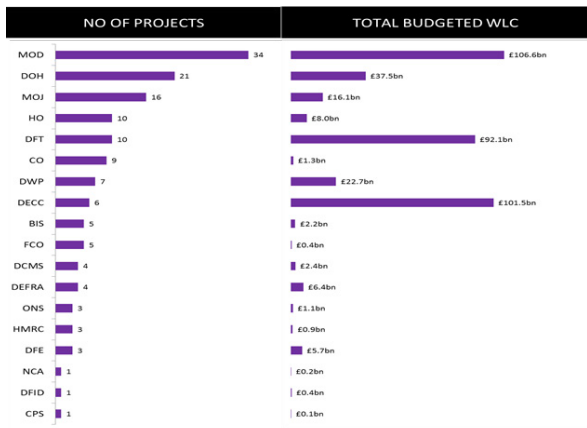


Figure 2. Total Number of Projects and Whole Life Cost by Department

The portfolio from September 2015 included projects from 18 government departments (see Figure 2). Unchanged from last year, the MOD has both the largest whole life cost and the largest number of projects. These are mostly defense equipment projects, while some are transformation projects.

The New Employment Model aims to deliver a simpler, better and fairer system of pay for the Armed Forces, while the Army Basing Programme will bring back all units from Germany by 2020.

DFT projects (10) represent almost a quarter of the total whole life cost of the GMPP, and include the highest number of infrastructure projects. These take the longest, need the highest levels of public investment, and often involve working in partnership with private sector finance. For instance, the Thameslink Programme will deliver improved connections, more reliable journeys, better stations and new trains to London and the South East by 2018.

The DOH has almost 15% (21 out of 143) of the projects in the portfolio. These range from ICT projects such as the Health & Social Care Network, which will provide a reliable, flexible

and more efficient way for health and care organizations to access and exchange electronic information, to infrastructure projects like Public Health England’s Science Hub, which will create a center of excellence for research, health improvement and protection, to service delivery projects like the Childhood Flu Immunisation Programme.

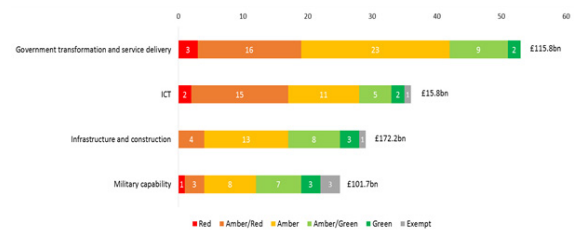


Figure 3. DCA Analysis by Project Category

An analysis of Delivery Confidence Assessment (DCAs)¹ by project category (see Figure 3) shows that the majority projects rated red or amber/red are transformation or ICT. This is unsurprising given the relative complexity of these types of projects compared with the others.

Government transformation and service delivery projects can be particularly challenging, typically involving long-term changes in the relationship between the government and the public, and the way in which services are provided.

These reforms may require complex changes to organizational structures and ways of working, the skills required in the government, the nature of commercial relationships with suppliers, and major IT development program. To successfully lead and manage the transformation programs, a different approach from traditional capital programs such as infrastructure is required.

In recognition of the challenging nature of these programs, the IPA has been working closely with number of government departments to develop a better understanding of the key elements that contribute to successful delivery of transformation projects, and how the government can increase the likelihood of their success. A group of senior transformation leaders from various departments has been established to lead this work, supported by experts based in the IPA.

¹ The delivery confidence assessment (DCA) is the IPA's assessment of a project's likelihood of achieving its aims and objectives on time and on budget. It is a five-point scale ranging from green for projects where successful delivery appears highly likely, to red where successful delivery appears likely to be unachievable unless urgent and substantive action is taken. The IPA will normally provide additional support to red and amber/red projects, for instance by providing additional expert support as required, and organizing follow-up assurance reviews to check that the project team is taking the right action. A red rating does not mean that a project cannot be successfully delivered if the right action is taken. It does, however, mean that fundamental aspects of the project need to be addressed promptly.

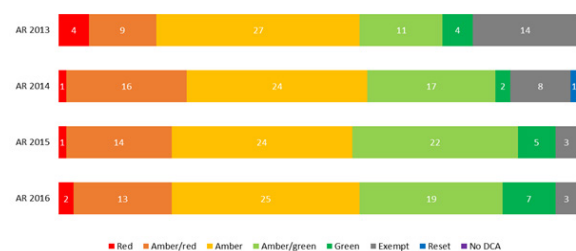


Figure 4. DCA Comparison Each Year

On 30 September 2015, the GMPP included 69 projects that were on it on 30 September 2012 (see Figure 4). Since then, there has

been a large reduction in the number of DCAs exempted from publication, which means that a comparison of the ratings of those projects since 2012 is difficult. However, a comparison between 2015 and 2016 (which have far fewer exemptions) shows that overall the DCAs have not changed significantly.

The continuing presence of red and amber/red projects on the portfolio is an indicator of the level of complexity and risk in these major projects. The DCA of projects tends to fluctuate during their life cycle and those rated red or amber/red do not generally remain so.

It has been predicted that 70% of global population in 2050 will be living in a digitalized cities. This means the UK Government have to prepare the infrastructure that will support the digital cities future.

The UK Government has adopted collaborative working in its Construction Strategy, by requiring that all publicly-funded construction work must be undertaken by using Building Information Modelling (BIM) to Level 2.

This mandate has been set as one measure to help in fulfilling their target of reducing waste in construction by 20%. It is considered that abortive work, discrepancies and mistakes, and inefficiencies in the information supply chain are major contributors to this waste. As the implementation of BIM already achieved level 2 in March 2016, the UK Government announced to commitment to BIM level 3.

The example of projects that UK Government has been doing is the aircraft carrier which can be called as Carrier Enabled Power Projection (CEPP). Basically, it is an airport, so we can imagine it will be a lot of logistics and also

people in one place. It is one of the biggest projects that the UK Government has been working. It involves a massive data in it and needs a lot of collaboration between each work units. Using BIM, it allows them to visualize it.

Risk Management Process

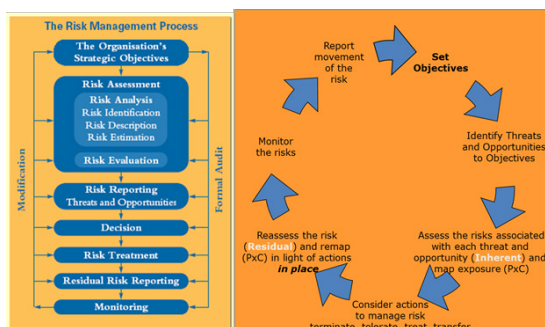


Figure 5. Risk Process

The risk process used in this project is similar to ISO 31000 (see figure 5), with some modification. It is started with organization's objectives establishment and the assessment process. After the assessment process, the next step is risk reporting. After the risk is reported, there decisions about the risk and its treatment are to be made.

With the risk treatment finalized, the organization should then does residual risk reporting. Finally, the last step is monitoring. In every step of risk management process, there are residual audit and modification to make sure that the objectives are achievable.

For CEPP Risk assessment, the UK Government use two approaches which are quantitative and qualitative.

The quantitative approach is an attempt to apply meaningful and objective probabilities, then subsequently consider and quantify the potential of such risks in terms of time, cost and quality (Laxtons guide to risk analysis and management).

The qualitative approach involves the registration of the identified risks by 'experts' in a formal manner using subjective probabilities. There are three key points that need to be considered: Selection of stakeholders is critical to its success; Need to take into consideration Group Dynamics; and also, used to identify Opportunities.



Figure 6. Risk Assessment

Figure 6 shows result of this risk assessment. The UK Government divides risk assessment into 4 groups, there are: Operational / Technical; Commercial / Legal / Finance / Regulatory; Strategic; Behaviour / Culture. The letter size indicates how high the risk is.

Written by: **Belianny Putri**

CONCLUSION

There are many changes happening in the UK after Brexit. Therefore, they used projects as the tools to deliver changes to overcome the changes.

All projects that will be delivered are based on GMPP, and not just any projects can be taken by the UK Government. Each project needs to get the approval from IPA. The objective of project selection is to take the right projects so it can be done right and efficiently.

In 2017, most of the projects that UK Government doing are funded by whole-life cost that will be used by every department. So far, the highest cost is being used by the Government Transformation and Service Delivery departments, as they can be the most difficult to get right because of their complexity and often challenging nature.

Transformation projects are often unique and therefore do not benefit from lessons learnt to the same extent. Other than government transformation and service delivery, ICT is the second category that has the biggest number of projects. This is because of the projection that in 2050, most of the global citizen will live in cities and since the technology will be more advanced, the cities need to be digitalized and supported with the appropriate infrastructures.

The large number of constructions and their complexities require the UK Government to use its capital effectively. Thus, they used BIM as the program to support its constructions. By using BIM, it can help the government to visualize the projects and minimize the costs.

RISK MANAGEMENT IN FAMILY BUSINESS:

Embracing Digital Uncertainty of the Future



BALI
ERM
2016

Risk Management in Family Business: Embracing Digital Uncertainty of the Future

Presented by:

Prof. Enrique Soriano, MBA

ATENEO Graduate School of Business Philippines; Coach for
Many 2nd and 3rd Generation of Family Business in Asia

Shanti L. Poesposoetjipto

Chairwoman of Family Business Networks Indonesia;
Chairwoman of Samudera Group

Hosted by:

Rodolfo Balmater

Independent Non-Executive Director of Sinarmas Land Ltd

There are so many family-owned businesses in the world, especially in South East Asia. In these businesses, the 1st generation is usually the founder, while the 2nd generation becomes the one who grows the business; however, the business comes to its downfall on the 3rd generation due to many factors. Therefore, managing risks in a family business is not an easy task; people need to know how to manage it properly.

Focusing on this issue, ERM Academy asked Prof. Enrique and Mrs. Shanti to share their experience in managing risks in family businesses.

Part 1

Prof. Enrique Soriano, MBA

ATENEO Graduate School of Business
Philippines; Coach for Many 2nd and 3rd
Generation of Family Business in Asia

Background

Why do we passionately allocating family business governance? Compared to other countries, South East Asia has the most number of family businesses. Also, in terms of stress, Indonesia and the Philippines are ranked as number 1 and 2 in the region. One of the stress sources is tax liabilities; however, since there is tax amnesty now, it should not become as an issue anymore.

Furthermore, in family businesses, there are always a lot of escalating conflicts between the family and the business side (e.g. how can you terminate a family member when he/she steals company's money, when he/she steals data and sells it to the competitors, and when there is a conflict of interest?). These conflicts usually happened because families generally use emotion while business is all about accountability and profit. Hence, they are like oil and water.

Additionally, most of the family businesses do not own business and IT governance. This situation is escalating risks whenever there is a transition from the owner-business to sibling-business to cousin-business until it becomes very complex.

Other than that, most of the time, business owners think that they will be able to lead forever only by themselves. For example, in China, there was a rich business owner with

millions of wealth. When he retired, he gave the business to his unprepared son. What happened next is that in only 3 years the business went bankrupt.

Things that can be done in family businesses

According to Prof. Enrique, governance is needed. Business owners have to accept the fact that they cannot lead their business forever; hence they need to implement governance as soon as possible, not when they are about to retire. Procrastinating in doing so could take a business out in only an overnight.

By having governance between the family and business, the chance of arising conflict might be reduced. Also, with good governance, company could reduce costs and improve the bottom-line impact, which eventually could make the business become very efficient. Other than governance, risk management and third non-emotion party are needed in order to reduce them further.

What kind of governance needed for family business? Since we are living in the digital era, such businesses need to focus on the business and IT governance. Prof. Enrique mentioned that family businesses have to upgrade their infrastructure and governance in order to grow. Hence, both of the business and IT governance should be linked.

Moreover, a lack of board oversight for IT activities is dangerous since it will put the firm at risk. Thus, family businesses have to ensure that their IT governance is put into place. For SMEs, the infrastructure should put their IT governance on top of the business governance.

Also, the alignment between IT and business governance has to be very intense; otherwise it is going to end up in a failure.

Biggest challenge

Family businesses' reluctance is their biggest problem. Whether they are doing too well or poorly financially, there is no sense of urgency to integrate IT into their business. Also, changes are too difficult: most family businesses have too many priorities (which mostly are sales) and turnaround issues.

However, IT is not in neither their business plan nor in their budget. This is the basic statement of most family businesses: they do not want to upset their sales, they do not want their customer to be digital ready, and even their own employees aren't digital ready. Most family businesses think that IT people are from another planet: they are unreachable and live in another world.

With this kind of mindset, most family business leaders think that they should just stay where they are. Another thing that could create this kind of mindset is the past experience of failure with IT which make them afraid to do reinvestment.

That kind of situation happens because most of the 1st generation (age 60s-80s) leaders are completely reluctant to IT, while most of the 2nd generation (age 50s) leaders know a little bit about IT (at least they could use email). Only the 3rd generation (age 30s) leaders who are generally more accustomed to IT. Thus, it becomes really difficult in most cases to pursue the business leaders to invest in IT, risk, and governance.

Now that we know about the current situation, what should we do? First of all, Prof. Enrique proposed IT leaders must sit down and discuss how technology can give benefits to their company. After that, IT and business leaders need to formulate a strategic plan together and present it across functional senior management team. From here, the plan must be reviewed and prioritized. Further, senior management must concur and establish the final strategic plan and incorporating all the IT (there must be a champion to pursue this). Finally, the project must be reviewed at least monthly in order to ensure that the plan's implementation is staying on track.

Final word

All of the recommendations will take so much time to do. Therefore, it is a must for family businesses to inspire the implementation of all these investments. Family business leaders have to choose between two priorities: family or business first? If they choose the former, then they can forget about growth. In contrast, if they choose to prioritize business first, then they have to put their family or love in the back.

Part 2

Shanti L. Poesosoetjipto

Chairwoman of Family Business Networks Indonesia; Chairwoman of Samudera Group

According to Mrs. Shanti, one of the key success factors in her family business is that they do not call themselves as a family-run business, but as a family-owned business. This means that the 2nd generation of the family business acts as the owner.

In Indonesia, there is a two-tier management system for family businesses (see figure 1). In this system, there is family at one side, and company at the other side. In the company side, you have two structures which are the Board of Commissioner (BoC) and the Board of Managing Director (BoD).

For the BoC, they are officially appointed by the shareholder and they are in charge of the strategic plan, continuity plan, contingency plan, and the succession plan. Basically, the BoC is responsible to guide the management team. For the BoD, they have the responsibility to lead the business, to prepare a management development plan for succession, and to prepare a business plan.

Also, since this is a model for family business, there is a family council entity. Family council is responsible for governing the family and preparing the family plan, such as: who is going to take what, based on what, what do you want from the business, who can join the business, etc.

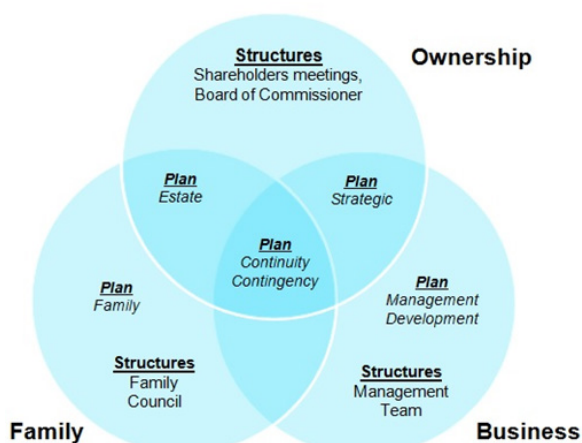


Figure 1. Two-Tier Management System - The Three Circle Model

In family businesses, there are seven territories as shown in figure 2.

- Territory one represents someone who is a part of the family, a part of the owner, but also sits in the management.
- Territory two represents family members who work in the business but do not have any shares or ownership.
- Territory three represents family members who have shares but do not work in the business.
- Territory four represents spouses, in-laws, and children who are not yet working in the business or who have chosen other careers.
- Territory five represents people who are working in the business and also have ownership.
- Territory six represents all non-family executives and employees who are not working in the business.
- Territory seven represents owners and shareholders who are not a part of the family and do not work in the business.

From all of these territories, it is important to realize that usually the conflict and confusion will happen in the place where the circles overlap (territory 1, 2, 3, and 5).

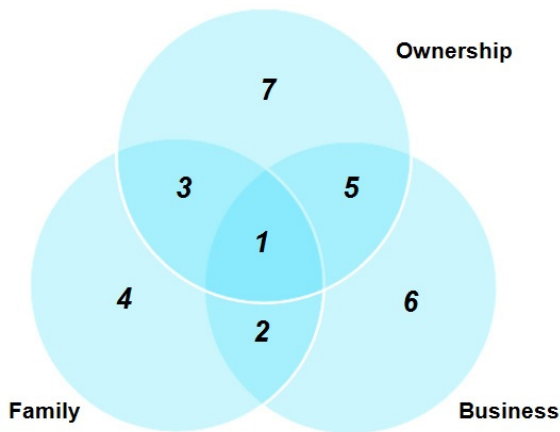


Figure 2. The Seven Territories

Regarding risk management, there are 5 areas in family business that need to be understood (see figure 3). These 5 areas include family governance risks, ownership risks, business management risks, wealth management risks, and succession risks.

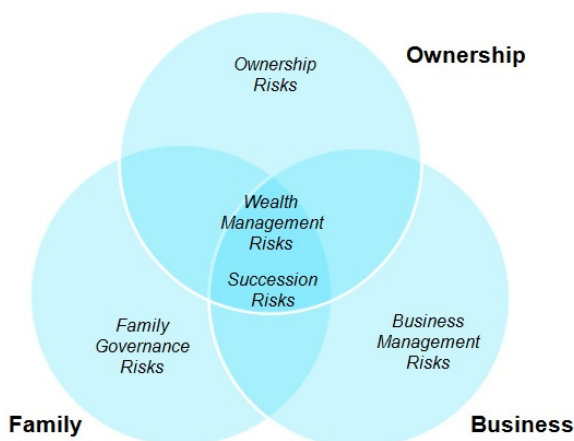


Figure 3. Five Risk Management Area in Family Business

Family governance risks are risks that are related to the family's unity, shared vision, shared values, harmony, and renewed competencies. Some examples of family governance risks are the illness/death of key family figures, major misalignment of family

values, major fight among siblings, rivalry between generations or family branches, and reputation effect.

Ownership risks are risks that are related to the shareholders' composition, agreements, leadership dynamics, unity, dividend policy, and role in the BoD's hiring at the business level. Several examples of ownership risks are the illness/incapacity/death of key family shareholders, divorce, IPO, acquisition/merger, dispersed ownership, lack of skills among members of the ownership group, change in regulatory, and discovery of outdated documents.

Business management risks are risks that are related to the business' vision, strategies, objectives, management and organizations, hiring, and compensations policies. Some examples of business management risks are the change of strategic business orientations, illness/death of key family executive, major change in competitive environment, and acquisition/merger.

Wealth management risks are risks that are related to the family's wealth that encompasses all financial assets, intellectual assets, and social capital. Several examples of wealth management risks are the illness/death of key family constituent, major disagreement over business' direction, change in regulatory or legal environment, major fight among siblings under joint trust, and economic downturn.

Finally, succession risks are risks that are related to leadership transitions in the family, business, and ownership circles. A few examples of succession risks are the illness/incapacity/death of key family constituent, major change

in regulatory or legal environment, acquisition/merger, sudden retirement of owner or founder, and divorce/remarriage.

To manage those risks, Mrs. Shanti applied several things, such as hiring professional managers in the family business, integrating professional management into the company, and having minimum professional requirements for the employees, including the family members.

The roles of professional managers in the business are to run the operation of the company, to act as the enforcer in establishing a culture of work-discipline in the company, and to develop the system procedures and professionalize the company's business conduct.

Next, the integration of professional into the company could be done by getting the founders' commitment to transfer their power and authority to the managers which should

occur while the founders are still in a productive age and while the company is in the take off period. The process of this transfer should be staged as such in accordance with the individual maturity and readiness of the professional managers.

Finally, it is important to make all of the employees (including the family members) a professional. The minimum requirements for a professional are the ability to communicate, proficiency in English and Bahasa Indonesia, leadership ability (both internal and external), flexibility in adapting to new developments outside the company's environment, wide business horizon and vision, ability to evaluate and handle a number of complex problems simultaneously without having to sacrifice other activities, and the ability to make informative and self-explanatory report for both oral and written report.

*Written by: **Ray Antonio***

CONCLUSION

Conflicts and confusions cannot be completely erased from any family businesses. Hence, it is important for family business owners to reduce or manage them.

Several ways in managing them are by integrating IT and business governance, hiring professional managers in the family business, integrating professional management into the company, and having minimum professional requirements for the employees (including the family members).

CLIMATE CHANGE RISK MANAGEMENT



BALI
ERM
2016

Climate Change Risk Management

Presented by:

Nur Hidayati

National Executive Director at WALHI

Yves Guerard

Board Member of ERMA, Canada

Hosted by:

Fadjar Proboseno, ERMCP

Board of IRMAPA

This session explained about the current condition of our environment, the risks we have to face due to the climate change issues, and how to face the climate change risks. Climate risk is an important issue to discuss since it actually will give huge impact for humanity. This impact can vary from social issues, health issues, up to economy issues.

In this session, the presentation will be divided into two parts. The first presentation was given by Mr. Yves Guerard, Board Member of ERMA, Canada. Mr. Yves explained the climate change issues in a more global scope.

The second presentation explained by Mrs. Nur Hidayati, National Executive Director at WALHI. Mrs. Nur Hidayati's presentation were more focused on

Indonesia's environment regarding this climate change issues.

While the speakers have different focus, both of them have one thing in common. They mainly explained several ways that can be done in order to mitigate climate change risks.

Part 1

Yves Guerard

Board Member of ERMA, Canada

Based on World Economic Forum (WEF) Survey, there are 5 top risks that companies face. For the next ten years, two of these top risks are climate related while the other two are partly related.

Figure 1 shows the WEF top 5 risks for the next 18 months and also for the next 10 years. A huge difference can be seen between those 2 time frames. For the next 10 years, it seems that climate issues will be the main issues that we have to control.

Talking about these 5 risks, Mr. Yves said that there are dual sources for the climate issues, which are direct physical impacts of global warming and impacts of decision maker's initiatives to control, mitigate, or adapt.

Any climate risks that we face will affect individual lifestyle, food security, and health. Also, these climate risks will impact the enterprises, economy, society, as well as the planet.



Figure 1. WEF Top 5 Risks

Since the climate change issues are becoming more and more important, Intergovernmental Panel on Climate Change (IPCC) produced the 5th Assessment Report. This report consisted of a Synthesis Report and 3 Working Group reports. Those Working Group report titles are: The Physical Science Basis; Impact, Adaptation, and Vulnerability; and Mitigation of Climate Change. The first of Working Group was published in 2013 and the rest was published in 2014.

This IPCC report actually brought some key messages. Climate change issues are real and they are caused largely by humans. These issues are a serious problem if people cannot do anything in order to mitigate those risks. Catastrophic outcomes for humans are also possible.

Unfortunately, science does not know yet when, where, and how such outcomes might occur. One of the biggest causes of this climate change risk is the emissions of Greenhouse Gases (GHG).

According to the IPCC report, additional emissions of GHG will increase the magnitude of this risk management problem. Besides all of that key messages, the IPCC climate models

are actually still work in progress, as data and research accumulate, the fit improves, and conclusion in successive reports are evolving.

Though IPCC report could remind us about the danger of climate change issues that we are facing right now, there are also critics and skepticisms about this report. Not everybody agrees with all of the IPCC conclusions; some believe IPCC scientists are being too optimistic; while others reject them as being overly negative.

There are some dissents regarding the result on the IPCC report. It is still questionable whether the climate change is real or not. It is also discussed whether the biggest contributors to our climate change issues are human activities or natural causes. Some people argued that the harm of climate change has done is more than 2oC increases, but the others argued that it has only done less than 2oC increases.

Another issue of this climate change is about the balancing of growth and sustainability. Sometimes those two things are contradicting one another; that growth sometimes abandones sustainability or sustainability that sometimes hampers the growth.

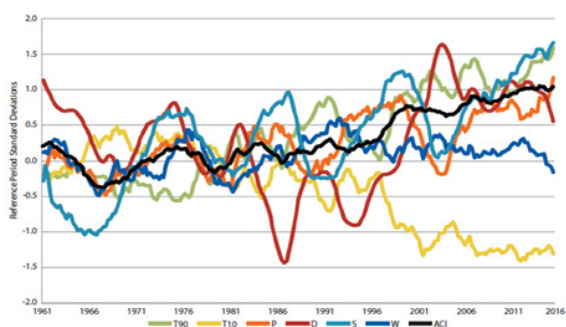


Figure 2. Monthly 5-Year Average of ACI Components

As mentioned before, there are direct physical impacts of the global warming. Mr. Yves explained these direct physical impacts extracted from Actuarial Climate Index (ACI) launched recently by 4 North American actuarial associations. This report is based on data series going back to 1961. It took big sample for the planet but due to the limitations in data, this report only covered North America.

ACI actually measures impact of a basket of extreme climate events, with a frequency outside the 10th to 90th percentile interval for the 1961-1990 reference periods. In their research, ACI combines 6 variables, including high temperature, heavy rain falls, violent winds, low temperature, long drought, and sea level.

From this research, it can be concluded that climate change affects our daily lives in myriad ways, it is evolving over the short term in ways that might seem random, and it also cumulatively makes our planet more at risk. Figure 2 shows the monthly 5-year average of ACI components.

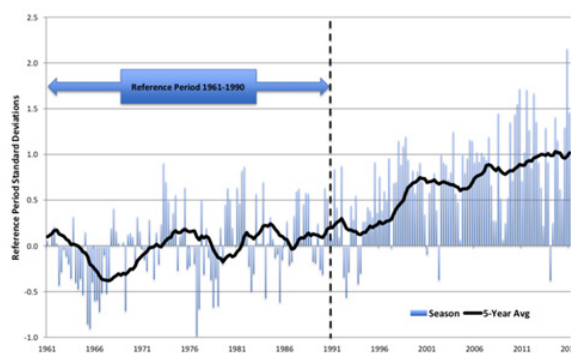


Figure 3. Actuaries Climate Index – USA & Canada

Specifically, figure 3 shows us the ACI of USA and Canada. We can see that ACI of USA and Canada move tends to have the uptrend since the lowest point in 1966.

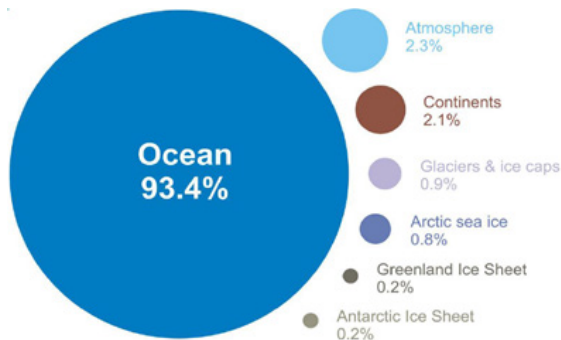


Figure 4. Where Does Global Warming Affect?

When it comes to the global warming, many people think that this temperature increase will happen in the air. However, according to the researches, global warming mostly affects the ocean. Figure 4 shows us the percentage where does the global warming affect.

From the figure, we can see that almost 95% of global warming affects the ocean. This means that when global warming occurs, the oceans will be the site of the most profound to response. The reason behind it is because the ocean is able to retain much more heat than the atmosphere.



Figure 5. Top 10 Cities that Has Highest Annual Flood Costs by 2050

The bigger consequence of this phenomenon is about the rising of sea levels. Since the global warming occurs, the warm water will expand. This can bring big impact for our environment, especially for those who live along the coastline.

Figure 5 shows the top 10 cities that will have the highest annual flood cost by 2050. Guangzhou, China, seems to be the city that will bear the highest flood cost of \$13.2 billion. Here we can see that the climate change risk also impacts our economy.

The rising sea level will also bring great impact to the Antarctic and Greenland. The Antarctic and Greenland ice sheets contain more than 99% of the freshwater ice on Earth. Some calculations have been made to measure the sea level rise if the ice sheet melted on those 3 regions.

The Antarctic Ice sheet is 14 million km² and the sea level will rise about 60 meters if the ice sheets are totally melted. The Greenland Ice Sheet is 1.7 million km² and the sea level will rise about 6 meters if they're totally melted.

Ice sheets are slowly flowing downhill under their own weigh. To remain stable, an ice sheet must accumulate the same mass of snow as it loses to the sea. Considering this issue, the catastrophic risk that a large chunk of ice breaks suddenly is not known yet but monitoring is in place.

	Climate Driver	Exposure	Health Outcome	Impact
 Extreme Heat	More frequent, severe, prolonged heat events	Elevated temperatures	Heat-related death and illness	Rising temperatures will lead to an increase in heat-related deaths and illnesses.
 Outdoor Air Quality	Increasing temperatures and changing precipitation patterns	Worsened air quality (ozone, particulate matter, and higher pollen counts)	Premature death, acute and chronic cardiovascular and respiratory illnesses	Rising temperatures and wildfires and decreasing precipitation will lead to increases in ozone and particulate matter, elevating the risks of cardiovascular and respiratory illnesses and death.
 Flooding	Rising sea level and more frequent or intense extreme precipitation, hurricanes, and storm surge events	Contaminated water, debris, and disruptions to essential infrastructure	Drowning, injuries, mental health consequences, gastrointestinal and other illness	Increased coastal and inland flooding exposes populations to a range of negative health impacts before, during, and after events.
 Vector-Borne Infection (Lyme Disease)	Changes in temperature extremes and seasonal weather patterns	Earlier and geographically expanded tick activity	Lyme disease	Ticks will show earlier seasonal activity and a generally northward range expansion, increasing risk of human exposure to Lyme disease-causing bacteria.
 Water-Related Infection (Vibrio vulnificus)	Rising sea surface temperature, changes in precipitation and runoff affecting coastal salinity	Recreational water or shellfish contaminated with Vibrio vulnificus	Vibrio vulnificus induced diarrhea & intestinal illness, wound and blood-stream infections, death	Increases in water temperatures will alter timing and location of Vibrio vulnificus growth, increasing exposure and risk of water-borne illness.
 Food-Related Infection (Salmonella)	Increases in temperature, humidity, and season length	Increased growth of pathogens, seasonal shifts in incidence of Salmonella exposure	Salmonella infection, gastrointestinal outbreaks	Rising temperatures increase Salmonella prevalence in food, longer seasons and warming winters increase risk of exposure and infection.
 Mental Health and Well-Being	Climate change impacts, especially extreme weather	Level of exposure to traumatic events, like disasters	Distress, grief, behavioral health disorders, social impacts, resilience	Changes in exposure to climate- or weather-related disasters cause or exacerbate stress and mental health consequences, with greater risk for certain populations.

Figure 6. Examples of Climate Impacts on Human Health

Another great impact of the climate change regards to the human health. Figure 6 shows us some of the impacts of climate change on human health.

The climate change issues will impact human health by extreme temperature, outdoor air quality, or disasters like flooding. The climate change issues can also stimulate the spreading of many diseases that will affect human health system. Water, food, or animal disease vectors can spread a great infection among the human being.

Explaining the great impact of climate change, Mr. Yves continued to the impact on food production and security. According to Mr. Yves, obvious climate impacts on terrestrial food production are observed in some sectors around the globe. Climate extremes such as droughts have occurred in major producing areas, resulting in price hikes for food and cereals. The forecasted ocean-level rise will also

threaten crucial food producing areas along the coasts, such as India and Bangladesh, which are major rice producers.

In the security perspectives, climate change will increasingly affect the food security. This happens particularly in low-latitude regions and will be exacerbated by escalating food demand. Unfortunately, right now the food insecurity is already generating conflict in vulnerable regions around the globe.

Climate change can also be caused by the emission resulted from human activities, such as agriculture, forestry, and other land use. The Food and Agriculture Organization (FAO) of the UN estimates that 18% of the emissions are caused by animal agriculture. Livestock are also responsible for 65% of emissions of nitrous oxide.

Nitrous oxide is a GHG that is 265 times more powerful than carbon dioxide. Other than that, methane emissions are also a powerful GHG that is emitted by livestock. However, CO2 accumulates over a very long period whereas methane and others are shorter lived.




	Institutional investors in France required to disclose how they are managing climate change risks.
	California's insurance commissioner calls for voluntarily coal divestment and will require disclosure of coal company holdings.
	SEC issues interpretive guidance on disclosure related to climate change (2010) and insurance commissioners in six states continue to administer NAIC climate risk disclosure survey.
	The Financial Supervisory Authority in Sweden calls on the financial sector in Sweden to develop stress tests to capture climate change risks.
	The Dutch Central Bank calls for more transparency (carbon foot-printing and energy transition plans) to help FIs assess climate risks.
	European Systemic Risk Board report suggests that a "sudden-transition policy scenario" should be included in macroeconomic scenarios and in stress tests of financial institutions and the financial system as a whole. ²⁵

Figure 7. Notable International Regulatory and Financial Industry Responses to Date

After explaining about the great impact of climate change to our human life and environment, Mr. Yves continued his presentation by showing us how climate change risk is related to our economy. This relation can be seen from the statement of the Governor of the Bank of England, Mark Carney.

Mark Carney said that there are three broad channels through which climate change can affect financial stability: physical risks (e.g. extreme weather), liability risks (e.g. litigation damages), and transition risks (e.g. stranded assets).

Answering these challenges on climate change, the Financial Stability Board proposed the creation of an industry-led disclosure task force on climate-related risk to the G20 on Nov 9th 2015. The Phase I report of this task force was issued in March 2016.

This phase includes survey of landscape to help inform scope, high-level objectives, and principles of disclosure. On the first phase, 'preparers' are likely to include financial and non-financial companies as well as financial sector participants such as large institutional investors, fund managers, and lenders.

After finishing the first phase, Phase II (and final report) should be delivered to the FSB in December 2016, and made available to the public in February 2017. Figure 7 shows us some notable international regulatory and financial industry responses to date.

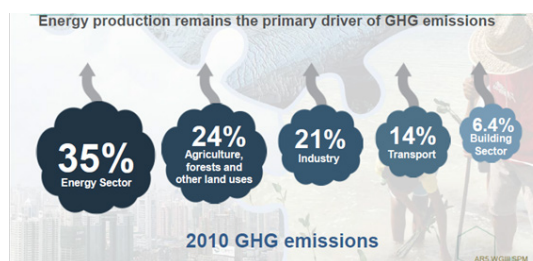


Figure 8. Sources of Emissions

Climate change is strongly affected by the emissions. GHG emissions seem to be the emission that brings most impact to the climate change problem. GHG emissions can be varying resulted from several sources.

Figure 8 shows us the sources of GHG emissions in 2010. From the figure, we can see that the biggest sources of GHG emissions in 2010 came from the energy sector.

Realizing the harm of climate change issues, many countries have developed some agreements or conferences for discussing the climate change problem. One of them is the Conference of the Parties (COP). The Conference of the Parties is the decision-making body for the United Nations Framework Convention on Climate Change (UNFCCC) which is held annually.

The IPCC mentioned before is a key participant to the COP meetings. COP 21 was held in Paris from November 30th to December 11th 2015 with delegates from 195 countries and other interested entities. COP 22 was held in Marrakech from November 7th to 18th 2016 and called "for the highest political commitment to combat climate change, as a matter of urgent priority".

Another agreement regarding the climate change mentioned by Mr. Yves is about the Paris Agreement. The Paris Agreement of December 2015 was declared to become effective on November 4th 2016. It was ratified by over 113 countries already representing 79% of GHG emissions. The minimum requirement was 55 parties (out of 193 signatories) and 55% of emissions.

By comparison, the Kyoto Protocol signed in December 1997 became effective only in February 2005. This shows that nations are now taking climate change more seriously. Furthermore, this momentum is confirmed by the adoption on October 15th 2016 of an amendment to phase down HFCs under the Montreal Protocol, committing 197 countries to cut the production and consumption of HFCs by more than 80% over the next 30 years.

These are some key features of the Paris Agreement:

1. Temperature Goal

An aim to limit overall global warming to less than 2°C, and possibly even down to 1.5°C. This will require a significant ramp up of national pledges to reduce emissions by 2030.

2. Net Zero Emissions Goal

It was agreed that the world would reach “net zero” emissions in the second half of the century, by balancing carbon released with an equivalent amount of sequestered (captured) or offset.

3. Five Year Review Cycle

Pledges to reduce emissions will need to ratchet up over time, with countries re-submitting every 5 years. Submissions can only be strengthened (i.e. no backtracking on prior pledges) and long-term targets are encouraged.

4. Climate Financing

To provide financial support to poor countries on the cost of the transition, the agreement has a climate finance goal of \$USD 100 billion per year by 2020. This amount is a floor so it is anticipated that it will increase over time.

5. Legal Status

Emission reduction plans are not legally binding, but the reporting mechanisms (yet to be determined) and the 5 years review process are. There will be a strong role for non-state actors in ‘policing’ the agreement.

In his presentations, Mr. Yves also showed us some warnings in IPCC Summary. According to the IPCC 5th Assessment Report, “Delaying mitigation efforts beyond those in place today through 2030 is estimated to substantially increase the difficulty of the transition to low longer-term emissions levels and narrow the range of options consistent with maintaining temperature change below 2°C relative to pre-industrial levels (high confidence)”.

In 2010, it also would have been necessary to aim at reducing the CO₂ equivalent emissions from 49 Gt to 22 Gt by 2050. In order to reduce the emissions to zero by 2100, the total emissions up to 2050 needed to be limited to 825 Gt and to 125 Gt after the first one accomplished. As we did not reduce emissions fast enough, future reductions need to be accelerated.

How about Indonesia? Does Indonesia contribute a lot in causing the climate change issues? Are climate changes issues in Indonesia also bring such a great impact? Figure 9 shows us about how much cumulative GHG emissions in 1990-2011 of some countries in the world. Indonesia contributes 4% of the world total cumulative GHG emissions in 1990-2011.

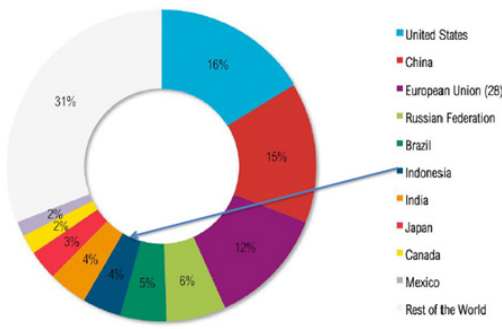


Figure 9. Cumulative GHG Emissions 1990 – 2011 (% of World Total)

In facing the climate change issues, Indonesia faces the risks in one side and also the opportunities in other side. Sea rise seems to be a major threat for Indonesia. Considering this, Indonesia needs to watch the risk of catastrophic loss of glaciers in Antarctica.

Compared to other countries, Indonesia is still doing well in terms of emissions per capita. However, Indonesia is still generating electricity from coal and high emissions from deforestation and land use. These emissions absolutely contribute to the climate change problem in our whole environment.

Figure 10 shows per capita emissions for top 10 emitters. Another challenge is that Indonesia produces only 2.5% of world GDP, but Indonesia contributed 4% of cumulative GHG since 1990. This should be considered. Figure 11 shows the Emissions intensity of top 10 emitters.

Regarding the opportunities, Indonesia could benefit greatly from innovations in efficiency to acquire solar energy. Solar, geothermal and gas can help minimize recourse to coal and oil.

Besides that, reducing emissions from deforestation and land use would also free up some space for the energy necessary to support growth. Figure 12 shows comparisons of total emissions of top 10 emitters.

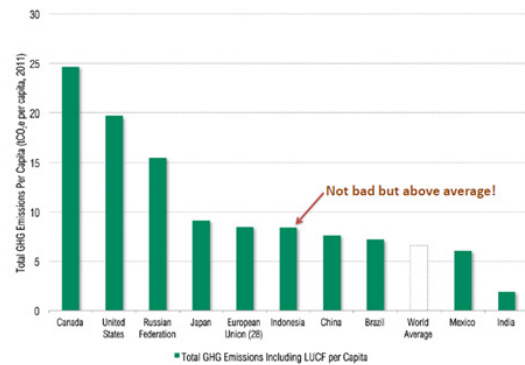


Figure 10. Per Capita Emissions for Top 10 Emitters

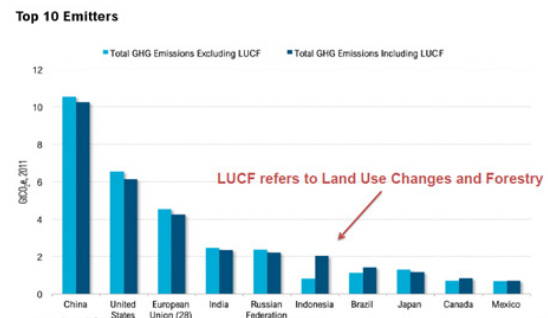


Figure 11. Emissions Intensity of Top 10 Emitters

After explaining the climate change issues in Indonesia, Mr. Yves discussed the mitigation, adoption, and control that can be done in order to face them. In facing the risks, Mr. Yves said that the likelihood of limiting global warming to 2oC is low. Thus, we better be prepared for the higher risks associated with +3oC or +4oC.

Talking about the CO₂ emissions, it is our task to use our capital efficiently and make a low carbon economy attractive financially. If we succeed, we can hope that human creativity and

inventions will allow humanity to thrive within a lower carbon budget and stabilize CO2 at levels below 450 or at most 500 ppm.

Net emissions also need to gradually be reduced asymptotically to zero before reaching about 475 ppm in order to stabilize temperatures at 2°C above historical levels. Mr. Yves also explained that zero net emission must be achieved earlier than 2100 to avoid overshooting or bet on the capacity to capture and sequester carbon to achieve negative net emissions.

There are some potential research breakthroughs considering the climate change risks we face. We better deploy our resources and shift from repair to prevention and also from subsidies to research. One of the potential researches is about extracting only the energy. Efficient methods to recuperate and sequester the carbon may become scalable to a level where it would dramatically expand the carbon budget.

The second potential research we may develop is about substituting solar energy to fossil. Since solar energy is one of the biggest renewable energy sources we have, it will bring vast advantages for us to replace the fossil with it. Besides that, the emissions caused by the fossil resource energy would be much higher than the solar energy. The efficient methods to replace fossil fuels as a source of energy by solar energy will practically offer an unlimited supply for human being.



Figure 12. Top 10 Countries Using Solar and Wind as Energy Sources

Furthermore, one of the best solutions we have to mitigate the climate change risks is by using more renewable energy. As mentioned before, Indonesia has a lot of renewable energy sources. Therefore, we need to develop some efficient methods in order to exploit them.

Two kinds of renewable energy mentioned in Mr. Yves’s presentation are solar and wind energy. Figure 13 shows the countries that mostly use solar and wind energy for their productivity.

If we succeed in maximizing these energy sources, it will bring unlimited energy for us. Some countries have developed these renewable energies, but some other countries have not. Hence, this would be our task to develop the solution.

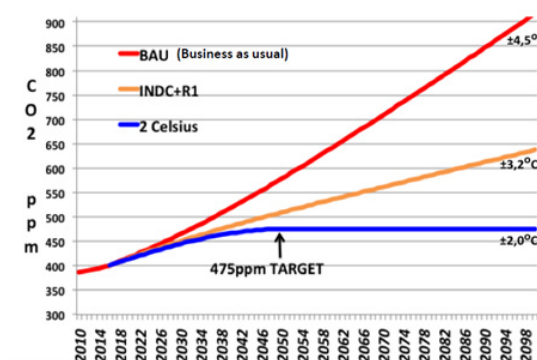


Figure 13. Comparisons of CO2 ppm/year for Three Pathways

At the last point of his presentation, Mr. Yves gave the explanation about a feasible pathway to achieve the atmospheric CO₂ at 475 ppm as well as the global warming limit into 2oC.

Figure 13 shows the comparisons of CO₂ ppm/year for 3 pathways. The NDCs tabled for COP21 do not reduce emissions fast enough to limit warming to 2oC. On the contrary, net emissions are still increasing. Thus, we need to reverse direction as soon as possible.

Unfortunately, the remaining “budget” is now less than 75 ppm even at the minimum. Trying to make some serious actions, COP22 has put pressure on countries to do more before the revision scheduled for 2030.

Part 2

Nur Hidayati

National Executive Director at WALHI

Recently, the issue of climate change risk management is very important in the business environment. This issue can bring great impact to our economy and has been considered since Rio Conference in 1992. However, climate change has not got enough attention from the people around the world, because not many people believe that climate change risk will bring impact to their economy.

Mrs. Nur Hidayati began her presentations by showing some facts from the Stern Review from the UK. Stern Review explains a lot about the climate change and its impact to the economy.

According to the review, all countries will be affected by the climate change, however the poorest countries will suffer the earliest and the most. This happens because poor countries are usually less prepared and lack of the capability in facing the climate change issue.

This review also says that average temperatures could rise by 5oC from pre-industrial levels if climate change goes unchecked. The impact of the global warming can be huge for our environment and humanity.

Warming of 3oC or 4oC could actually cause floods, which are caused by the rising sea level and other climate change disasters. By the middle of the century, 200 million people may be permanently displaced due to rising sea levels, heavier floods, and droughts.

These global warming issues can also bring impact to the food production and leave 15-40% species to face extinction. The Stern Review declared that warming of 4oC or more is likely to seriously affect global food production.

Facing these issues, some actions should be taken. If no actions were taken by world governments, it will cost about 5% of global GDP every year. Furthermore, if it goes on like that, it will cost about 20% of global GDP eventually. The later we act, the greater the cost of economy will be.

Mrs. Nur Hidayati also visualizes this climate change issue like the story behind a frog in the boiled water. We cannot feel anything until it is too late for us to react. Slowly but sure, the temperature will continually increase until we suffer as the temperature becomes too hot. Many of us have not realized that climate change can impact our country so much.

Talking about the climate change in Indonesia, some researches have been conducted explaining these issues. In Indonesia, the average annual temperature has increased by about 0.3oC. Overall, annual precipitation has also decreased by 2% to 3%. Thus, precipitation patterns in Indonesia have also changed recently.

There has been a decline in annual rainfall in the southern regions of Indonesia and an increase in precipitation in the northern regions. As many climate changes happen, we now can hardly predict whether it is rainy season or dry season. Rainy season is actually shifting to another month.

In Indonesia, the seasonality of precipitation (wet and dry seasons) has changed. The wet season rainfall in the southern region of Indonesia has increased while the dry season rainfall in the northern region has decreased. These facts are based on the research conducted by Hulme & Sheard (1999) and Boer & Faqih (2004).

Furthermore, Mrs. Nur Hidayati revealed some projected climate impacts in Indonesia in this presentation. According to some researches, there will be changes in water and food availability in Indonesia. This is mostly caused by the effects of El Nino and La Nina. Some people even predicted that the effects of El Nino/La Nina today may portray how Indonesia will be impacted by climate change in the future.

Talking about the food availability, this climate change issues will affect the decision of planting the food. Any disaster happens in Indonesia will affect the food supply.

Sea level rise also creates risks for Indonesia because as an archipelago nation, Indonesia has a very long coastline around the islands. Indonesia has a coastline as long as 81.000 km (one of the longest coastlines in the world).

Statistically, about forty-two million citizens live less than 10 meters above sea level. This makes sea level rise risks become more vital in Indonesia. One meter rise in sea level could

inundate 405.000 hectares of land and reduce Indonesia's territory by flooding low-lying islands.

Furthermore, warming sea-surface temperature seems can potentially bring disadvantages to the economy of Indonesia. Warming sea-surface temperatures are causing changes in oceanic circulation patterns and salinities. This is likely leading to a reduction of primary production in tropical oceans and also has serious effects to coral reefs. The temperature also affects fish productions because fish movement is greatly affected by the sea temperature.

Finally, climate change in Indonesia will certainly affect the human health as well. This issue may include more widespread vector-borne infections (e.g. malaria and dengue). Also, climate change issues can bring an expansion of water-borne diseases, such as diarrhea. Those diseases are greatly related to disasters caused by climate change, like flooding.

Table 1a. Summary of 2000 GHG emission and removal (in Gg)

Source/Sink	CO ₂ emission	CO ₂ removal	CH ₄	N ₂ O	CO ₂ e
Energy	305,983		1,221	6	333,540
Industry	31,938		104	0	34,197
Agriculture	2,178		2,419	72	75,419
Land Use Change and Forestry		1,593	3	0	649,254
Peat Fire ¹	172,000				172,000
Waste	1,662		7,020	8,05	151,578
TOTAL					1,415,988

¹Note: Emission from peat fire was taken from van der Werf et al (2008). Source: MoE (2009)

Table 1b. Summary of GHG emissions from 2000-2005 from all sectors (in Gg)

	2000	2001	2002	2003	2004	2005
Energy	333,540	348,331	354,246	364,925	384,668	395,990
Industry	34,197	45,545	33,076	35,073	36,242	37,036
Agriculture	75,419	77,501	77,030	79,829	77,863	80,179
Waste	151,578	153,299	154,334	154,874	155,390	155,609
LUCF	649,254	560,546	1,287,495	345,489	617,280	N.E
Peat Fire ¹	172,000	194,000	678,000	246,000	440,000	451,000
Total with LULUCF	1,415,988	1,379,222	2,584,181	1,226,191	1,711,443	1,119,814+LUCF
Total Without LULUCF	594,734	624,676	618,686	634,701	654,162	668,814+LUCF

¹Note: Emission from peat fire was taken from van der Werf et al (2008). Source: MoE (2009)

Figure 1. Summary of GHG Emission in Indonesia

The influence of human activities on climate change is clear. The emission issues are one of the biggest causes of the climate change problem. Emissions in Indonesia are mostly coming from land use and forestry.

The projection of our energy mix is still quite worrying. Figure 1 shows the number of greenhouse gas (GHG) emission in Indonesia and its source of emission. This data was taken from Indonesia 2nd National Communication to UNFCCC (2009). The data shows the energy caused the second biggest of CO2 emission.

Another interesting thing about this data is that peat fires created large emission in Indonesia. This issue should be monitored by Indonesia so that climate change risk can be managed better.

Facing all of those climate change issues, Paris Agreement has committed to make contributions in reducing global emissions. Unfortunately, although all pledges have been submitted, it will not affect so much in reducing the temperature below 2oC. As things go, the world is on track to a temperature rise of around 3oC by 2100. This will bring significant climate impacts.

As the country that also affected by climate change issues, Indonesia had done some actions in order to mitigate those climate change risks. In the G20 meeting in Pittsburgh (2009), SBY committed to reduce greenhouse gas (GHG) emission. It is planned that GHG emission will be reduced by 26% from business as usual scenario (BAU) with own resources and 41% by international supports by 2020.

According to the Indonesian INDC (Intended Nationally Determined Contribution) issued on 24 September 2015, Indonesia is committed

to reduce GHG to 29% by 2030 with own resources, and 41% by 2030 with international supports. Furthermore, this has been ratified through the Act No.16/2016.



Figure 2. Indonesia Intended Nationally Determined Contribution (INDC)

Figure 2 shows us the Indonesia’s Intended Nationally Determined Contribution (INDC). From the figure, it is seen that there is a gap between the commitment in the agreement and the plan. Unfortunately, there is still an increase in the use of coal and GHG emission. Indonesia has to change that as soon as possible because the climate change issue is urgent. Thus, everyone has to participate actively and run their businesses accordingly.

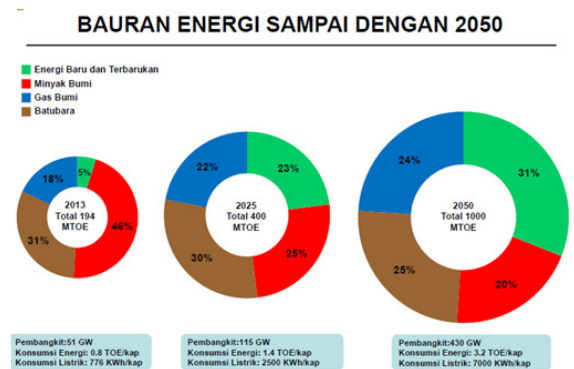


Figure 3. Indonesia’s Energy Mix

The next question is what can Indonesia do to deal with those climate change issues? One of the answers is the acceleration of transition towards low carbon development.

According to Mrs. Nur Hidayati, Indonesia needs to make serious efforts in the development of renewable energy. This solution of renewable energy seems quite powerful in managing climate change risks. Indonesia actually has a lot of potential renewal energy sources that have not been explored, such as water, geothermal, sun, and biomass. These alternative energy sources should be used in creating the better environment for the future.

Indonesia planned that renewable energy in the energy mix used by Indonesia will reach 23% by 2025 and 25% by 2030. As of 2013, the renewable energy is accounted for 5% of all the energy mix of Indonesia. Coal and crude oil had the biggest portion of Indonesia's energy mix by 2013. Figure 3 shows the energy mix of Indonesia by 2013, 2025, and 2050.

Another issue beside the renewable energy, Indonesia also face the problem from emission caused by deforestation and peatland degradation. The 60% of emission now comes from deforestation and peatland degradation. The current trend of forests destruction will cause Indonesia to lose 25% of its current forest area in 2030.

Mrs. Nur Hidayati also explained that Indonesia's deforestation contributes 30-40% of global deforestation emission in the period of 2000-2010. Another fact shows that forest fires emission reached 1.043 million metric ton (more than total US emission in a year) in 2015.

Based on those data, it seems that Indonesia should pay more attention to these emission issues in managing climate change risks. Indonesia should enhance its efforts until 2020 to reduce emission from deforestation and forest degradation.

Written by: Reynaldi Hartanto

CONCLUSION

Climate change issues will bring great impact to the economy. However, most people haven't realized the threat surrounding climate change risks in our environment.

These issues are actually pressing matters and need to be mitigated as soon as possible. The later we act, the bigger the impact that we will have to bear. It needs a lot of commitment from the nations to collaborate together for managing these risks.

One of the solutions to cope with the climate change risks is the use of renewable energy sources, as those can provide humanity unlimited sources of energy with a smaller amount of emissions.

STANDARDS BUILD TRUST:

The use of SNI ISO 31000 Risk Management Standard to Embrace Digital Challenges and Opportunities - Public and Private sectors



BALI
ERM
2016

Standards build trust:

The use of SNI ISO 31000 Risk Management Standard to Embrace Digital Challenges and Opportunities - Public and Private sectors

Presented by:

Bernado A. Mochtar

Head of Risk Management ABM Investama Group;
Member of National Technical Committee SNI: ISO 31000 BSN;
Board Member of IRMAPA

Mohammad Mukhlis

Member of National Technical Committee SNI: ISO31000 BSN;
Indonesia Stock Exchange

Boy Michael Tjahyono

Risk & Governance Lead – PwC Consulting Indonesia

Hosted by:

Ivan Lanin

Internet Expert; ISO Based System Certification Expert;
Former Executive Director of Wikimedia Indonesia

International Organization for Standardization (ISO) is one of the organizations that issued standards which can be adopted by various organizations. So far, ISO 31000:2009 for Risk Management, ISO 27000 series for Information Security Management System (ISMS) standard, and the new

one ISO 9001: 2015 for Quality Management System (QMS) are the standards that have been published by ISO. Standard is important to optimize the competitiveness of organization.

In this session, there are three speakers: Bernado A. Mochtar, Mohammad Mukhlis, and Boy Michael Tjahyono. This session will provide an overview of how the three ISOs are applied in organizations based on experience of the speakers.

Part 1

Bernado A. Muchtar

Head of Risk Management ABM Investama Group; Member of National Technical Committee SNI: ISO31000 BSN; Board Member of IRMAPA

In this session, Mr. Muchtar shared his experience in integrating 3 kinds of ISO in his company. His company has already implemented ISO 31000 and ISO 9001, but ISO 27001 and ISO 27005 are still in the process to be implemented. Among those standards, ISO 9001 is the oldest ISO standard that has implemented in his company. Therefore, the implementation of ISO 31000 and 27000 series need to align with ISO 9001.

How would the three ISOs be related? According to Mr. Muchtar, ISO 9001 is a standard that make sure the quality of business processes and a guidance to manage all the processes (for example by SOP).

The new ISO 9001, which is ISO 9001:2015, mentioned to address risk and opportunity. However, the details of risk assessment process are still referred to ISO 31000 series.

On the other hand, the digital era brings many impacts to organizations, such as managing data and information. Thus, the use of ISO 9001 to manage data recording and ISO 27000 series to manage the information and protect the security information in the digital era are needed. Furthermore, to protect the security information (mitigating cyber risk), organizations can refer to ISO 31000.

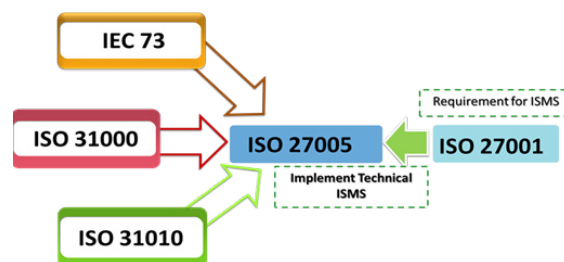


Figure 1. Integration Process ISO 27000 Series

Figure 1 describes the integration process of ISO 27000 series and how it is related to ISO 31000 series. ISO 27000 series that will be discussed are ISO 27005 and ISO 27001. ISO 27005 is the standard for technical implementation of ISMS. However, to implement ISO 27005, organizations need to consider ISO 27001 which consists of requirement of ISMS.

Both standards can help organizations to assess risks that are related to information technology. Therefore, the implementations of those standards are walking hand in hand with ISO 31000 which is the standard that focuses on risk management.

ISO 31000 consists of requirements and guidelines to manage risks which is also related to ISO 73 and ISO 31010. ISO 73 is a set of vocabulary that will be used in ISO which is necessary to minimize communication biases; while ISO 31010 is a guide for implementing risk management. Therefore, according to Mr. Muchtar, ISO 27001 will guide the requirements for implementation of ISMS, ISO 27005 will guide implementation of ISMS and will be related to ISO 31000, and ISO 9001:2015 will guide all of the integration process.

ISO 31000 and ISO 27005 have the same risk management approach which can be seen in the process of both standards. Thus, combining both processes is possible.

The first step of risk management process is establishing the context. Based on Mr. Muchtar's experience, ISO 31000 and ISO 27005 are implemented to make a clear context so that it will be easier to implement ISO 31000, ISO 27005, and ISO 91000; and move to the next steps which are identification, analysis, evaluation, and mitigation.

There is a slight difference between ISO 27005 and ISO 31000. In ISO 27005, there is a chance that the process will be back to establishing the context after risk mitigation.

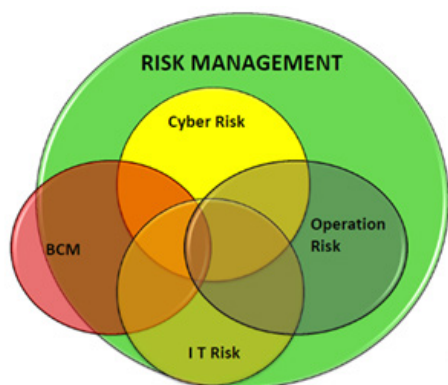


Figure 2. Risk Management

All risks that might occurred in an organization are maintained using risk management (see figure 2). Those risks are cyber risk, operation risk, and IT risk.

Any risks that include cyber risk and IT risk can affect the organization's sustainability. Thus, we need to evaluate business continuity management so we can make a business continuity plan. However, not all of those risks including business continuity management can be managed by risk management, because there might be events or occurrences that deviate beyond what is normally expected of a situation which are extremely difficult to predict.

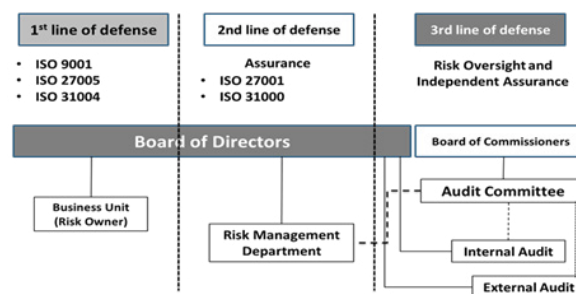


Figure 3. ISO Standards and Three Lines of Defense

Figure 3 shows how every line implements standard based on ISO. The 1st line of defense mainly deals with implementations or executions, so organizations can refer to ISO 9001, ISO 27005, and ISO 31004.

The 2nd line of defense is assurance process and organizations can refer to ISO 27001 and ISO 31000, since both are the necessary guidelines to make sure everything is according to guidelines and requirements.

Mr. Muchtar also stated that ISO 31000, as risk management framework, can be used on the 3rd line of defense or all of line of defenses, since the usage of ISO 31000 is generic.

Implementing a new standard in an organization is not a simple thing to do. Mr. Muchtar said that to implement a new culture or a new thing in an organization, it has to be done in one step at a time. Otherwise, there will be a lot of resistances during the process.

If an organization is still in the process of implementing ISO 27000 series, they should make adjustments in several policies to align with previous ISOs (ISO 31000 and 9001) which have already been implemented and the new standard that will be implemented (ISO 27000 series). In this session, Mr. Muchtar also shared several policy adjustments, including:

1. Information Security and Organization

Structure of organization is already established. When the organization wants to implement a new standard, it needs to make an adjustment to the structure.

2. Information Control (internal and external parties)

In the old days, all important files (like SOP) are being saved in books or cabinets. Nowadays, all data are being managed through a system. That is why it is necessary to manage all the incoming and outgoing data.

3. Acceptable User and Device

Employees are not allowed to use their own computer because there is a chance of malwares or viruses that can harm the system.

4. Data Classification

Before, everyone can access data easily whether they use their own hard disk or flash disk. Now, all data must be kept in a password-protected system and no one can access the data from home unless they use a VPN. The classification is

based on each process, for example finance can only see finance's data.

5. Data Storage Management

Similar with data classification, all new data in a system will be controlled.

6. Disposal Media

It is easy to delete data. But, there is a chance that the deleted data may contain specific information and important data about the company. Hence, it needs to be controlled.

7. Obligation of Managing Risk and Mitigation

Data are usually being controlled by a server and IT system. Now, everyone who has the access to a computer has to manage who can access the data, internally and externally.

8. Business Continuity Management

9. Recovery and Remedial (Information Management System)

In this case, for example there is a fire in one site, the system in that site will shut down immediately. Therefore, the company can do the continuity process when everything is already repaired, including system recovery and remedial.

Part 2

Mohammad Mukhlis

Member of National Technical Committee SNI: ISO31000 BSN;
Indonesia Stock Exchange

In this session, Mr. Mukhlis explained the integration between three ISO standards which are ISO 9001:2015, ISO 31000:2009, and ISO 27005. According to Mr. Mukhlis, organizations

need to integrate 3 kinds of ISO (ISO 9001, ISO 31000, and ISO 27000 series) because organizations can gain a lot of benefits from them.

First, these standards are similar and using the same language (coming from the same organization, which is ISO); hence, organizations could make an effective progress when integrating the ISO standards.

Second, organizations should integrate the three standards because it is more efficient that way. Moreover, there are several sections that are related or complement each other, so it will take less effort to implement them in organizations.

ISO 9001:2015 promotes the adoption of quality management system. The adoption of Quality Management System (QMS) is a strategic decision for an organization that can help improve its overall performance and provide a sound basis for sustainable development initiatives. QMS needs risk-based thinking to be effective. Risk-based thinking emphasizes organization requirements to make plans and implement actions to address risks and opportunities.

To support the implementation of risk based thinking in ISO 9001:2015, it can be collaborated with ISO 31000 which consists of principles and guidelines of risk management. ISO 31000 recommends organizations to develop, implement and continuously improve a framework whose purpose is to integrate the process for managing risk into the organization’s overall governance, strategy and planning, management, reporting processes, policies, values, and culture.

Risk Management can be applied to the entire organization, at its many areas and levels at any time as well as to specific functions, projects and activities.

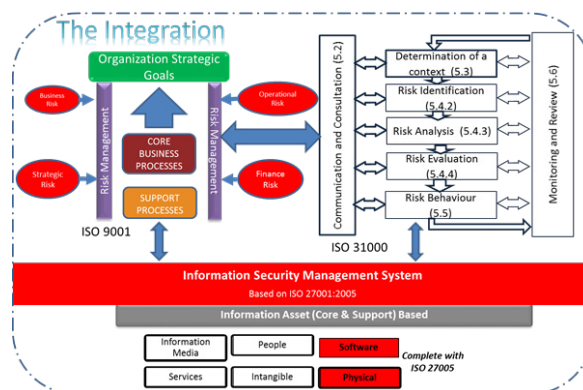


Figure 1. Integration of Three Standards

Figure 1 shows the integration between three kinds of ISO, which are ISO 9001:2015, ISO 31000, and ISO 27005. Managing and ensuring quality at the core and business processes in order to achieve strategic goals of organizations are parts of ISO 9001:2015.

However, in practice, in managing and achieving their strategic objectives (in accordance with defined quality in the organization), the organization is always faced with risks (e.g. business risk, strategic risk, operational risk, financial risk, etc.). Therefore, the new clause of ISO 9001: 2015 emphasizes the need to address risks and opportunities. The ISO 31000 can also be used as a guideline for managing risks.

For supporting the support process of organizations in the digital era, Information Security Management System (ISMS) is important. Organizations need to implement ISMS because in this digital era, information assets are not only physical but also digital (data). Therefore, after implementing ISO 9001 and 31000, organizations can also implement

ISO 27005. ISO 27005 specifies the requirement for establishing, maintaining and continually improving an information security management system within the context of an organization.

According Mr. Mukhlis, implementing three kinds of ISO can be started with implementing Quality Management System (QMS) while referring to ISO 9001:2015 for the guidance. After implementing QMS, the organization should then implement risk management based on ISO 31000. Risk management is required because QMS emphasizes risk-based thinking. After that, in managing critical information in the digital era, the Information Security Management System (ISMS) should be implemented.

Mr. Mukhlis explained that in implementing QMS, organizations should start with Create Quality Guidelines as the reference. Afterward, Create Quality Objectives of the Company and Identify the Level 0; Level 1; and Level 2.

After implementing QMS, the organization should implement risk management framework. According Mr. Mukhlis, these steps are needed to be considered when implementing risk management process and framework based on ISO 31000:

- Creating enterprise risk management guidelines (All matters relating to framework principles and processes);
- Define general criteria for the determination of the likelihood, consequences and exposures;
- Building a risk profile regularly and consistently;
- Consistently Monitoring and Reporting to the stakeholders;

- Risks assessment based on processes and information assets (according to the information asset classification of ISO 27001).

After having QMS and risk management framework, the next step is the implementation of ISO 27001 and ISO 27005 as a guideline to Implement Information Security Management System (ISMS). In accordance with the explanation from Mr. Mukhlis, there are several steps that need to be considered, including:

- Creating the guidelines of ISMS. The concept of risk management in ISMS processes can use the process in ISO 31000;
- The Object of managed risk covers 6 classification asset information (media information, services, people, intangible, software and physical);
- The Risk assessment that we use is:
 - Before assessing the risk, we must do some asset evaluation first, based on the CIA aspect
 - Next, do the assessment risk management process as a holistic view in accordance with the concept of ISO 31000.

In this session, Mr. Mukhlis also shared some advices to integrate the three ISOs. First, the organization should define their strategic goals and define the needs of standards for their business. After that, find the similarity, the effectiveness, the efficiency between the chosen standards. Lastly, use quick win technique or any techniques to define the priority for the business and the integration of them.

Part 3 Boy Tjahyono

Risk & Governance Lead – PwC
Consulting Indonesia

Mr. Tjahyonoto explicated that to understand the relationship between quality and risks, there are two main reasons.

Firstly, the organization must know whether they have put quality as a part of their objectives or not. If the quality is a part of the organization’s objectives, then the quality will have risks, because based on the ISO 31000, risk is defined as the effect of uncertainty to objectives.

Furthermore, in the eleventh principle of ISO 31000, it is mentioned that risk management facilitates continual improvement and enhancement to organizations. It means that risk management can accommodate the efforts for quality improvement.

(Quality Management System) and start with understanding the context of the organization and the needs of parties interested in the QMS, which is then used to define the scope of the QMS and its processes. This is followed by the commitment of the leadership to drive the organization to a customer focus by defining the organizational roles and responsibilities and by establishing a quality policy to give the overall QMS a focus.

The next level of planning is to identify and address risks and opportunities of the QMS, including setting and planning for quality objectives and changes to support continual improvement.

The final level of planning is to identify and implement the support structure to allow organizations to carry out its plans. This includes resources, identifying competence, awareness, communication and to set the processes for creation and control of documented information.

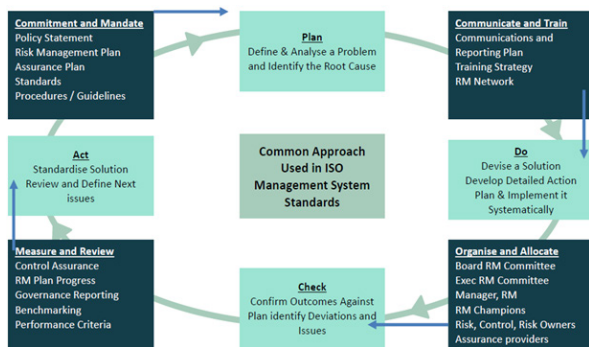


Figure 1. Correlation between Risk Management and Quality Management System

Figure 1 shows the Quality Management System in PDCA concept. The component of PDCA including:

• Plan

Planning is one of the biggest parts of the QMS

• Do

Planning is useless if the plan is not carried out. Controls need to be identified for the QMS operations; thus, product or service requirements need to be identified, designs need to be developed, and controls need to be placed on externally provided processes, products and services.

The process of producing the product or service needs to be carried out with control of product and service release; and any non-conforming products or services need to be addressed. In short, the activities of creating and providing products or services to the customer need to be done.

• **Check**

There are several requirements in the standard to check the processes of the Quality Management system to ensure that they are functioning properly as they have been planned. There is a need to monitor, measure, analyse and evaluate the products or services to ensure that they meet requirements, the processes used are adequate and effective, and customer satisfaction is being met.

Internal Audit of the processes is the key to effectively assess the system. The last one is the Management Review process, which reviews and assesses all of the monitored data to make changes and plans to address the issues.

• **Act**

Action involves the actions needed to address any issues found in the check step. Improvement is the overall heading for these action steps with the activities of addressing non-conformities and Corrective Actions to eliminate the causes of actual or potential non-conformities as the first step in acting to improve the system.

• **Plan**

As stated, this cycle starts again to ensure that there are plans in place for further improvement. Findings during the Internal Audit in the “Check” phase may have led to corrective actions from the “Act” phase, which in turn will require changes in planning to meet the updated requirements in the next “Do” phase.

The Management Review looks at the outcomes of Internal Audit, Corrective Actions and outputs resource plans to support any changes. Resources are assessed and increased, decreased or re-assigned as the business needs dictate. This leads into another round of Doing, and the cycle continues.

The darker boxes in figure 1 shows some comments about PDCA regarding to risks. According to Mr. Tjahyono, in the step between Plan and Do, risk management plays an important role in doing communication and facilitates training. It could reduce the gap between planning and execution (Do). Between Do and Check, there are risks regarding organize and allocate which related to governance aspects.

On the stage between Check and Act, measurement and review is essential. Lastly, between Act and Plan, mandate and commitment is required. It is necessary for the board members to fully support the mandate and commitment, because otherwise risk management will become meaningless.

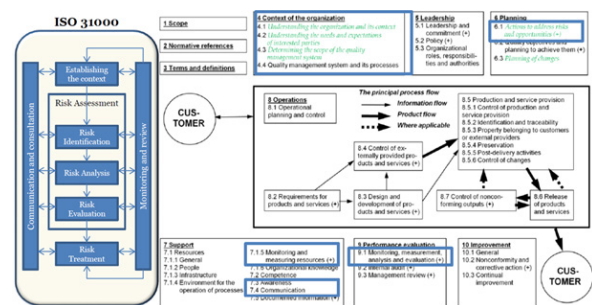


Figure 2. ISO 9001:2015 and ISO 31000

Figure 2 describes the relation between ISO 9001 and ISO 31000. In managing risks, ISO 31000 can be used as a guideline. In addition, they have the same initial step in the implementation process which is context establishment. The other similarities between QMS and risk management are not only the component of communication and monitoring but also measurement, analysis, and evaluation.

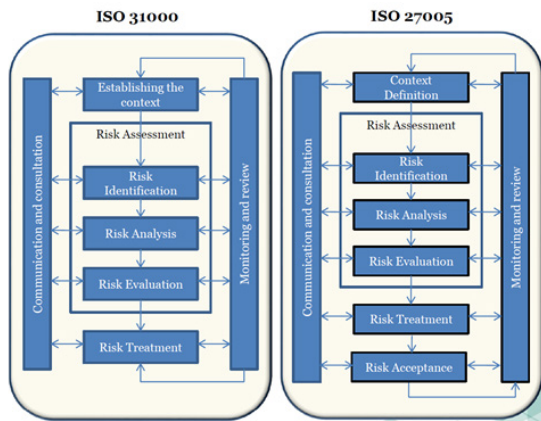


Figure 3. ISO 31000 and ISO 27005

Figure 3 shows us that there are some similarities between ISO 31000 and ISO 27005 processes. It starts with context establishment and they also have a similar Risk Management Process, with exception of the Risk Acceptance section in ISO 27005. It is distinguishable that ISO 27005 has its focuses on information security risk management.

In this session, Mr. Boy also mentioned some key takeaways to implement the three ISOs:

1. Risk Management and Quality Improvement are aligned in identifying their problems and implementing corrective strategies

2. Implementing the two programs can strengthen the RO/BUS abilities to minimize errors, enhance efficiency and improve the process

3. The framework for integrated Risk Management and Quality Management should be documented in a plan provided to all staff members

4. To coordinate the plan, consider the establishment of a committee that meets on regular basis and includes representatives from all departments

5. It takes time and effort to develop, implement and refine an Integrated Risk Management/Quality Improvement program. However, the benefit of such program – including a reduced error rate, more efficient operations and decreased litigation risk – makes it worthwhile for investment for even the smallest and most specialized organizations.

*Written by: **Belianny Putri***

CONCLUSION

In implementing standards in an organization, it needs an alignment because otherwise the business process will be hampered or it might be in contradiction with the other standards.

With the same sources, implementing standards would be more effective and efficient due to the similarity of their terms, language, and elements. For example, in implementing these three ISOs, it has the same initial step which is organizational context establishment. Moreover, the other important aspects are communication and monitoring.

The first thing to do in integrating ISO 9001:2015, ISO 31000: 2009, and ISO 27005 is establishing an organization's context. If the organization already uses ISO standards, it can integrate it by finding the similarities in every ISO standards and implement it one step at a time.

Supposedly, every organization should implement ISO 9001:2015 first before implementing the other standards. ISO 9001 is the ground rule if the organization's objective is to deliver the best quality to its customers. With the changes in ISO 91000:2015, risk-based thinking is necessary.

Risk considered as inherent aspect in quality management system rather than preventive action had been mentioned before in previous ISO version. By using risk-based thinking, the consideration of risk becoming an integral aspect. To accommodate it, ISO 31000 can be the standard of risk management implementation.

In this digital era, most of document assets are digitalized which introduces new risks. ISO 27005 can be a guide for Information Security Management System (ISMS).

ENTERPRISE LEGAL RISK MANAGEMENT:

Digital Environment



BALI
ERM
2016

Enterprise Legal Risk Management: Digital Environment

Presented by:

Leo J. Susilo, SH, CERG

Principal of CRMS Indonesia

Prof. Dr. Normah Omar, CPA

Accounting Research Institute (ARI) Higher Institutions'
Centre of Excellence (HICoE) Universiti Teknologi
MARA Malaysia

Hosted by:

Sri Rahayu, SH, LLM

Managing Partner of Rahayu and Partners Law Offices

The digital era brings various impacts to many disciplines in risk management, including legal risk, compliance risk, and fraud risk. This session discussed enterprise legal risk management in digital environment. This session is presented by two speakers, which are by Mr. Leo J. Susilo, SH, CERG and Prof. Dr. Normah Omar, CPA. Mr. Susilo mainly explained enterprise legal risk management, especially about legal and compliance risk.

After Mr. Susilo's part, Prof. Omar explained specifically about financial fraud risk. Prof. Omar shared the reasons why frauds could happen in organizations

and a research or an empirical study from CPA Australia entitled 'Importance and Usage of Fraud Risk Indicators (ISA 240) by Auditors'.

Part 1

Leo J. Susilo, SH, CERG
Principal of CRMS Indonesia

According to OCEG, Principled Performance is a point of view and an approach to business that helps organizations reliably achieve objectives while addressing uncertainty and acting with integrity. Figure 1 shows the correlation between governance, management, assurance, performance, risk, compliance, and also the standard of each element in the context of achieving Principled Performance.

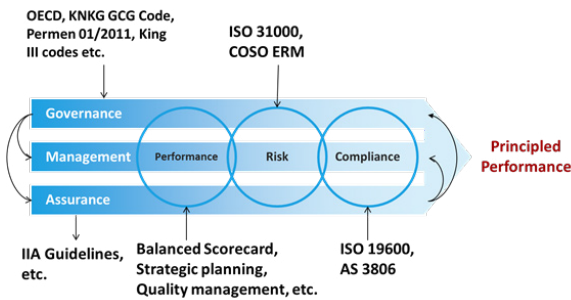


Figure 1. Risk in the Context of Achieving Corporate Objectives

In figure 1, there are governance, management and assurance of performance, risk, and compliance activities called GRC (governance, risk, and compliance). The GRC must work together to achieve the principled performance. To optimize achieving the principled performance, organizations use standards and frameworks.

For governance, Indonesia has OECD, KNKG GCG Code, Ministerial Regulation 01/2011 and King III codes for South Africa. In Assurance,

Indonesia has IIA Guidelines, and so on. For performance, there are some standards such as balanced scorecard, strategic planning, and quality management.

In risk, there are standards like ISO 31000 and COSO ERM. Whereas in compliance, there are standards such as ISO 19600 and American Standard 3806. These standards are used to facilitate each organization to have the same measurement instrument of GRC.

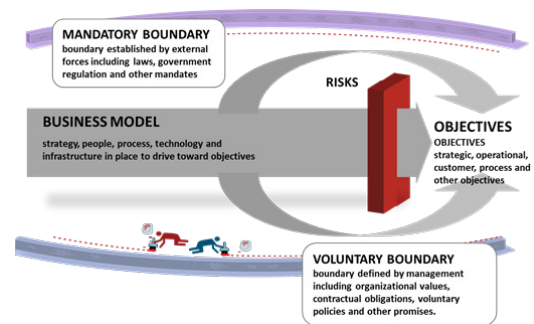


Figure 2. Risk in the Context of Achieving Corporate Objectives

When organizations are running their business or trying to achieve their targets/objectives, they are always facing risks. The risks could be barricades in achieving objectives (risks can illustrate as blocks or wall). Occasionally, they can go through the risks.

However, sometimes they cannot go through the risk because they are restricted by boundaries which become a barrier (see Figure 2). The boundaries hinder organizations by restricting them to do something against the risk through regulations, laws, organizational cultures, etc.

The boundaries in question are mandatory and voluntary. Mandatory boundary means external forces including law, government regulation,

and others mandates. This mandatory boundary will result a “compliance requirement” (external compliance).

On the other hand, voluntary boundary is defined by management including organizational values, contractual obligations, voluntary policies and other promises. Voluntary boundary has a character of a self-regulating norm. Compliance related to this is called “compliance commitment” (internal compliance).

Either the effect of uncertainties on compliance objectives or the failure to achieve the compliance objectives, both of them are compliance risk. Compliance risk consists of mandatory compliance risk and commitment compliance risk. Besides that, there is also legal risk. Legal risk arises where there is a legal relation between the legal subjects, which some party is breaking the rule of conduct, involving the rights, obligations and responsibilities.

People frequently have a wrong understanding between compliance risk and legal risk. These are the differences of compliance risk and legal risk.

- Compliance risk arises because there is compliance obligation, and the risk is the failure to achieve compliance obligation, may it is compliance requirement or compliance obligation (mandatory) or compliance commitment (voluntary);
- Legal risk arises where there is legal relation between legal subject, and one of or both parties is violating the rule of conduct (existing positive law) relating to rights, obligations and responsibilities;

• In the compliance risk, most likely there is also the aspect of legal risk.

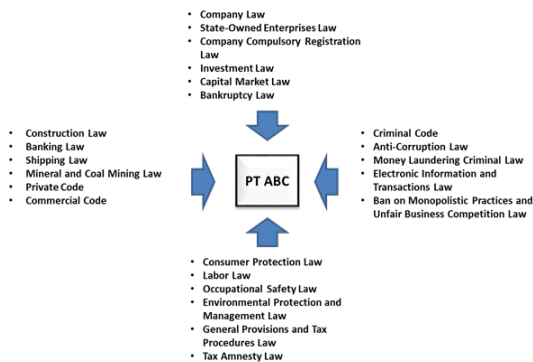


Figure 3. Compliance Risk: Regulatory Risk

Figure 3 shows a small picture of a company in Indonesia in the context of legal environment. Some of the companies do not really realize that they are facing a lot of legal regulations. For example, according to Mr. Susilo, there are around 70 legal regulations in a company and there are around 300 legal regulations including local regulations in other companies. The regulations required compliance. Mr. Susilo said that there is only one way to mitigate the compliance risk, which is by complying.

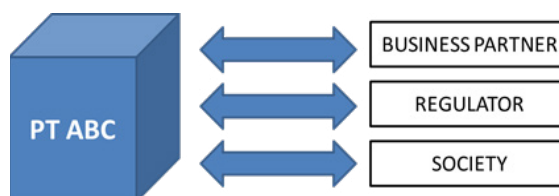


Figure 4. Legal Relation between the Legal Subject

As mentioned previously, legal risk arises when there is a legal relation between the legal subject (person and legal entity). Figure 4 shows the legal relation between PT ABC with their business partners, regulator, and society/community. Legal relation has also risks against business partners, regulator, and society/community.

To understand risk in legal relation better, these are some kinds of risk in legal relation against business partners, regulator, and society/community.

1. Against business partners:

- Contractual risk, in Indonesia called “wanprestasi”
- Tort, in Indonesia called “perbuatan melawan hukum”

2. Against regulator:

- A bank violates banking regulation
- A construction company violates safety building permit regulation

3. Against society/community:

- Violating environmental regulation
- Broadcasting pornographic items, hate speech
- Beware of Indonesian revised Legislation on electronic transaction and information.

Organizations cannot control the external compliance but they can control their internal compliance/voluntary boundary. In the context of achieving the corporate objectives, management defined boundary voluntarily which consist among others organizational values, contractual obligations, voluntary policies and other promises is called self-regulating compliance.

Self-regulating compliance also have its own compliance objectives. Compliance objectives are the objectives established within the policy of the compliance management system for both compliance requirement and compliance commitment.

When somebody failed to comply with the obligation, they will have consequences relevant to the binding agreement between the parties and the management.

These are the examples of self-regulating compliance:

- Agreements with community groups or non-governmental organizations;
- Agreements with public authorities and customers;
- Organizational requirements, such as policies and procedures;
- Voluntary labelling or environmental commitments;
- Obligations arising under contractual arrangements with the organization;
- Relevant organizational and industry standards;
- Voluntary principles or codes of practice, corporate ethics program;
- Whistle blowing system; and
- Fraud prevention and control program.

Legal and compliance risk are risks that organizations regularly face. As an illustration, Mr. Susilo shares about case studies in terms of legal risk or compliance risk, there are:

1. IM2 case – corporate criminal law case (2012 – 2014)

The court ruled the company was guilty of misusing Internet frequency licenses. The verdict has sent jitters to telecommunication companies as it emphasized legal uncertainty that could stunt the industry from expanding amid the high demand for faster Internet and data access. Presiding judge Antonious Widiantoro said at the court that he had found PT Indosat Mega Media (IM2) former president director Indar Atmanto guilty of enriching the company by mistreating the 2.1 GHz telecommunication frequency.

Final verdict by Supreme Court (2014):

- The defendant IA – President Director of PT

IM2 is found guilty and punished for 8 years in prison plus fine in the amount of IDR 300 Million or replaced by 6 months in prison

- Punished PT IM2 to pay fine in the amount of IDR 1.358 Trillion or its assets will be confiscated by the law;
- Judicial review of the cassation is rejected (2016)

2. MPL case – corporate private law case (2014 – 2016)

A landmark Supreme Court ruling ordering a plantation company to pay a high fine for illegal forest clearing is expected to serve as a deterrent for companies that seek to engage in deforestation. The Supreme Court ruled that PT Merbau Pelalawan Lestari (MPL) was guilty of illegally clearing forests in Pelalawan Regency, Riau, from 2004 to 2006. The pulp and paper company was ordered to pay IDR 16 trillion (US\$1.19 billion) in fines, the highest of any case of environmental destruction in the nation's history.

Final verdict by Supreme Court (2016):

- The defendant PT MPL is found guilty to commit tort by conducting illegal logging within the area of IUPHHK-HT (Business License for the Utilization of Forest Timber Products in Plantation Forest) and outside the area of IUPHHK-HT that destroyed environment and pollution;
- Punished the defendant PT MPL to pay fine in the amount of IDR 16.2 Trillion which consist of:
 - IDR 12.167 Trillion for destroying the environment of 5.590 ha of forest area within IUPHHK-HT area; and
 - IDR 4.076 Trillion for destroying the environment of 1.873 ha of forest area outside IUPHHK-HT area.

Part 2

Prof. Dr. Normah Omar, CPA Accounting Research Institute (ARI) Higher Institutions' Centre of Excellence (HICoE) Universiti Teknologi MARA Malaysia

According to Tobias Mahler, legal risk is a risk that has a legal issue as its source. A legal issue is a set of facts that are assessed under a set of legal norms. Criminal act, security exchange, copyright, warranty, financial reporting, corruption, code of ethics, code of corporate governance are the examples of legal risks. According to Prof. Omar, legal costs can range from 3% to 10% of business annual revenues.

In Malaysia, if organizations do not comply with the code of corporate governance and they are a listed company, there will be some legal implications. Therefore, organizations need to have a good method not only for managing legal risks but also compliance and regulatory risks.

There are many examples of legal risks. Falsification of financial statements and corruption in the examples of legal risk are the part of fraud risks which is also part of legal risks. In the broadest sense, fraud can encompass any crime for gain that uses deception as its principal modus operandus.

Fraud includes any intentional or deliberate act to deprive another of property or money by guile, deception, or other unfair means. Fraud looked like an iceberg, just a few of many events that are reported. A lot of companies do not want to report frauds, because it will involve reputational risks. The higher level of fraud occurring in a company, the

worse its reputation will get. Fraud against a company can be committed either internally by employees, managers, officers, owners of the company, or externally by customers, vendors, and other parties.

Internal fraud, or also known as occupational fraud, can be defined as: “the use of one’s occupation for personal enrichment through the deliberate misuse or misapplication of the organization’s resources or assets”. Whereas, external fraud can cover a broad range of schemes such as:

- Dishonest vendors might engage in bid-rigging schemes, bill the company for goods or services not provided, or demand bribes from employees.
- Dishonest customers might submit bad checks or falsified account information for payment, or might attempt to return stolen or knock-off products for a refund.
- Security breaches and thefts of intellectual property perpetrated by unknown third parties.
- Hacking, theft of proprietary information, tax fraud, bankruptcy fraud, insurance fraud, healthcare fraud, and loan fraud.

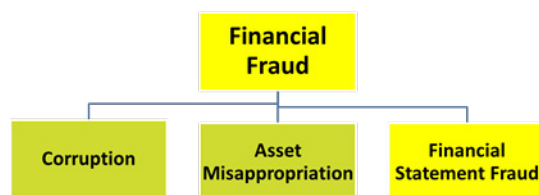


Figure 1. Types of Financial Fraud

One of the most common frauds in an organization is financial fraud. Financial fraud can be broadly defined as an intentional act of deception involving financial transactions for purpose of personal gain. Fraud is a crime, and also is a civil law violation.

In figure 1, there are three specific financial frauds in organizations: corruption, asset misappropriation, and financial statement fraud. Asset misappropriation can be exemplified as: when someone buys a company’s asset but he/she places it in his/her ownership. Financial statement fraud can be committed by the people in an organization, e.g. accountant or auditors.

To solve the fraud cases, an organization need to know why their employees commit financial statement. According to Prof. Omar, they commit financial statement fraud because of:

- It pays to do it (risk vs bottom line);
- It is unlikely that you will get caught;
- Weak governance/internal control;
- No/weak code of ethics;
- Accommodating auditors, attorneys, analysts and regulators;
- “Over-powering” CEO and Insider Board Influence;
- Competence and integrity of auditors; and
- Focus on Short-Term Performance Goals.

Financial statement fraud may involve the company’s income statement, balance sheet, and cash flow. The responsibility to make sure that the financial statement is true and accurate is coming from the BOD. That means, the BOD has a very important responsibility to ensure that the financial statement is not rigged.

Financial statement fraud also has a consequence or effect if it happens. Figure 2 shows what kind possible effect of financial statement fraud could happen in an organization.

No	Possible Effects of Financial Statement Frauds
1	Undermines the reliability, quality, transparency and integrity of the financial reporting process
2	Jeopardizes the integrity and objectivity of the auditing profession, auditors and auditing firms
3	Diminishes the confidence of the capital markets, market participants and reliability of financial information
4	Makes the capital markets less efficient
5	Adversely affects the nation's economic growth and prosperity
6	Results in huge litigation costs
7	Destroys careers of individuals involved in financial statement fraud.
8	Causes bankruptcy or economic losses by the company engaged in financial statement fraud
9	Encourages regulatory intervention
10	Causes devastation in the normal operations and performance of alleged companies
11	Raises serious doubt about the efficacy of financial statement audits
12	Erodes public confidence and trust in the accounting and auditing profession

Figure 2. Possible Effects of Financial Frauds

The ACFE (Association of Certified Fraud Examiners) has identified five classifications of financial statement fraud. What follows are the classifications, supplemented by some risk factors cited in the SAS 99 Appendix, "Examples of Fraud Risk Factors."

1. Fictitious Revenue

- Significant, unusual, or highly complex transactions, especially those which close to the end period that pose difficult 'substance over form' questions.
- Overly complex organizational structure involving unusual legal entities or managerial lines of authority.
- Significant related-party transactions not in the ordinary course of business or with related entities not audited or audited by another firm.

Examples of items to watch:

- Fictitious or altered invoices.
 - Sales with conditions that have not been met.
 - Merchandise shipped to warehouses for storage or consignment counted as sales.
- Significant transactions with related parties or special purpose entities (e.g. Enron), or entities whose substance and ownership are not known.

2. Timing Differences

Examples of items to watch for:

- "Billing and holding" schemes (creating receivable but holding the goods for a later shipping, or not shipping at all; often used with large customers).
- Multi-year projects for which the majority of cash is paid in the first year, but revenue is not spread out over the number of years required for the project (common in the construction business).
- Subscription revenue taken for a multi-year period, obligating the company to multi-year expenses, but all of the revenue is recognized in a one-year period.
- Backdated sales invoices and predated shipments.
- Large journal entries at year end.

3. Improper Asset Valuations

Examples of items to watch:

- Fictitious records for items that do not exist.
- Unsupported journal entries.
- Inflated inventory count sheets.
- Bogus shipping and receiving reports.
- Fake purchase orders/account receivable.
- Backdated investment documents to report fixed assets at market values.

4. Concealed Liabilities/Expenses

Examples of items to watch:

- Pending legal, disciplinary or regulatory actions, investigations or inquiries not disclosed by management.
- Capitalizing expenses as assets (e.g. WorldCom).
- Expensing capital expenditures (to minimize tax liabilities).
- Expenses shifted to a later or earlier period.

5. Improper Disclosures

Examples of items to watch:

- Management failing to disclose significant information such as:
 - Loan covenants
 - Contingent liabilities
 - Court judgments
 - Regulatory decisions
 - Related party transactions
- The use of confusing footnotes (e.g. Enron).
- Footnotes inadequately describing the qualitative nature of investment.

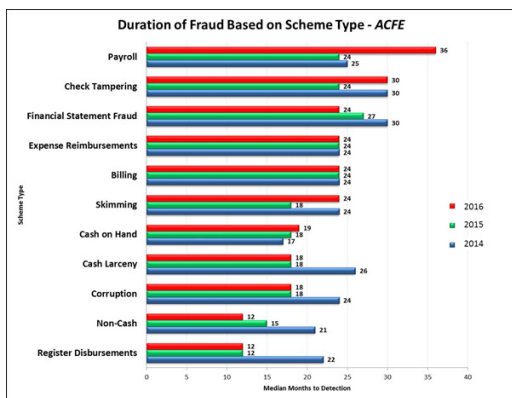


Figure 3. Median Duration of Fraud Based on Scheme Type

To detect occupational fraud is not easy, and it takes a long time. Figure 3 shows the duration of fraud based on scheme type. For example, as seen in Figure 3, the typical cash register disbursement scheme was uncovered the most quickly, with a median duration of 12 months. In contrast, payroll, check tampering, financial statement fraud, expense reimbursements, and billing schemes all lasted a median of two years before being detected.

Problems would occur if organizations take too much time to detect the occupational fraud. The longer an occupational fraud scheme goes undetected, the greater the losses tend to be.

Prof. Omar shared one theory about fraud which explains how the fraud can happen in the workplace. It is called Fraud Diamond theory. The Fraud Diamond theory is a newer theory of fraud proposed by David T. Wolfe and Dana R. Hermanson.

Essentially, there are four elements of the Fraud Diamond Theory, which are Opportunity, Pressure (also known as incentive or motivation), Rationalization (sometimes called justification or attitude) and Capability. For a fraud to occur, all four elements must be present.

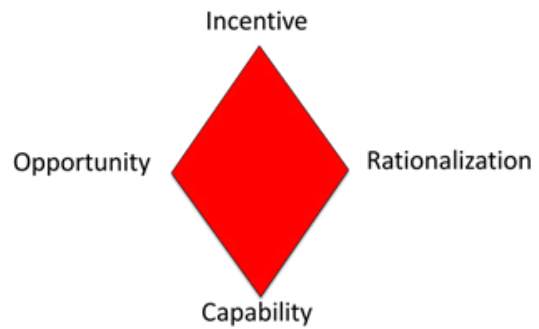


Figure 4. Fraud Diamond Theory

This is some explanations about each element in the fraud diamond theory according to the National Association of State Auditors, Comptrollers and Treasurers (NASACT) and the Oregon State Controller’s Division:

1. Opportunity

If one is talking about theft, there must be something to steal and a way to steal it. Anything of value is something to steal. Any weakness in a system—for example, lack of oversight—is a way to steal.

Examples of opportunity by Prof. Omar:

- There is a weakness in the system that the right person could exploit. Fraud is possible;
- Lack of controls that prevent fraudulent behaviour inability to judge quality of performance;
- Failure to discipline fraud perpetrators;
- Lack of access to information;
- Ignorance; and
- Lack of audit trail.

2. Incentive/Pressure

Pressure in this case is another way of saying motivation. What is it in one's life that drives one to commit fraud? Pressure sometimes involves personal situations that create a demand for more money; such situations might include vices like drug use, gambling or merely life events like a spouse losing a job. At other times, pressure arises from problems on the job; unrealistic performance targets may provide the motive to perpetrate fraud.

Examples of incentive/pressure by Prof. Omar:

- I want to, or have a need to, commit fraud;
- Financial pressure;
- Vices – addictions such as gambling, drugs;
- Work-related pressures; and
- Other pressures.

3. Rationalization

There are two aspects of rationalization. One, the fraudster must conclude that the gain to be realized from a fraudulent activity outweighs the possibility for detection. Two, the fraudster needs to justify the fraud. Justification can be related to job dissatisfaction or perceived entitlement or saving one's family, possessions or status. Rationalization is discernable by observation of the fraudster's comments or attitudes.

Examples of rationalization by Prof. Omar:

- I have convinced myself that this fraudulent behavior is worth the risks;
- The organization owe it to me;
- I am only borrowing the money – I will pay it back;
- Nobody will get hurt;
- I deserve more;
- It's for a good purpose;
- We'll fix the books as soon as we are out of this financial difficulty; and
- Something has to be sacrificed.

4. Capability

The fraudster, it is said, must have the required traits (e.g., greed, weakness of character, excessive pride, dishonesty, etc.) and abilities (e.g., knowledge of processes and controls) to actually commit the fraud. It can be argued, however, that traits are components of pressure and that abilities are opportunity factors.

Examples of capability by Prof. Omar:

- A person's specialized position or function within the organization that provides him/her the ability to create or exploit an opportunity for fraud not available to others;
- A person who is smart enough to understand and exploit internal control weaknesses and to use his or her position, function, experience or authorized access to the greatest advantage;
- A risk taker has a strong ego and great confidence and believes that he or she could easily talk himself out of trouble if caught;
- A person with a very persuasive, coercive personality who has the ability to influence and convince others to go along with a fraud or simply look the other way to commit fraud; or
- A successful fraudster who lies effectively and consistently to avoid detection and who possesses the skill to keep track of the lies, so that the overall story remains consistent.

In the explanations by Prof. Omar, there are some fraud risk indicators for the fraud diamond theory, including:

1. Opportunity Fraud Risk Indicators

- Inadequate monitoring of significant internal controls;
- High turnover of chief executive officers or board directors;
- Ineffective BOD or AC oversight over the financial reporting process and ICS;
- Assets/liabilities/revenues/expenses based on estimates that involve subjective judgments; and
- Significant, unusual, or highly complex transactions, especially occurring close to year end.

2. Incentive/Pressure Fraud Risk Indicators

- Management and/or board directors holding significant financial interests in the entity;
- Operating losses causing threat of imminent bankruptcy/foreclosure/hostile takeover;
- High vulnerability to rapid changes in technology, product obsolescence, or interest rates;
- New accounting, statutory or regulatory requirements; and
- High degree of competition or market saturation accompanied by declining margins.

3. Rationalization Fraud Risk Indicators

- Frequent disputes with the current or predecessor auditor on accounting/auditing matters;
- Management failure to correct known reportable conditions in internal controls in a timely basis;
- Excessive interest by management to maintain or increase the entity's stock price or earnings trend;
- Formal or informal restrictions on the auditor that limit his access to people or information; and

- Ineffective communication or enforcement of the entity's values/ethical standards by management.

Prof. Omar also shared a research or an empirical study from CPA Australia entitled Importance and Usage of Fraud Risk Indicators (ISA 240) by Auditors. This research involves 91 external auditors, 113 internal auditors, and 109 government auditors as respondents. The respondents come many demographic traits such as: gender, type of auditors, years in audit experience, and highest educational qualifications.

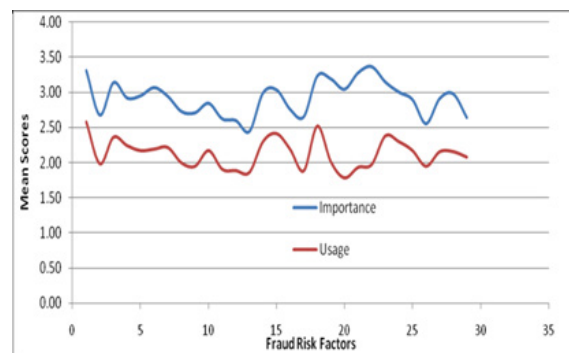


Figure 5. Opportunity – Level of Importance versus Level of Use

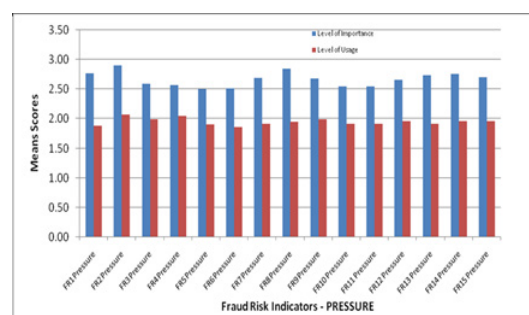


Figure 6. Incentive/Pressure – Level of Importance versus Level of Use

Figure 5 and 6 show the level of importance (LoI) and level of use (LoU) in opportunity and incentive/pressure fraud risk indicator. Figure 5 shows that, in fraud risk indicator (FRI) for

opportunity element, they put the LoI at range level between 2,5 – 3,5. Meanwhile, they put the LoU at range level between 2,0 – 2,5. In figure 6 or FRI for incentive/pressure element, their put the LoI at range level between 2,5 – 3,0. Meanwhile, they put LoU at range level between 1,5 – 2,0 except the block FR 2 Pressure, it at the level above 2,0.

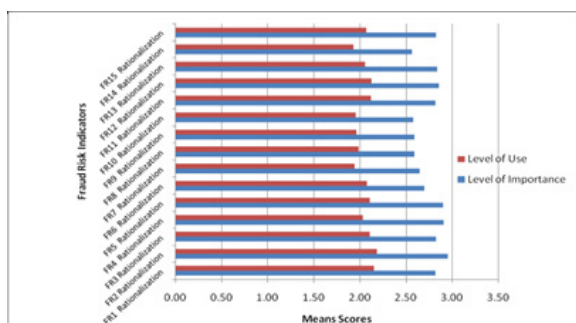


Figure 7. Rationalization - Level of Importance versus Level of Use

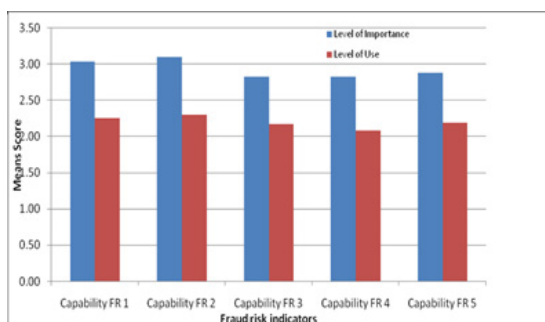


Figure 8. Capability - Level of Importance versus Level of Use

Figure 7 and 8 show the level of importance (LoI) and level of use (LoU) in rationalization and capability fraud risk indicator. In figure 7 or FRI for rationalization element, they put the LoI at range level between 2,5 – 3,0. They put LoU at range level between 2,0 – 2,5 and some others at the level below 2,0.

In figure 8 or FRI for capability element, their put the LoI at range level between 2,5 – 3,0 and two of others at the level above 3,0. Meanwhile, they put LoU at range level between 2,0 – 2,5.

From figure 5 until figure 8, there are 4 elements in fraud diamond theory, all of them have LoI with range level between 2,5 – 3,5. In the other side, all of them have LoU with range level between 1,5 – 2,5. These mean, there are still very much of the auditors that have not implemented FRI, whereas most of them agreed that FRI need to be implemented.

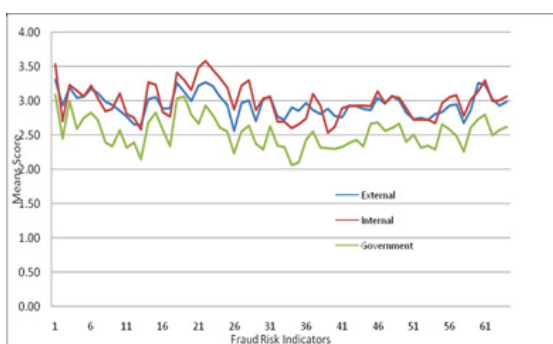


Figure 9. Level of Importance – External, Internal, and Government Auditors

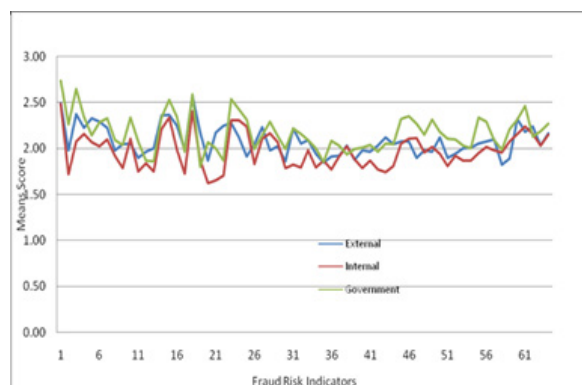


Figure 10. Level of Use – External, Internal, and Government Auditors

In the figure 9 and 10, it show LoI and LoU divided based on types of auditors (internal, external, and government). From mean score 0 – 4,0, each of auditors put the LoI FRI at the

level 2,5 – 4,0; 2,5 – 3,5; 2,0 – 3,5 and LoU FRI at the level 1,5 – 2,5; 1,5 – 2,5; 1,5 – 3,0.

When seen deeper, government auditors have LoU mean score higher than internal and external auditors and LoI of itself.

Therefore, most of government auditors have implemented the fraud risk indicators.



Figure 11. Fraud Prevention Mechanisms

Overall, the figures show that most of auditors think the fraud risk indicators is important, but they are not using it in their audit. The big

question is why? Why indicators perceived as important but organizations are still not using it? It can be sourced from managerial and professional implications or the competency issue and it should be discussed.

Moreover, fraud risk should be prevented and it should come from BOD, audit committee, external auditors, internal auditors at all level. Figure 11 explains that, to make fraud prevention running as it should be, fraud prevention must be run from the top-level management, starting from BOD, audit committee, external auditors, internal auditors, and then anti-fraud specialist.

Written by: **Fransiskus Bobby Wijaya**

CONCLUSION

As the world is changing to be more digitalized, it brings changes on legal environment, especially in rules and regulations. There are some negative impacts/ consequences if organizations do not take a concern about it.

Generally, the consequences are reflected on financial aspects. To address the challenges from this new environment, organizations must be ready in their legal and compliance aspects.

On the fraud side, the development of technology can make fraud easier. Nevertheless, technology could also be useful to prevent fraud depending on an organization's capabilities and treatments. Thus, the synergy between top-level and bottom-level management (between organization and their employee) in an organization is really needed, particularly for top-level management.

THE NEW FACE OF FINANCIAL RISK MANAGEMENT IN THE NEXT DECADE

Talk Show



BALI
ERM
2016

The New Face of Financial Risk Management in the Next Decade

Presented by:

Aurelie Saada

Head of Enterprise Risk Management at AIG Asia Pacific

Kenji Fujii

Head of Global Risk Management, Mizuho Securities Co., Ltd.
Chair of Tokyo Risk Managers Association (TRMA)

Benito Mable

Vice President & Head, New Opportunities Tokio Marine Asia
Pte. Ltd. Singapore

Hosted by:

Irwan Habsjah, MBA, CERG

Commissioner and Chair of Risk Oversight Committee of BTPN;
Board Member Indonesia National Committee on Governance

The rapid changes of technology in the digital era create more risks for the business industries. Financial industry is one of the field of businesses that mostly affected by this Therefore, in this new digital era, some new risks related to the financial industry might arise. This session discussed about the new face of financial risk management in the next decade.

This talk show session was hosted by Mr. Irwan Habsyah and presented by 3 keynote speakers: Mrs. Aurelie Saada, Mr. Kenji Fujii, and Mr. Benito Mable. Mr. Irwan Habsyah is the Commissioner and Chair of Risk Oversight Committee of BTPN, and the Board Member Indonesia National Committee on Governance. He has 35 year of experiences in banking industry.

The first speaker of this session, Mrs. Aurelie Saada, is the Head of Enterprise Risk Management at AIG Asia Pacific Insurance, based in Singapore. Before that, Mrs. Aurelie Saada was a Senior Vice President, Operational Risk and Internal Control of HSBC private bank.

The second speaker, Mr. Kenji Fujii, is the Director of Mizuho Securities, Co. Ltd., Head of Global Risk Management. He has more than 30 year of experience in the capital market and has become a fulltime risk manager in the last 20 years. Most of his career as a risk manager is in the capital market and trading industries.

The third speaker was Mr. Benito Mable, the Vice President & Head, New Opportunities Tokio Marine Asia Pte. Ltd, Singapore. He is a Senior Executive with broad experience in multi channels distribution and marketing management. In this session, Mr. Benito Mable talked about risk from the marketing perspectives.

In the beginning of this talk show session, Mr. Irwan Habsyah talked about the most recent digital environment that we have to face. The development of technology and digital environment has moved rapidly in the past ten years. These changes will create a new face of financial risk management.

Fast moving technology, the development of digital era, and the changes on cybersecurity perspective will affect a lot on the industry, including the financial industry. The financial institution obviously cannot escape and runaway from these facts. The companies should embrace this new digital era. The aspects of risk in financial industry need to be further clarified and developed.

Part 1

Aurelie Saada

Head of Enterprise Risk Management at AIG Asia Pacific

In this talk show session, Mrs. Aurelie Saada was given the first chance to deliver her opinion about the developing digital environment and her vision about what are companies going to face in the future regarding the financial risk management in insurance industry.

Insurance business is one aspect of financial industries that is really impacted by new technology and digital changes. This technology development will also affect the way companies do their business, which is important for the insurance industries to adapt with such conditions.

In this digital era, the insurance institution helps corporations to be able to monitor the cyber threats and to protect themselves against those threats. Insurance companies also encourage some cyber risk policies that could help the companies and also protect them from any losses regarding these cyber risks.

Cyber risk is one of the biggest challenges both for the clients and the insurance companies itself in this digital era. Thus, the insurance

companies have to identify and assess these cyber risks before making some decisions.

The changes in the technology in this emerging digital era will change the assessment process performed by the insurance companies and its result. This assessment will change every year since there are changes in technology, new players in the market, and/or events that could change the company's risk rating.

After undergoing the assessment system, another important thing is what insurance companies are going to do with these risks once they are quantified. This is how insurance companies can mitigate those risks. Another thing should that should be noted is that a company should also align the risk appetite with the company's strategy and determine how much investment they want to spend regarding the cyber issues.

Mrs. Aurelie Saada also said that companies actually never know what exactly will happen in the future. However, one thing for sure is that changes will happen, whatever the changes are. In facing these rapidly changes in technology, insurance companies need the flexible mind to identify the risks and find out how to deal with those risks. The companies should always be ready with those changes.

Besides those cyber risk and technology changes, another challenge in this digital era is that insurance companies sometimes have to face some more moral hazard in running their business. One of the moral hazard is about the money laundering. It is possible for a client to buy the policy just for taking advantage over it, for example to avoid paying for the tax.

In order to manage this risk, Aurelie Saada said that her company has made more and more

requirements regarding the buying policy. Besides that, the regulators in Singapore also have acted more sensitive and strictly considering these issues. The regulators in Singapore make more requirements for the insurance company in running their business.

Part 2

Kenji Fujii

Head of Global Risk Management,
Mizuho Securities Co., Ltd.

Chair of Tokyo Risk Managers
Association (TRMA)

In the second session, Mr. Kenji Fujii commented on what actually are happening right now in the banking industry regarding the development of technology, what are the opportunity considering those things, and what kind of risk and risk management should be implemented in the banking industry in this digital era.

In this digital era, it is much easier for people to do transactions. Transactions become faster in the practice due to the supports from technologies. One of the examples of the change in the way we do business in financial industry is the mobile banking system. Transferring money using any mobile device shows us that changes in technology greatly impact the way that the banking industry run their business; everything become faster and easier.

In this session, Mr. Kenji also explained about the High Frequency Trading capacity. This platform enables a much faster transaction. Mizuho actually has a system that facilitates half millisecond transactions. This means that in just 1 second, this system will be able to finish around 5000 transactions. This platform also provides the need of the institutional investors.

The institutional investors usually try to avoid the market impact of their investment, when buying or selling securities. Therefore, they want to make more frequent investment in small amount in order to avoid those market impacts. Thus, High Frequency Trading can actually answer their needs.

The development of those very fast transactions system will lead to another risk or potential hazards for the trading industries. It is actually impossible for risk managers to oversight every transaction in one second. If something wrong is happening, like insider trading, it is impossible to see that insider trading among those 5000 transactions. This is one of the issues that company should consider.

On the banking side, the digital technology (like blockchain) could reduce the operation processes, which eventually reduce the cost. Global technology in asset management also provides the AI capacity to make new investment. From this argumentation, we can see some evidences that the development of fintech can also bring opportunity for the financial companies in running their business.

Another issue in running the financial services is about the cyber security. The stakeholders sometimes try to take advantage of these high-speed transactions and there will always be people who are trying to make a fraud. These people are actually well-organized and have the fund to support the activities. They could make insider trading in order to take advantage in the capital market.

Therefore, it is a challenge for any banking industry or security industry to manage this risk. It is also a challenge for regulators to catch more insider trading practice in the financial industry.

Cyber security issue is actually not only the issue of banking or security companies. However, it is the issue of one program of all the industries, whether the risk is in public or private sector. Considering these conditions, the collaboration between industry and regulators is needed. From Mizuho's perspective, the cyber security issue should not become the responsibility of Mizuho security only, but it has also to be the effort of Mizuho financial group as a whole.

Continuing his view, Mr. Kenji Fujii then started to discuss the market crashes. What is going to happen if the market crashes and what is going to happen if the automatic trading functions go wrong beyond our expectation? According to Mr. Kenji Fujii, if it happens in the transaction systems, the financial institution have to stop it, otherwise the companies will lose money.

How about the malfunctioning? In this case, risk managers have to have courage to stop the malfunctioning of trader system or the market. If something happens, the financial institutions have to stop whatever that works improperly. The companies should also have the procedures to stop since it concerns very huge transactions. Those are some of the challenges that the financial institutions have to face.

Part 3

Benito Mable

Vice President & Head, New Opportunities Tokio Marine Asia Pte. Ltd. Singapore

The talk show continued to talk about the risks in financial industries from the marketing perspective. In this part, Mr. Benito Mable shared his experience from the marketing perspective for insurance industry.

Entering the marketing perspectives, Mr. Benito began to discuss the customer side of this financial industries business. In this digital evolution, customers are the center of the risks. Actually, it is not really about how complex the technology is; it is just about finding the new way in doing something according to the customers.

It is about the customer; they are looking in the new ways to engage with the companies and looking new ways to transfer their money. Running the insurance business, the insurance companies should facilitate that engagement. From a risk manager perspective, the companies need to come up with the new way to understand the data in front of them. The data are useless if companies do not get any insight from the data.

Mr. Benito said that today the insurance companies can use millions of data to develop more attractive product and make consumer more willing to deal with the products. Customer sometimes gets frustrated with the products offered because they don't understand the products. Sometimes the product offered by insurance companies to the customer is too complicated and not suitable with their need.

If insurance companies can understand the customer's need, it will be much easier to manage the risk. It is the answer of how to engage with the customers related to the product in order to willingly engage with them. Mr. Benito explained that the main point is that their product right now should be more customer centric and customer driven. The development of products should pay more attention to this issue.

After all of the keynote speakers told their perspectives and views, the moderator continued to ask about the regulators in the financial industries. It seems that regulators are sometimes left behind in the technology. Also, the products are developing so fast that the regulators may actually do not understand about what is going on. While to say the least, regulators are supposed to overview the whole risks of the industry.

According to Mrs. Aurelie Saada, if regulators are left behind, they tend to contradict with what the companies actually want to achieve. The regulators around the world actually better to work together and to define some new agencies or monitoring systems about this cyber risk threats.

In the ASEAN region, some agreements can also be made among the member countries in order to be able to work together and develop each of their countries' expertise in managing such kind of risks.

The risk in the cyber world is actually enormous that we need to collaborate and share the competencies among the countries. The main point is that we can fight against the threat coming up from the cyber security issues.

Talking about the regulators in Singapore, Mrs. Aurelie Saada explained that the Monetary Authority of Singapore (MAS) is quite sensitive for being aware and step ahead into the regulation. In the middle of 2016, they have issued a consultative paper regarding their willing to create the sandbox.

The MAS published its "regulatory sandbox" guidelines to encourage and enable experimentation of solutions that utilize technology innovatively to deliver financial

products or services. This shows that regulators in Singapore are actually aware that cyber risk happens around us recently.

In this session, Mr. Kenji also explained his perspective about the regulators. Since he attended the Fintech Festival in Singapore and had a chance to talk with Federal Reserve Bank (FRB) New York who said that right now cyber risk is the top risk for them. It is also common in Tokyo, that Securities and Exchange Commissions (SEC) in Japan sees cyber risk as one of the top priority.

Moreover, SEC in the US is more concerned to the cyber security. Mr. Kenji Fujii suggested that it would be great if there is something like global regulatory community like Basel concerning about the cyber risk. It should not only be able to be implemented in one individual country, but also in global financial industry as a whole.

Mr. Kenji also gave his opinion about the regtech (regulation technology). It is about how to introduce financial technology into the regulators. For example, we have a lot of regulatory reports submitted to the regulators that can be automated (possibly using blockchain) and also the settlement with the central bank that can be requested by the blockchain.

As the technology develops rapidly, some challenges arise from the regulators regarding the development of more digital type of products. From Mr. Benito's perspectives, sometimes the regulators aren't keeping up with the development of digital products. To answer this challenge, the financial institution

should share the common understanding with the regulators (what is the risk and the opportunity).

The financial institution and the regulators should collaborate so that the regulators become more informed about the financial industry when they come up with their regulation. This can also minimize the financial institution to make a costly adoption process regarding those regulations.

In the final topic of this session, Mr. Irwan Habsyah led the discussion to talk about the investment against the cyber risk. Every keynote speaker obviously agreed that this effort needs a lot of investment. According to Mrs. Aurelie, the companies cannot deny that cyber risk has become one of the major risks that have to be faced in this developing digital era. Therefore, the investment for facing this risk should be well considered.

Mr. Kenji Fujii commented that actually no one can assure how much investment will be sufficient to manage the cyber risk in the digital era. However, this investment is obviously enormous. It is actually hard for one company to bear all of this cost alone. One of the solutions regarding this investment issue is by sharing the cost to treat this cyber risk. Collaboration is one of the keys to face this challenge.

Written by: Reynaldi Hartanto

CONCLUSION

The development of digital era will obviously affect any industry in the business environment, including the financial industry. The financial institutions cannot predict about what exactly will happen in the next decade, but changes absolutely will happen. The main point is that the companies must be ready when these changes happened. One of the evidence of such changes is about the technology in transactions.

Nowadays, transaction system has become much faster. Managing risks in such fast and huge transaction systems bring more challenges to the financial industry. From the marketing perspective, the products that financial institutions offer to their customer should be more customers driven. This means that the products should match with the customers' need.

Managing risks in financial industries must also be related with the regulators that regulate the industry. The role of regulators becomes more important for financial industries. There should be collaboration among the regulators around the world to share a common and comprehensive understanding in managing cyber risks in financial perspectives. Besides that, the regulators should always keep up with the changes of digital environment and collaborate with the financial institutions in order to create supportive business environment

THE JOURNEY OF RISK MANAGEMENT IMPLEMENTATION IN STATE- OWNED ENTERPRISES - EMBRACING DIGITAL ERA

(Keynote)



BALI
ERM
2016

The Journey of Risk Management Implementation in State-Owned Enterprises – Embracing Digital Era

Presented by:

**Dr. Gatot Trihargo, Ak., MAFIS, CA,
QIA, CFE**

Deputy Minister of Financial Services, Survey, and Consulting
Indonesia Ministry of State-Owned Enterprise

Hosted by:

Dr. Antonius Alijoyo, ERMCP, CERG

Chairman of Enterprise Risk Management Academy

This digital era has intensified customer power as well as created new competitions. In this era, the market is driven by customer behavior. According to Mr. Trihargo, in the past, people tend to focus on business to business, but now the focus has changed to customer to business. This means that organization is becoming more customers based in the process.

Moreover, with many technology innovations, deteriorating industry boundaries, regulatory compliance, and pressure of profitability, the competition will heat up. Hence, emerging new businesses that are more digital can be a threat in the future.

Additionally, digital era also brings a new chapter to the business environment. Current business will move from digital business to autonomous business era. This means that human involvement will be minimized because processes, programs, people, and products/services will be changed into be more digitalized.

Successful platform implementation and strong position are the keys in autonomous business era. This challenge shows that Indonesian government should be prepared for it. According to Mr. Trihargo, the Indonesian Ministry of State-owned Enterprise (SOE) already planned the strategy to face the autonomous business era. Soon, Indonesian SOE will establish new database.

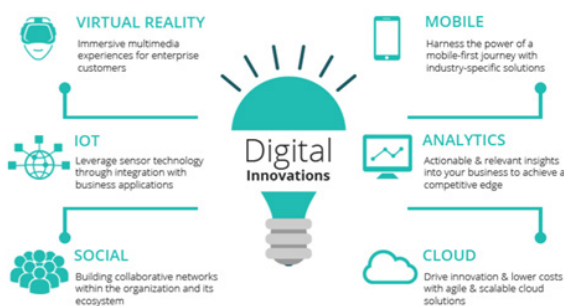


Figure 1. VISMAC in Digital Transformation

With the challenging environment, organizations are required to evolve their business process and adapt to newer technologies. VISMAC (Virtual Reality, IoT, Social, Business analytics, and Cloud) is an example of tools to upscale organization's business process and adapt it to newer technology.

By using VISMAC, organizations can transform their business with digital solution (see figure 1). This can help organization to build the foundation to transform their business into

future digital enterprises where organization can relate to their customers, interact with employees, and bring products and services to market.

While VISMAC can help organization to be more digitalized, there are several new risks that emerge due to this digital era. Those risks are:

1. In this digital era, there is a new risk and one of them is hacking. We should be prepared for this kind of attacks and considering what data are at risk;

2. There are many gadgets that can be used to access our data. We should know what kind of devices that will be used to access our data. Moreover, in this digital era, devices are easily changing;

3. Digital era allows us to access many data. The question is, do we understand the data that we obtain and how do we keep track of everything;

4. Cloud or cloud computing means storing and accessing data and program over the internet instead of computer's hard drive. If organizations use cloud, it is necessary to know where the data is and how their employees, customer and vendors access it;

5. Digitalization allows us to build collaborative environment that connects us with several people. Information that we share will be easily spread to many people. That is why it is necessary to know things that will be or being said, since it will affect our reputation;

6. If we are going to use digital system, we should understand how digital technology interacts. By knowing it, we will know what kind of risks that we are facing and how we will manage it.

The explanation above shows that in the digital era, several new risks are appearing due to the technology usage. When an organization digitalized its business process and something wrong happened to the system (e.g. cyber-attack), it will affect the whole organization process and the customer itself.

Mr. Trihargo said that 48% of Western critical infrastructure managers find it likely that cybercrime will take down critical infrastructure with potential loss of life. There are many kinds of cybercrime and they happened globally. Several examples of cyber-attack are as follow:

1. In Ukraine, the 1st power outage caused by cyber-attack suggests similar attacks possible around the globe. The attack caused six-hour outage for some 80,000 customers of Western Ukraine.

2. On 31st Dec 2015, BBC received a 602Gbps DDoS attack, the highest ever recorded in history. NewWorldHacking, who claimed responsibility, announced that it was a test of their power.

3. In Indonesia every day! That makes it the 2nd-most targeted country by cyber-attack after Vietnam, according to Yono Reksoprodjo, advisor to the Minister of Political, Legal and Security Affairs in his speech at Indonesia's National Cyber Agency, 8th Jun 2015.

4. Few weeks ago, a state bank under SOE has been skimmed, affecting 1000 cards. Although the perpetrators have already been caught, this incident requires organization to restore the money that has been stolen.

5. More than 100 million healthcare records compromised in 2015. Medical records are worth 10 times more than credit card information in the dark web.

The growth of digital era is also related with the escalation of fraud. According to research that was held by PricewaterhouseCoopers in 2015, security incidents were detected 38% higher than 2014. One example of security incident is the increase of "hard" intellectual property theft by 56%. The high possibilities of security incident makes organization increase their information security budget by 24% in 2015.

The increase of information and securities budget makes financial losses decreased by 5% from 2014 to 2015. Besides cyber-crime, another fraud that increases is fraud by internal party. Mr. Trihargo said that there are usually internal party that is involved in fraud cases.

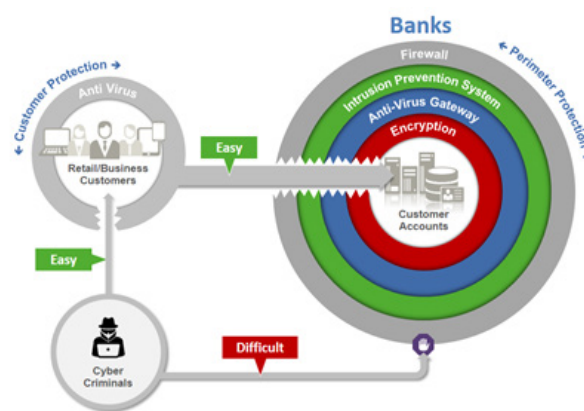


Figure 2. How Fraudster Attacks

Learning from the past events, Mr. Trihargo said that besides protecting organization system, it is important to take care of the stakeholder (e.g: customer) as well. In some cases, cyber-attack happened from customers. Customer is considered as the main target, because customers are assumed to have low protection system compared to organizations although they have an access to organization system (see figure 2).

If perpetrators directly attack internal system, it will be hard to hack that system. For example, in a bank, customers have, although limited, access to that bank system. The internal unit of the bank might apply strict protection system. However, customers that have limited access might not have sufficient digital protection. These customers do not have a tight protection system which could be an opportunity for bad people to access the bank system/data from them.

Therefore, the cybercrime perpetrators can pass to the bank system through customer. That is why, no matter how we protect our system with firewall, the fraudster can attack us from our weakest point which is our customer.

Overview of Indonesia State-Owned Enterprise in Digital Era

Indonesia could be one of the digital powerhouses in ASEAN. Indonesia will have 40% worth of US \$197 billion ASEAN's digital opportunity in 2030. This opportunity can lead Indonesia to have highest number of startups in region which are 29% (2033) of startups in ASEAN.

Moreover, with e-commerce is expected to reach US \$46 billion by 2025, Indonesia's internet economy will be worth US\$ 81 billion. To realize this prediction, Mr. Trihargo said that ecosystem components such as a talent-pool, payment mechanisms, stable and reliable connectivity, logistics infrastructures, and greater consumer trust should be improved.

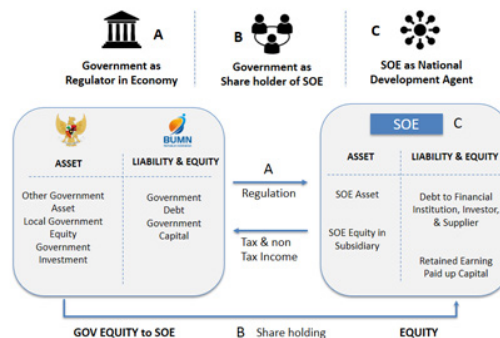


Figure 3. Government & SOE Relationship

Figure 3 shows the relationship between government and SOE. State budget and state owned enterprise (SOE) are two entities that helped Indonesian government in supporting its function in providing public goods and services.

Often, Indonesian state's budget is limited; therefore the support from SOE is needed. SOE is the entity owned by government and also is a tool that Indonesian government has to provide effective and efficient public needs. Although SOE is owned by government, it also has to pay tax and obey the regulation. Since government is one of its shareholders, SOE has the obligation to give dividend to the government.

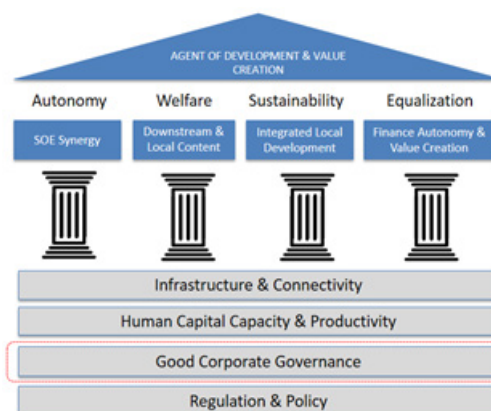


Figure 4. SOE Framework Roadmap

SOE's role is to become the agent of development and value creation. There are 4 strategic pillars (see figure 4) to support SOE function as agents of development and value creation, which comprise of Autonomy, Welfare, Sustainability and Equalization. SOEs strive to align these to aim for value creations and agents of development.

All four SOE components aim to encompass the essential components of a successful business and were developed to meet its functions as value creator and agents of development.

1. SOE synergy:

Synergy in SOE can be seen from its collaboration or consolidation of similar functions. SOE synergy intends to help SOE to realize economies of scale, reduce redundancy and inconsistency, and encourage the achievement of best practices. This synergy is performed by several state-owned enterprises which included in a group with similar value chain and cooperating with each other to optimize result and reduce redundancy.

2. Downstream and local content:

SOEs are increasing its participation in developing the support products (e.g. spare parts, machines, etc.) needed by various SOEs domestically. The goal of downstream and local content is to give value addition to the products in order to reduce costs, increase volume, and decrease raw material.

3. Integrated local development:

Various SOE are effectively integrating to drive economic development in several locations through project implementation that have the potential to create spill-over effect or to contribute in local regional empowerment (through creating job opportunities).

4. Finance autonomy and value creation:

To perform its function as value creator, SOEs need to be independent and financially sustainable. Other than that, they also need to create financial value outside of their role as the development agent. SOE is expected to find their own source of income, either from internal or external parties.

In implementing those pillars, foundation is required as a support. In this case, there are four things to support those pillars, which are: infrastructure and connectivity, human capital and productivity, good corporate governance, regulation and policy.

According to Mr. Trihargo, from those four foundations, Indonesian SOEs are emphasizing on the good corporate governance; hence both internal and external parties are expected to implement good corporate governance.



Figure 5. SOE Sectors in Indonesia

In Indonesia, there are 15 sectors in SOE (see figure 5) and each has their own risk driver. According to Mr. Trihargo, the most vulnerable sectors are telecommunication & digital and financial & banking. Those sectors are influenced by this digital era since they are growing fast.

For example, nowadays, majority of people are still using cash but in the future, there is a chance that people will start to pay with their gadget (using e-cash) rather than take their money from ATM. That event is likely to occur, since digital and telecommunication market is bigger than customers banking. To answer that challenge, SOEs in banking sector start to use technology, digitalized its services and strengthen its risk management to prepare for all possibilities that might happened.

Case Study Mandiri

In order to increase SOEs role, one of the supporting aspects that Mr. Trihargo highlighted is the digital aspect. In this digital era, it is necessary for banking and financial sector to adapt. As an example, Mandiri bank could simplify its business process as well as lowering the cost by digitalizing its services. Figure 6 shows the digitalized services in Mandiri bank.



Figure 6. Mandiri Non-Branch Channel

The usage of digital banking is rising because it simplified processes and organization must be prepared for risks that come along. Digital risk is different from conventional risk management. Therefore, it will be a challenge for banks to give customer the best experience and safety.

These are the example of risks that might appear in digitalizing the organization:

1. Increased velocity requirements to respond to risks in a 'hyper speed' interconnected digital environment
2. Changing risk profile of banks due to shifts in digital banking
3. Inadequate risk management processes and coherent information resulting in an inability to respond to risk events in timely manner
4. Digital infrastructure and technology innovation are raising new entry points of risks
5. The increasing dependence of banks on third parties that provide the necessary information technology & infrastructure.

Organization needs to consider action steps to overcome risk in digital era. The mitigation of those risks can include board management oversight, security controls, and legal & reputational risk management.

The board management oversight activity can refer to plan-do-control-action phase that is reflected in effective management oversight of e-banking activities, establishment of a comprehensive security control and management oversight process for outsourcing relationships. In security controls, Mandiri used the top-down approach to aim for transformation in these aspects:

1. Information Security Strategy

Information Security is business-back rather than technology-forward

2. Policies & Standards

Comply with international standards and specific requirements for critical assets

3. Technology Architecture

Protecting critical information within the perimeter. Technology architecture is structured along 5 dimensions:

- End-Point Security: Security controls that apply to end user devices, e.g. desktops, laptops, smartphones. Enabling the conduct of secure and efficient business process on all interfaces.
- Application Security: Security controls that apply to server-based applications, embedding security into the business frontend of IT (e.g. CRM systems, web-based systems)
- IT Infrastructure Security: Security controls that apply to IT Infrastructure, e.g. servers, switches, routers. These controls ensure the crucial security of the underlying infrastructure.
- Data Security: Security controls that protect data, overarching of location and status.

Guarantees safe data transfer, data monitoring, data loss prevention and other data safeguards.

- Perimeter/Network Security: Security controls that protect the physical and logical parameter around Mandiri's customer information & banking transaction. This includes ring-fencing of desktops, servers & infrastructure through e.g. firewalls & secured doors.

4. Operations & Processes

Information Security is a key business enabler and an integral part of all operations and processes

5. Organization & Governance

Information Security is a shared Business / IT responsibility with a strong governance process

Case Study Telkom

Telkom is a state-owned telecommunications enterprise that has Rp 418 trillion worth of market capital. Telkomsel, one of Telkom subsidiaries, has already covered (more or less) 99% of Indonesian population which makes Telkom as the largest telecommunications services company in Indonesia. Telkom could achieve that because they have already used the core standards when the others are still in the process to implement it.

The growth of telco business in digital era makes Telkom renewed its vision, mission and its strategic objectives. For 2016 – 2020, Telkom's vision is to be the king of digital region with a mission to lead Indonesia's digital innovation and globalization. Its new strategic objective is to be in the top 10 of market capitalization of telco in Asia-Pacific by 2020.

In the digital era, disruption cannot be avoided. Disruption usually has negative association which causes troubles and stopping something from continuing as usual, but in this digital era, disruption can have positive connotation. Nowadays, disruptive means something that is out of the box or out of establishment as a result from innovation in creating a new market and or a substitute of the existing market.

The digital era has a close relationship with disruption. Therefore in 2016, Telkom made an alignment to adapt in this situation especially in portfolio strategy and parenting strategy. In the portfolio strategy, Telkom is focusing on customer-facing strategy.

The strategy is used to improve customer value through Telkom digital TIMES (technology-information-media-edutainment system)

portfolio. While in parenting strategy, the working system is made to be simpler in order to establish more targeted and synergic control of its subsidiaries company.

When those strategic initiatives implemented in business functions. This transformation impacts Telkom's process across all functions and shapes 4 key digital Challenges:

1. Digital customer management: Leverages digital to boost sales and improve customer lifecycle while reducing cost-to-serve
2. Corporate transformation: Leverages digital to enhance corporate performance
3. Embracing digital and OTT Model: Provides innovative digital services to meet customer's expectations & leads to development of usage
4. Developing the pieces to build up a new ecosystem: Finds new external innovation levers and animates the right partners to boost its own innovation.

Meanwhile, since digital business is new business portfolio for Telkom, then there are some challenges such as shorter product life cycle, digital competency and different working

culture.

- Product life cycle: Creativity and innovation are very dominant in digital business, lots of products can become famous but often are not sustainable. Fast new product development, despite validation process is needed since product ideation, business modeling, market test and commercial test before the introduction to the market.
- Digital Competency: In Telkom, the new hired employees are trained with digitalization, thus they have a strong competency. But, the previous members that will give legacy to organization only have limited competency in digital business.
- Different Working Culture: Telkom already have their own culture which is living the Telkom Way, but the challenge is how to adopt digital culture in that organization culture. Moreover, the generation has already changed and it is necessary to fulfill millennial expectation.

Written by: **Belianny Putri**

CONCLUSION

In this digital era, market is rapidly changing and influenced more by customer. This situation brings new challenges to organization, and SOE is no exception. Indonesia's SOEs are still in the process to be digitalized. Digitalization can help organization to be more customer-centric, therefore it can give the best services to its customer. In the other hand, digitalization has also triggered new risk which is cyber risk.

In this digital era, big data is important because it contains our customer profiles. With the growth of cyber risk, those data could be in danger. Therefore, organizations need to be prepared so they can overcome this new risk and maintain their customer trust.

INTERNATIONAL PERSPECTIVE:

GRC towards Economic Value Addition



BALI
ERM
2016



International Perspective:
GRC towards Economic Value Addition

Presented by:

James Christopher Razook

IFC East Asia Pacific Corporate Governance Lead

Hosted by:

Leo J. Susilo, CERG

Principal of CRMS Indonesia

IFC is a global investment firm who acts as an active investor in the emerging market. As a global investment firm, IFC is working together with regulators and other companies to strengthen their governance framework.

With IFC, Mr. Razook has been working in the GRC environment for more than 15 years. He has provided assistance to central banks, capital market authorities, and other regulators. In this session, Mr. Razook shared his perspective regarding governance, risk, and compliance towards economic value addition.

According to Mr. Razook, emerging risks in the digital era, cyber security, and enterprise risk management are all framed by the corporate governance. Therefore, it is crucial for both financial and non-financial sector to have good corporate governance. For example, one of IFC's investee in Indonesia is a medical equipment supplier company.

This company's competitive advantage is not its medical equipment supplies, but its superior technology-based supply chain. Therefore, basically it is an IT company that provides medical equipment to the customers. Hence, having good corporate governance is a must.

Corporate governance is not only good for the company as an individual, but it also plays a big part in attracting investors into the market. According to IFC, there is a methodology to define corporate governance. This methodology consists of several elements including commitment to corporate governance, board effectiveness, shareholder and stakeholder relation, family governance, control environment and process, and disclosure and transparency.

Commitment to corporate governance is an assessment of overall level of commitment, formalization, and awareness of governance in the company. Board effectiveness is an assessment of board roles, composition, committee structure, procedures, and director duties within the company.

Shareholder and stakeholder relation is an assessment of shareholder rights and protections, AGM procedures, information to shareholders, and conflict or RPT (Related Party Transactions) policies.

Family governance is an assessment of family's role in the business and mechanisms used to govern the relationship with the shareholders. Control environment and process is an assessment of the overall effectiveness of internal controls, risk management, internal audit, external audit, and compliance.

Disclosure and transparency is an assessment of information disclosures to shareholders and the market, transparency of information, and accounting standards used by the company.

While corporate governance is important, IFC observed that there are some challenges for companies to implement it, especially in Indonesia. From the market-level challenge, many companies in Indonesia still see corporate governance as compliance rather than value-addition. Other than that, unclear business case, weak market forces, and the scarcity of qualified directors/commissioners have also become major challenges for implementing corporate governance.

For the firm-level, the challenges come from the lack of formal corporate governance framework, key-person risk assessment, undue shareholder influence, controlled/contrived board of directors/commissioners, conflicts of related party, and non-commercial frameworks of state-owned enterprises.

Now, as an investor, what does IFC search for from a company? According to Mr. Razook, IFC is looking for a company that has good practices with:

- Formal corporate governance framework which really functioning in practice;
- Balanced board;
- Clear director duties;
- Practices to manage conduct and conflict;
- Formal shareholder rights and practices; and
- Other specific minority protections.

Finally, to improve Indonesia's good corporate governance, Mr. Razook said that we need to:

- Continue educating companies on the business case;

- Reach out beyond the top listed companies;
 - Sharpen focus on state-owned enterprises and family-owned enterprises;
 - Emphasize value-addition vs compliance;
 - Ramp-up shareholder education due to the weak market forces;
- Focus on change agents, such as corporate secretary and audit committees; and
 - Board E&S risk governance.
-

Written by: **Ray Antonio**

CONCLUSION

Companies need to see corporate governance as value-addition rather than only as compliance. By having this mindset, companies will tend to implement good corporate governance practice which eventually will lead to longer-term value creation. With longer-term value creation, investors will be more confident with that company and attracted to invest in that company.

THE NEW FACE OF STRATEGIC RISK MANAGEMENT IN THE NEXT DECADE:

Real Sector, Global Practice Sharing



BALI
ERM
2016

The New Face of Strategic Risk Management in the Next Decade: Real Sector, Global Practice Sharing

Presented by:

Marc Schaedeli

Former Global Head of Risk Management of
Nestle Headquarter Switzerland

Mehmet Zeki Kanadikirik

COO of Asia Pacific, Kordsa Global Turkey

Hosted by:

Timothy J. Corbett

Board Member of ERMA, USA

Organizations ought to be ready in facing the new strategic risk management in the next decade. Strategic risk management can be defined as the process of identifying, assessing and managing risks in an organization's business strategy. Along with the development of today's digital era, the development or changes have given a lot of impact on today's business.

Talking about the impact of the digital era, this session discussed how to deal with the new face of strategic risk management in the business practitioner perspective. This session is presented by two speakers, Mr. Marc Schaedeli

and Mr. Mehmet Zeki Kanadikirik. Mr. Schaedeli specifically explained supply chain as a strategic risk in manufacture industry and Mr. Mehmet Zeki Kanadikirik explained how to deal with strategic risks in his experience.

Part 1

Marc Schaedeli

Former Global Head of Risk Management of Nestle Headquarter Switzerland

Since business become an 'interlinked clusters', all of activities with external parties/partners are regulated in a system which is a supply chain. Supply chain helps organizations to manage the activities, information, people, resources, and so on, so that organizations can create value to the customers.

Today's supply chain is different from the past. Fifty years ago, food manufactures had farmers who brought their product to a local manufacturing and the product produced there. Then, they were sold in the local village or may be region.

Today, supply chain is much more complex starting from buying the raw materials; produce somewhere in Asia or America; shipping to manufacture in Europe; then shipping again to somewhere in the world to be sold with a lot of partners and interconnections.

In the manufacturing industry, you need to have the right products and right raw materials. Right products mean the right quality and right quantity. Either right quality or quantity, both becomes essential because now it will be more challenging to find the right quantity and quality.

Quality should not be something you do apart, quality integrated in all the processes. When you develop a new product, it is essential to think of the quality and also regulatory first. Quality can be your competitive advantage and value added. Also, regulatory can be your standard to produce a new product.

Every activity that we have done in order to run a business certainly contains risks. According to Mr. Schaedeli's experience, organizations must have a clear specification of every certified supplier in order to minimize the risks.

Organizations need to follow one standard for suppliers, neither standard of Nestle, Unilever, nor Indofood. Too many standards can make the supplier confused and may increase the likelihood of the risks. In Nestle, supply chain is actually one of the strategic risks which have clearly identified to really make sure that those risks are well address or not.

There are two main parts of supply chain, which are upstream and downstream supply chain. Upstream supply chain is the transaction between organizations and their suppliers and intermediaries. Downstream supply chain is the transaction between organizations and their customers and intermediaries. In upstream supply chain, organizations may not only have one supplier but they have suppliers, sub-suppliers, and sub-sub-suppliers.

In the development of today's digital era, people easily get much information either legally or illegally. Fraud also could happen in food manufacture, which is called as food fraud or food authenticity. Food authenticity is like false description, substitution of cheaper ingredients, and adulteration, as well as incorrect origin labelling.

Food fraud is included in food authenticity. Food fraud has potential issues that are related to reputational risk that can cause a big impact to the company.

In order to integrate the quality management processes with enterprise risk management, organizations need to make sure that quality management is exactly part of the holistic business risk assessment. The holistic assessment means employee should not only focus on parts of the businesses that directly affect them. They should also focus or understand the full processes and interdependencies of their operations.

In Mr. Schaedeli's perspective, Indonesia has a bigger opportunity in the Asian Free Trade market. There is strong economic growth especially through exchange of knowledge, exchange of sales, exchange of people, etc.

On the other hand, Mr. Schaedeli said that he saw complexity in negotiation between different partners in case something goes wrong. Also, if these partners are not able to negotiate because of cultural differences or because they are not prepared for the events which they confronted with, that can be a big issue and could harm the environmental. Nonetheless, there is still a bigger opportunity.

Part 2

Mehmet Zeki Kanadikirik

COO of Asia Pacific, Kordsa Global Turkey

According to Mr. Kanadikirik, businesses are affected by 2 factors, internal and external. External factor related to customers and how to be a market leader. In order to be a market leader, every company have their own strategy respectively. In practice, every strategy will

face risk, either in formulating or implementing phase. Therefore, strategic risk management is needed in order to face the risks.

Strategic risk management is an organization's response to uncertainties. It involves a clear understanding of risk in the corporate strategy, either the risks in corporate strategy formulation or the risks in corporate strategy execution. These risks may be triggered from inside or outside of an organization. Once they are understood, an organization can develop effective and integrated strategic risk mitigation.

In the digital era, effective communication between the entities is very crucial for developing companies. Kordsa Global Turkey have been creating special platform for the employees to be in effective communication in every level.

Storing and accessing data in the same manner become very important in this era. When organizations are storing and accessing the data, cyber-attacks might strikes. Thus, Kordsa Global Turkey is investing in the protection system to prevent critical risk from cyber-attacks.

Mr. Kanadikirik shared that organizations must be ready for any unthinkable approach and event of the future. They need a very strong strategy, so they have a decent preparation strategy. They need to get ready and adapt as soon as possible for the rapid change of customer trends. They should be fast enough to overcome customers' needs and demand not only for today but also for the future.

In order to fulfil the needs and demand, there are problems such as differentiations and lack of information about the needs and

demand. Differentiations means different customers, country regulations, regional expectations which make organization ought to adjust their products or strategies to many regions, countries, and customers. Thus, many organizations are trying to get the information and to have reliable market intelligence first to understand the needs of customers and stakeholders.

Furthermore, to be ready in embracing the new face of strategic risk management in next decade, Mr. Kanadikirik said that organizations need a very strong strategy. Mr. Kanadikirik shared that there are three pillars according to the time that need to be established as a strategy.

The first pillar is called about today's business in very competitive environment. In this pillar, he was generally focusing on the compatible environment, trying to get prepared for what can be placed in today's competitive world.

In the second pillar, he was focusing on tire reinforcement. Organizations need to be innovative in the light weighting tire developments to control the carbon emissions.

The last pillar is beyond reinforcement. It means that being more sustainable reinforcement in the future, not only for tire reinforcement but also other industries. For instance: airspace, automotive industry or some others.

*Written by: **Fransiskus Bobby Wijaya***

CONCLUSION

Today's strategic risk is different from the past, for example are supply chain and value creation. Throughout the time, supply chain has been changing to become more complex now. Organizations should face many suppliers as an upstream supply chain and many customers as a downstream supply chain. Besides that, value creation has also become much more complex.

Organizations cannot just create value once, but they must create value continuously (continuous value creation). Thus, all over organizations should also be more integrated and focused on continuous value creation for all stakeholders, not only on one partner or one customer, but for all of them.

Strategic risk management can be called as a response to uncertainties in the organizations environment. To deal with the new face of strategic risk management in the next decade, organizations can use three pillars according to the time to establish as a strategy that has been said before by Mr. Kanadikirik. The first pillar is focusing on the compatible environment, second pillar is focusing on reinforcement, and third pillar is focusing on beyond reinforcement.

CHILDREN OF THE FUTURE - RENEWABLE ENERGY RISK MANAGEMENT

(Talk Show)



BALI
ERM
2016

Children of the Future - Renewable Energy Risk Management

Presented by:

Mostafa Ramzy

Senior ERM Expert of Emirates Nuclear Energy Corporation UAE

Timothy J. Corbett

Board Member of ERMA, USA

Dr. Ir. Milton Pakpahan, MM, CERG

President Commissioner PT East Continent Energy Indonesia

Hosted by:

Dr. Miriam Wijaya, ERMCP

Member of National Technical Committee SNI:ISO31000 BSN; Academic Advisory Board Chairperson of CRMS Indonesia

Energy is important for human life as it could make people's life better and easier. It is difficult to imagine if there is no energy in this life. Without energy, it is impossible for people to watch television, to use other electronic goods, to travel by car, etc. In term of business, energy is also very important as it is the soul of operation in many businesses.

Energy can be divided into renewable and non-renewable energy. Most energy type being used right now is the non-renewable energy which is

a type of energy that will not be able to be replenished or reproduced after being used. Even if it could be reproduced, it will take a lot of time to be reproduced (e.g. hundreds or even thousands of years are needed in order to reproduce coal, gasoline, diesel, etc.).

In this session, three speakers presented renewable energy risk management as the main topic. All of these speakers have different backgrounds (country characteristic and culture); thus they have different perspectives about the topic.

Mr. Ramzy presented about renewable energy in terms of risk management from the European Union (EU)'s perspective. Mr. Corbett shared his view about risk management and renewable energy from the US' perspective. Mr. Pakpahan shared his thoughts about renewable energy from Indonesia's perspective.

Part 1

Mostafa Ramzy

Senior ERM Expert of Emirates Nuclear Energy Corporation UAE

In this session, Mr. Mostafa Ramzy shared his view regarding risk identification, assessment, and mitigation of the renewable energy from the European Union Perspective.

Investment in renewable energy projects is now outpacing investment in the new fossil fuel-powered generation capacity. This situation arises because many countries now realized that renewable energy is important for their energy's sustainability. Therefore, they increase utilization proportion from renewable energy.

For example, the European Union has set itself a binding target of "at least" 20% renewable energy in final energy consumption by 2020. To fulfill that target, the European Union has invested around €60-70 billion per year. Investment in renewable energy is very expensive. However, many countries are willing to invest in it. So, what are the main reasons?

First, we need to have a look at the opportunities offered by the renewable energy. The opportunities include securing long-term energy supplies and the diversity of economy. Second, many countries want to change into renewable energy because fossil fuel have negative impacts such as carbon emissions. Third, dependence on fossil fuels also threatens energy sustainability.

Just like an old proverb that says 'don't put the eggs in one basket'. If we do not diversify our energy into many kinds of energy sources, we could be faced with energy sustainability threat.

With many opportunities offered by renewable energy, implementing and building energy infrastructure with renewable energy also have risks. Some risks associated with the implementation of renewable energy are:

1. Country Risks

Country risks refer to political stability, level of corruption, economic development, design and functioning of the legal system, and exchange rate fluctuations. Mr. Ramzy said that not every country has country risk on renewable energy project. The risk itself may depend on the country characteristic, such as culture.

2. Social Acceptability

Social acceptance risks are defined as risks of refusal of renewable energy installations by civil

society due to:

- Not in My Backyard (NIMBY). Sometimes renewable energy has negative externalities. For example, generators from wind power plant produce noise.
- Local communities benefit. The acceptance of a project is sometimes associated with the benefits that would be received by the local communities.
- Increasing costs paid by final consumers. After the project has done, sometimes people are worried that the price would be higher than the estimation.

3. Administrative Risks

Administrative risks are defined as investment risks related to approval needed from the authorities. According to Mr. Ramzy, not every country has administrative risk. Rather, it depends on the commitment from authorities on implementing renewable energy.

4. Financial Risks

Financial risks are associated with experience. Limited experience with renewable energy projects combined with tighter bank regulations could make funding scarcity on renewable energy project.

5. Technical & Management Risks

Technical and management risks refer to the availability of local knowledge, experience, as well as the maturity level of using the technology.

6. Grid Access Risk

After the renewable energy project (for example, electricity from renewable energy source) has completed, there will still be a problem. The problem is how to connect it to the grid. According to Mr. Ramzy, electricity generated by solar panels and by conventional power plants (coal, diesel) have different

treatment when connected to the grid. The sources of this risk are a lack of experience of the operator, and the legal relationship between grid operator and plant operator.

7. Policy Design Risks

According to Mr. Ramzy, policy design risk may arise when policy design does not account for all revenue risks, such as wind yield, demand and price fluctuations.

8. Market Design & Regulatory Risks

This risk may arise due to the uncertainty of governmental energy strategy and lack of independent regulatory body.

9. Sudden Policy Change Risks

Sudden policy change risks refer to risks associated with drastic and sudden changes in the renewable energy strategy and the support scheme itself. For example, before the 2008 crisis, many countries have ambitions to increase utilization of renewable energy.

However, after the crisis hit, many countries try to revisit the project. If there are no treatments, the project could be abandoned. The source for sudden policy change risk is not only economic factors, but also other factors such as politic.

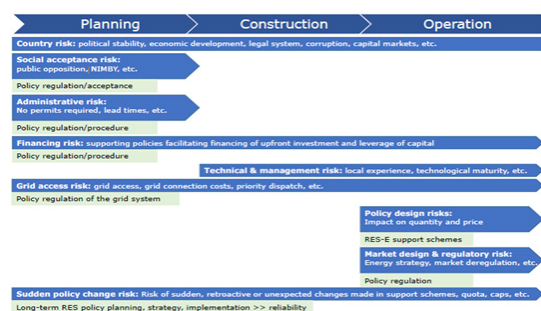


Figure 1. Stages of Renewable Energy Project

Renewable energy project can be divided into three phases (planning, construction, and operation). Figure 1 shows the risks associated with three phases of project.

Risks associated with each phase are different, including country risk, social acceptance risk, administrative risk, financing risk, grid access risk, and sudden policy change risk. Risks associated with the construction phase are technical and management risk.

Risks associated with operations phase are policy design risk and market design & regulatory risk. Every phase has different risk. According to Mr. Ramzy, risks on one phase cannot leap into another phase. In other word, risks on the planning phase could not leap into risk on either the construction or operation phase. While risks arise on planning phase could only be on that phase and could not move into other phases.

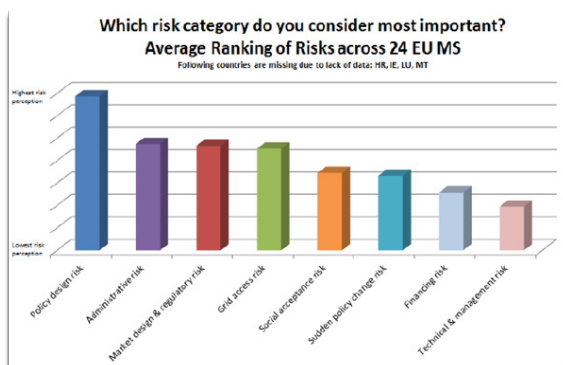


Figure 2. Risk Assessment

Risk assessment on renewable energy can be seen from the figure 2 above. Figure 2 shows the survey's result of the most important risk on renewable energy project from the EU perspective.

The first position belongs to the policy design risk. Policy design is about the benefit (revenue, price, return on investment, etc) after the renewable energy project has done. It is very difficult to measure the real benefit of renewable energy, so policy design risk is very important.

The second place belongs to administrative risk. Administrative risk is related to approval from authorities. This risk becomes a problem due to the difficulty of measuring the real benefit gained from renewable energy.

The third place from the survey is the market design and regulatory risk. From the survey, it can be looked that the most important risks on the EU are the ones related to the government and policy. This result also shows that, from the EU perspective, implementation renewable energy risks are considered as risks that related to policy and policy is related to the government.

After Mr. Ramzy gave his opinion about risk assessment on renewable energy project, he shared his experience regarding mitigation actions. Some mitigation plans that should be considered are:

- Stakeholders participation;
- Streamline administrative procedures;
- Prescribing financial participate;
- Facilitate citizen ownership;
- Communications with facts & Figures;
- Clear strategies and policies;
- Careful tender design;
- Performance & risk database for new innovative technologies;
- Flexibility with banking;
- Create a market place for all actors;
- Neutral party to settle disputes; and
- Integrate RES policies into economic & industrial policy framework.

Part 2

Timothy J Corbett

Board Member of ERMA, USA

Renewable energy can be defined as energy collected from resources which are naturally replenished. Many people and countries realized that renewable energy is important. Therefore, in this session, Mr. Timothy Corbett shared his knowledge about renewable energy in the US, including its development and risks.

First, Mr. Corbett shared some fact and development of renewable energy in the US and the rest of the world. Some facts are:

- In USA, utilization of renewable energy projected to increase by 40% in the next 5 years.
- Worldwide investments on renewable energy are estimated about US\$286 billion in 2015. In U.S. surged 57% to \$65 billion.
- Other effect from people are getting aware about renewable energy is job creation. Globally 7.7 million jobs created from solar panel industry.
- In USA, based on Massachusetts Institute of Technology (MIT), after 2012 renewal energy patents rising faster than fossil fuels patents.

Renewable energy offers many benefits which make people start to aware of implementing it. But, there are risks that have to be faced when implementing renewable energy project. For example, the US is investing heavily in wind, hydro, solar and biofuels as renewable energy source. This strategy is risky due to the environment situation and weather condition dependencies.

Besides weather condition, implementing renewable energy requires innovative efforts (e.g. new technologies) and pioneering projects. On pioneering project, limited track record and standards make renewable energy project become a project with high risk. Due to the scarcity of standard, renewable energy projects are often only rely or based on best practices.

According to Mr. Corbett point of view, implementing and increasing utilization of renewable energy is not an easy job. The complexity of renewable energy is high. In addition, renewable energy has a wide-ranging risk (like the US example on previous paragraph).

Therefore, risk identification is important for the success of renewable energy projects. Management and owners are responsible for risk identification. Additionally, they also need to be confidence that the potential threats have been assessed and well-managed.

High Risk	
Financing	25%
Regulatory	18%
Design	13%
Build	12%
Operate/Maintain	16%
Retrofit	5%
Decommissioning	3%

Figure 1. Risk Assessment on Renewable energy – USA Perspective

Figure 1 shows risk assessment for risk related to renewable energy project in the US. Based on survey that was held in the US, in the first place,

around 25% of respondents assess the financing stage of renewable energy project development as “high risk”. The perception that financial risk is high because renewable energy projects are often capital intensive, and are typically highly leveraged with up to 70-80% of the total project being financed through debt.

As projects gain in scale and complexity, risks arise as well, and financing may become more difficult. Financial risk has several aspects, including raising the capital needed to fund the development of the project, and covering interest payments on debt in the project’s initial years of development and operation.

In the second place, regulatory risk is another important risk where around 18% of the respondents define regulatory risk as high risk. Regulatory risk relates to government support for renewable energy.

In the third place, operate and maintain risk defined as high risk according to the survey result. It is driven by the implementation of new technologies and the lack of sufficient experience. Operate and maintain risk is also related to other risks, which are the build and design risk. Design risk may arise because new technologies sometimes contain hidden risk. It may arise because new technology may not be tested properly for all aspect.

Meanwhile, build risk is associated with experience on managing renewable energy projects. As mentioned before, the limited track record and standards make renewable energy become a project with high risk.

From the last survey result, other risks that are defined as high risk are retrofit and decommissioning risk. Retrofit risk appears because of the updates and enhancements

made in renewable energy projects. While decommissioning risk is related to the life cycle.

Standards as Mitigation Tool

One of the many problems of risk identification is the scarcity of both standards and best practices. Limited standards and best practices make renewable energy projects become projects with high risk because projects might not have sufficient information regarding the best and worst possible case.

Therefore, the US has several standards on implementing renewable energy. These standards are:

1. Leadership in Energy and Environmental Design (LEED)

LEED is green building certification programs used worldwide. This certification developed by the non-profit U.S. Green Building Council (USGBC) includes a set of rating systems for the design, construction, operation, and maintenance of green projects. The purposes of this certification are to help the owners and operators to be environmentally responsible and to use resources efficiently. The need for this certification is encouraged by the fact of increasing greenhouse gases.

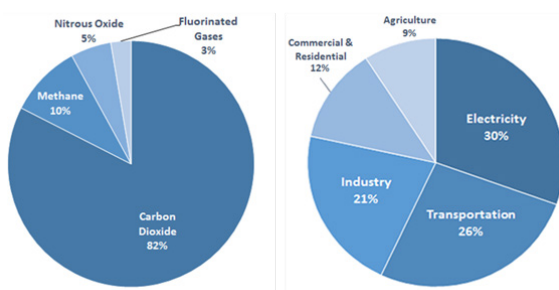


Figure 2. US Green House Gas

Figure 2 shows the composition and sources of greenhouse gas in the US. From the figure, it can be seen that electricity production generates the largest share (30 percent of greenhouse gas emissions).

The second largest greenhouse gas emissions come from transportation (26 percent of the greenhouse gas emissions). Greenhouse gas emissions from transportation primarily come from the fossil fuel used/burned for the cars, trucks, ships, trains, and planes.

The third largest source comes from industry (21 percent of greenhouse gas emissions). The fourth place comes from commercial and residential (12 percent of greenhouse gas emissions). Greenhouse gas emissions from businesses and homes arise primarily from fossil fuels burned for heat, the use of certain products that contain greenhouse gases, and the handling of waste.

Lastly, agriculture contributes around 9 percent of greenhouse gas emissions. Greenhouse gas emissions from agriculture come from livestock such as cows, agricultural soils, and rice production.

2. Renewal Energy Standard (RES)

The purpose of this standard is to encourage the utilization of energy from renewable sources. Some targets that set on this standard are:

- Increase renewable generation by 2% each year for 10 years
- Resulting in 20% renewable power in that state.
- Targets, compliance mechanisms, can vary widely from state to state.
- States include more specific requirements

(called carve-outs), which further incentivize the deployment of particular market segments or energy technologies.

- Half of all U.S. states have renewable energy standards in place.
- National RES policies have been considered by Congress but have yet to be signed into law.

3. Carbon Pollution Standards

In 2013, U.S. Environmental Protection Agency (EPA) adopted Carbon Pollution Standards for existing power plants, known as the Clean Power Plan. Clean Power Plan establishes unique emission rate goals and mass equivalents for each state. This initiative is projected to reduce carbon emissions from the power sector about 32% from 2005 to 2030.

On February 9, 2016, U.S. Supreme Court issued a stay of the Environmental Protection Agency's (EPA's) Clean Power Plan, freezing carbon pollution standards for existing power plants while the rule is under review.

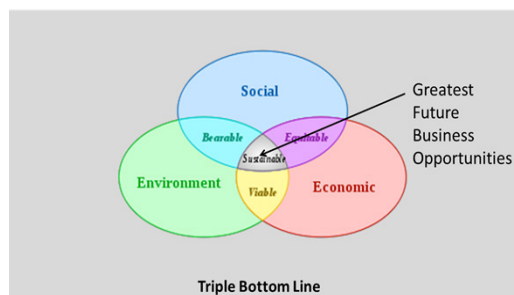


Figure 3. Sustainability Aspect – Triple Bottom Line

After knowing about the standard, we need to understand why we should be aware about renewable energy and why we should implement standard related to renewable energy. According to Mr. Corbett, the answer is sustainability.

Brundtland Commission of the United Nations defined sustainability as development that meets the needs of the present without compromising the ability of future generations to meet their own needs. According to Mr. Corbett, sustainability could be the greatest future business opportunities because sustainability is blended from three aspects, including: social, environment, and economics (see figure 3).

Sustainability means that we should be aware about future generations. Future generations mean that we should be aware about the world's capacity limitation and increasing populations. The resources of the world, such as: space, food, air, water, energy, and natural resources, are limited.

Talking about space, currently the number of humans living on the Earth is about 17% of the whole Earth surface and this number of population will increase every year. World population is expected to increase by 2.6 billion; from about 6.5 billion in 2005 to 9.1 billion in 2050 (almost all growth will take place in the less developed regions).

On the other side, it is estimated that the growth of crops is only 4%. According to Mr. Corbett, with these developments, it needs at least three Earth again to be able to meet all of the human needs.

With the increasing number of human needs and the limited resources from Earth to meet all of the human needs, the need for renewable energy is crucial. Renewable energy can realize the concept of sustainability, which can meet the current needs without making future generations worse off. In implementing

renewable energy, there are various risks associated with it. Therefore, risk identification is an important thing to do.

After identification of renewable energy risk has been done, the next step is to analyze the risks. According to Mr. Corbett, there are some risks analyses that should be considered based on the US perspective, which include:

- Location;
- Life cycle costs;
- Technology performance;
- Current industries data;
- Specialized design and construction;
- Worst case scenarios;
- Environmental impact;
- Observation & measurement; and
- Updates.

Part 3

Dr. Ir. Milton Pakpahan, MM, CERG

President Commissioner PT East Continent Energy Indonesia

In this session, Mr. Milton Pakpahan shared about energy strategy in Indonesia. Indonesia has policy about energy which is expressed on the Government Decree No. 79/2014 about National Energy Policy. This policy talks about energy resilience and energy management as a mission.

Energy management is defined as the activity to provide, to produce, and to utilize the national strategic energy reserve and energy conservation. Energy Management is dedicated to achieve the energy authority by having

the ability to control the energy resources, energy prices, and distribution. On energy management, the objectives are energy sovereignty.

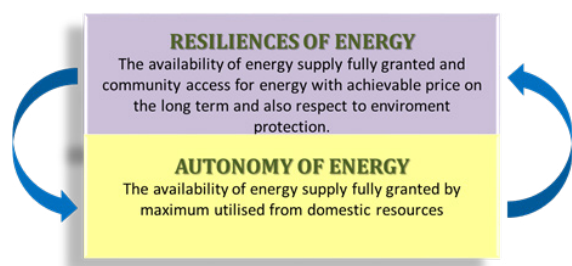


Figure 1. Energy Management – Resilience and Autonomy Relation

The Important factors of energy sovereignty are resilience and autonomy of energy (see figure 1).

Resilience of energy can be defined as the availability of energy supply fully granted and community access for energy with achievable price on the long term and also respect to environment protection.

Autonomy of energy refers to the availability of energy supply fully granted by maximum utilized from domestic resources. Resilience and autonomy of energy are much related and strengthened each other.

Since the middle of the last decade, Indonesia switched from being a petroleum exporting nation into a petroleum importer. This transition made the nation realize that alternative sources of energy should be developed. New and Renewable Energy (NRE) could be the answer for the energy problems in Indonesia.

According to Mr. Pakpahan, The NRE in Indonesia has an overall potential to generate 200,000MW. Currently, the utilization of renewable energy is only 6.8%. Three percent of power generation capacity comes from small hydro and biomass power, with rapid growth of wind power.

Realizing that Indonesia has great potency on renewable energy and in order to create energy sovereignty, Indonesian Government sets a regulation. This regulation is expressed on Government Regulation number 79/2014 about National Energy Policy which sets a target to increase the provision of renewable energy.

In 2025, from 400 Million Tons of Oil Equivalent (MTOE) energy which projected by government, 23% comes from New and Renewable Energy (NRE) which is equivalent to 92 MTOE. The growth of NRE is projected around 17% for the next 10 years.

To achieve this target, an investment of at least 1,600 trillion IDR is required. This investment value by 2025 is divided into Rp. 475 trillion for geothermal, Rp. 645 trillion bioenergy, Rp. 320 trillion for hydro and Rp. 160 trillion for new energy.

Mr. Pakpahan mentioned that due to the ambitious targets set through Government Regulation 74/2014 and the challenges faced by the new and renewable energy sector, business patterns need to be changed. An innovative change is needed in terms of integrated models of funding, planning, technology development and monitoring.

targeted that Indonesia would get 35GW additional electricity by 2019 (see figure 4).

In 2025, the government sets the production target of 115 GW electricity generation. Currently, from 55 GW of energy produced, only 5% are contributed by the renewable energy. The score is expected to rise to 23% in 2025. In 2050, the utilization of renewable energy as electricity generation is projected to become the main source of electrical energy in Indonesia by taking the proportion of 31%.

To achieve Indonesia's vision on renewable energy in 2025, Indonesia has adopted several optimization strategies. These strategies include:

- Set up new regulation including selling price of renewable energy with issued Ministry of Energy and Mineral Resources (MEMR) Decree no. 38 /2016.
- Set up mandatory Bio Fuel B-20 that consist of 80% Diesel and 20% Fatty Acid Methyl Esters (FAME).
- Indonesian Bright Program which governs acceleration of Electrification Ratio in east part of Indonesia through utilization of Renewable Energy Power Plant.
- Acceleration of geothermal power plant by encouraging: (i) Assignment to state enterprise Minister/ General Services body, (ii) Drilling optional through State Budget before bidding phase; (iii) Preliminary survey assignment and exploration

- Acceleration of Bioenergy, through Pilot project of Waste Disposal Power Plant in 7 cities: Jakarta, Tangerang, Bandung, Semarang, Surakarta, Surabaya, and Makassar;
- Mandatory efficiency program to Government property building and Industrial, Campaign cut of 10 % power saving program.

Increasing the utilization of renewable energy in Indonesia is a good step to meet with the national energy needs and to realize energy sovereignty. However, in order to do so, there are some risks that have to be faced by the country. According to Mr. Pakpahan, the risks associated with renewable energy in Indonesia are:

- Licensing issues (related to financing because of the delay in government-backed loan);
- Land clearing (sometimes a source of renewable energy in remote are hard to access, which could make construction and various technical difficulties);
- Site Acquisition;
- Government Regulation;
- Technology Manufacturer / local content;
- Autonomy Region;
- Poor infrastructure;
- Human Resource Capacity;
- Economic Resource Capacity;
- Political Resource Capacity;
- Social Communication Capacity; and
- Scattered location.

Besides those risks above, there are also several other challenges. According to Mr. Pakpahan, these challenges are:

- Equal mindset from stakeholder in terms of developing renewable energy is still required to be upgraded;

- Business scheme and incentives are still not optimum;
- Dependence on foreign technology (local technology still have small portion);
- High and expensive selling price;
- Potential and reserve data still need to be revised and updated;
- Mini scale and limited;
- Limited interconnection system; and
- Social problems.

After understanding about the risks and challenges of renewable energy, it is important to also know about the opportunities. According to Mr. Pakpahan, these opportunities are:

- There are still a lot of region that have not fully got the electricity facilities access until 2015;
- Trend of sustainable development to use clean energy and renewable energy;
- Indonesia's commitment on Paris Agreement;
- Abundant potential of renewable energy resources and spread all in Indonesian territory; and
- Indonesia could become the prime mover of green energy because Indonesia has big potential.

Written by: Yusuf Munawar

CONCLUSION

From all of the various experiences shared by the speakers (from the EU, the US, and Indonesia perspective), it can be concluded that the need for renewable energy is real. Renewable energy can ensure energy sustainability for a country. Therefore, several attempts to change the behavior of energy consumption, from non-renewable energy to renewable energy, have been realized and started.

From this session, it can also be seen that all of the countries have the same objectives; however, they have different perspective. Differences in perspective come from different background (country characteristic such as culture, human resources, and natural resources). Different background generates different result on risk identification.

The main risk of one country may not be the same as the main risk of other countries. Different resources, including human and natural resources, owned by each country may become one of the reasons of why it happens. Thus, practice sharing is important to enrich the perspective about the same problems as well as to give the latest development updates.

CYBER RISK MANAGEMENT



BALI
ERM
2016

Cyber Risk Management

Presented by:

Muh. Nuh Al Azhar

Superintendent Police; Senior Digital Forensic Analyst and
Chief of Computer Forensic Sub-Department Indonesia
Criminal Investigation Police

Alan Simmonds

Board Member of ERMA, United Kingdom

Isnaeni Achdiat, CISA, CISM, CGIT

President of ISACA Indonesia Chapter

Dr. Walid Ghannouchi

Senior Project Manager Standard Chartered Bank, Singapore

Hosted by:

Handikin Setiawan

Director Risk Assurance of PwC

While information and technology bring many benefits to a business, they also bring risks. Knowing how to manage cyber risks is essential for success. By managing cyber risks, companies could become more powerful against many threats.

Cyber Risk is an emerging risk with new complexities that calls risk managers to jointly develop innovative solutions and tools, and to enhance awareness and underwriting expertise. Therefore, knowing this phenomenon, Enterprise Risk Management Academy (ERMA) invited four experienced practitioners to share their knowledge, thoughts, and experiences about cyber risk management.

The first practitioner, Mr. Muh. Nuh Al Azhar, is currently working as superintendent police for Senior Digital Forensic Analyst and Chief of Computer Forensic Sub-Department Indonesia Criminal Investigation Police. The second practitioner, Mr. Alan Simmonds, is a board member of ERMA in United Kingdom. The third practitioner, Mr. Isnaeni Achdiat, CISA, CISM, CGIT, is currently working as the president of ISACA Indonesia Chapter. The fourth practitioner, Dr. Walid Ghannouchi, is currently a senior project manager of Standard Chartered Bank in Singapore.

Looking at their roles, ERMA believes that their experience sharing will be useful for the participants of BaliERM 2016. Hence, below are the summaries taken from their presentations during BaliERM 2016 which explain about cyber risk management.

The influence of the Internet towards the world where we live and do business will be increasing. A lot of estimation saying that around a trillion devices could be connected by 2020, which could lead to a significant increase in cyber vulnerability because new technologies will create new vulnerabilities. Cyber criminals could exploit this increase in interconnectivity.

According to Mr. Isnaeni Achdiat, as technology evolves, older devices that remain in use could also create vulnerabilities, especially when

they rely on outdated operating systems and unsupported software. The prospect of a catastrophic cyber loss is becoming more likely. An attack or incident resulting in a huge data loss or business interruption and the subsequent reputational damage could put a large corporation out of business in the future.

Cyber risk can be defined as any risk of financial loss, disruption or damage to the reputation of an organization due to some sort of information technology systems failure. Cyber risk is now a major threat to businesses and it is not something that can be avoided, but instead it must be managed.

According to Dr. Walid Ghannouchi, it is never a matter purely for the IT team, although they obviously play a vital role. An organization's risk management function needs a thorough understanding of the constantly evolving risks as well as the practical tools and techniques available to address them.

Moreover, the process of digitizing and connecting is not slowing down; instead, cyber risk introduces a whole new range of risks from a variety of known and unknown sources along with intentional (e.g. hacker attack) and unintentional (e.g. failed software update) events. Thus, business and government leaders place cyber security high on their agenda. Knowing about this, all of us should also put cyber security on the board agenda before it becomes the agenda.

Attacks and incidents are increasing with costs climbing into the multimillions. There are certain risks that cause data breaches and the potential for significant business interruptions. Data breaches, involving personal data, have become a major concern for many organizations. Major corporations,

governments, and public services have all been targeted by cyber criminals.

As stated by Mr. Alan Simmonds, an attack will occur if an attacker has both the capability and the incentive to strike at vulnerabilities in a target's assets. These days, attackers' capabilities and incentives are increasing – the former due to technological developments and the latter due to the fact that more data and assets are now accessible online.

Meanwhile, targets' vulnerabilities are decreasing, but in a slower pace than the increase in attackers' capabilities, which suggests that attacks will continue to increase in terms of frequency and impact.

Figure 1 is helpful not only to understand the cyber security landscape, but also to identify and plan for most serious threats, which government leaders must be able to quantify the impact of attacks.

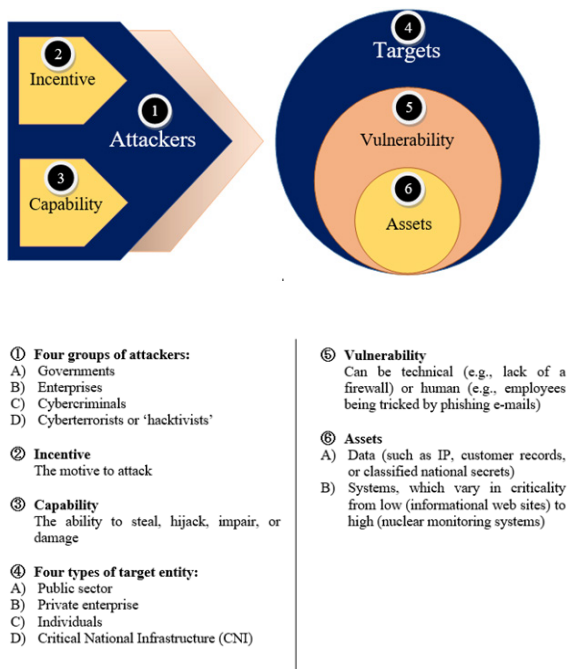


Figure 1. Cyber Security – Risk Landscape

In accordance with the explanation from Mr. Muh Nuh Al Azhar, in order to increase the benefits and minimize the harms in the digital landscape, we should be considering cyber resilience as an evolving perspective that is rapidly gaining recognition which is also a strategic goal.

Entities with potential needs of cyber resilience abilities include critical infrastructure mapping, threat mapping, human resource mapping, and tools mapping. The concept essentially brings the areas of information security, business continuity and organizational resilience together.

We also need cyber risk to be seriously handled by creating several divisions, such as: cyber risk oversight committee, cyber risk governance committee, and cyber risk operations directly team to take care, assess, emerge, respond, and defense cyber threats (see figure 2).

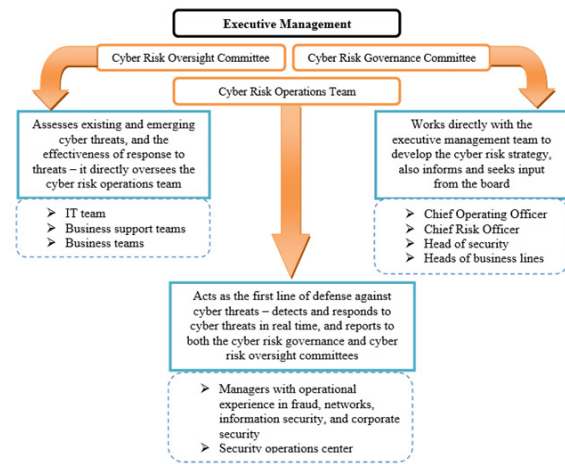


Figure 2. Cyber Risk Management

In 2014, NACD (National Association of Corporate Directors) identified five steps which should be considered by all corporate boards to enhance their oversight of cyber risks.

The five key principles are as follow:

1. Directors need to understand and approach cyber security as an enterprise-wide risk management issue, not just an IT issue;
2. Directors should understand the legal implications of cyber risks as they relate company's specific circumstances;
3. Boards should have an adequate access to cyber security expertise, and discussions about cyber risk management should be given regular and adequate time on the board meeting agenda;
4. Directors should set an expectation that the management establish an enterprise-wide cyber risk management framework with adequate staffing and budget; and

5. Board-management discussions about cyber risk should include identification of which risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach.

These five principles for effective oversight of cyber risk are presented in a relatively generalized form, in order to encourage discussions and reflections by corporate boards of directors. Naturally, boards will adapt these recommendations based on their company's unique characteristics, including: size, life-cycle stage, business plans, industry sector, geographic footprint, culture, and so on.

*Written by: **Aldi Ardilo***

CONCLUSION

Cyber security is a serious corporate risk issue affecting all levels of significant business activity virtually. It is not just the IT department's problem, but it is an enterprise-wide risk management issue that needs to be addressed from strategic, cross-departmental, and economic perspective. However, cyber security alone is insufficient; firms should also begin to move from cyber security to cyber risk management.

It is no longer enough for firms to only try to protect their assets, as potential breaches must also be analyzed within the context of both probability and impact. Thus, cyber security should be established as a tactical subset of an enterprise-wide strategic risk management framework.

In addition, risk managers have to be familiar with the latest technology trend. They also need to be able to anticipate how the latest technology could impact their organizations in the future in terms of cyber risk exposure. Lastly, as technology advances, cyber risk cannot be avoided but it can be managed.

ABOUT AUTHORS



RAY ANTONIO, M.Sc., ERMCP

Chief Financial Officer at Enterprise Risk Management Academy (ERMA)
Bachelor of Economics from Catholic Parahyangan University
Master of Science from University of Manchester



YUSUF MUNAWAR, S.E., ERMCP

Senior Researcher at Center for Risk Management Studies (CRMS)
Bachelor of Economics from Catholic Parhyangan University
Master Degree Student at Padjadjaran University



REYNALDI HARTANTO, S.E.

Researcher at Center for Risk Management Studies (CRMS)
Bachelor of Economics from Parahyangan University
Master Degree Student at Parahyangan University



ALDI ARDILO, S.Psi.

Researcher at Center for Risk Management Studies (CRMS)
Bachelor of Psychology from Padjadjaran University



RADEN AYU BELIANNY PUTRI JULIANINGTYAS, S.E.

Researcher at Center for Risk Management Studies (CRMS)
Bachelor of Economics from Parahyangan University



FRANSISKUS BOBBY WIJAYA, S.E.

Researcher at Center for Risk Management Studies (CRMS)
Bachelor of Economics from Parahyangan University
Master Degree Student at Parahyangan University

THANK YOU

From everyone at Enterprise Risk Management Academy, we would like to express our utmost gratitude to CRMS Indonesia, our gracious sponsors Tokio Marine Life Insurance and Kalbe, as well as our partners and everyone that have attended BaliERM2016.



(c) 2016, Enterprise Risk Management Academy, ERMA Pte Ltd
All contents featured in this whitepaper belong to its respective author(s).

To find out more about ERMA, visit www.erm-academy.org

CONNECT WITH ERMA

info@erm-academy.org | www.erm-academy.org



[erm-academy](https://www.linkedin.com/company/erm-academy)



[@ERMAcademy](https://twitter.com/ERMAcademy)