ERMA

RISK BEYOND 2018

INTEGRATED GRC IN A NEW DIGITAL WORLD

ERMA International Conference on ERM 2018
6-7 December 2018, Yogyakarta, Indonesia

www.riskbeyond.com

RISK
BEYOND
2018

Table of Content

ISO 31000 as The International Risk Management Standard - Embrace Future Risks with Confidence 2

The New Digital World: Opportunity and Complexity to Enhance GRC 6

Governance, Risk Management, and Compliance (GRC) – From Concept to Practices 10

Integrated GRC - Digital Culture Transformation 14

Implementing Integrated GRC in Indonesia; an Insight on the Ongoing Initiatives and Challenges Faced by Indonesian State-Owned Enterprises 18

Practice Sharing of GRC in Public Sector 24

Practice Sharing of GRC in Financial Service Industry - Banking Environment 27

Practice Sharing of GRC in Non-Financial Services Industry 33

Practice Sharing of GRC in E-Commerce Industry 39

Integrated GRC in Entrepreneurial University; Creating Public Value in Digital Era 42

Cyber Risk - Game Simulation for Board 46

Managing Climate Risk as Part of GRC Transformation 49

ISO 31000 AS THE INTERNATIONAL RISK MANAGEMENT STANDARD

EMBRACE FUTURE RISKS WITH CONFIDENCE

SPEAKER
Jason Brown
Chairman of the ISO/TC 262 Risk Management, Switzerland

HOST
Prof. D. S Priyarsono, ERMCP, CERG
Lead of Public Risk Management Standard Development – Komtek 03-10
Advisory Board of Center for Risk Management Studies Indonesia
Professor at Institute of Agriculture, Indonesia

ISO 31000 as The International Risk Management Standard - Embrace Future Risks with Confidence

SPEAKERS
Jason Brown
Chairman of the ISO/TC 262 Risk Management, Switzerland

HOST
Prof. D. S Priyarsono, ERMCP, CERG
Lead of Public Risk Management Standard Development – Komtek 03-10
Advisory Board of Center for Risk Management Studies Indonesia
Professor at Institute of Agriculture, Indonesia

In a rapidly changing business environment, VUCA, which stands for Volatility, Uncertainty, Complexity, and Ambiguity; describes the phenomenon of risk perfectly. These elements might cause impediments, but might also lead to opportunities. Global organisations must possess a right management framework which would enable them to establish an integrated approach to deal with the present and future risks, and take advantage of opportunities at the earliest. Noticing that the future will be enveloped with significant uncertainties, global standardisation is a pivotal point that organisations need to support.

Figure 1. “Blind monks examining an elephant”, an ukiyo-e print by Hanabusa Itchō (1652–1724).

Taking a lesson from the story of “The Blind Men and An Elephant”, the story illustrates that problem that will occur because of an incapability to grasp the whole picture of risk, which emphasises the importance of understanding risk completely. The story informs us about the negative impact that could be brought by accomplishing the action without analysing the problems in detail. This provides a lesson to the business leaders regarding the importance to grasp information that possibly causes the problem and its consequences on the business process. Therefore, business leaders have to look at the risks thoroughly, and they also must have a better point of view to comprehend the entire issue of uncertainty.

The Enterprise Architecture as a Concept in Managing Organisation

Enterprise architecture is a valuable concept in relation to managing organisations. It is a conceptual blueprint that interprets the structure and operation of the organisations, including how the boards and the other business units work. It also includes the purpose of determining how the organisation achieves current and future objectives effectively.

Enterprise Architecture should be associated with the organisation’s strategic planning. It consists of goals and objectives, governance, risk management, compliance, laws, regulations, and controls. Among these structures, the most critical property is governance. The governance involves the rules, the norms, the actions, and the division of accountability which are structured, sustained and regulated. It is the process of making and implementing decisions, which is not about making ‘correct’ determinations, but using the best possible process for making those decisions. There are eight characteristics of good governance for a better decision-making process: anticipatory, consensus-oriented, accountable, transparent, responsive, effective and efficient, equitable, inclusive, and follows the rule of law.

ISO 31000 as The International Risk Management Standard

A global standard is a tool used by organisations to manage and improve their performance in a confident, efficient, and sustainable manner. It provides a flexible framework to be applied in the organisations' business process.

ISO 31000 is a global standard, which is confirmed as a risk management framework that can be customised for organisations around the world. It becomes an open standard for managing risk which serves as a capstone standard of risk management quality system. It also defines the language of risk as part of the international community. The organisations are adopting and applying the ISO 31000 to enhance their potential in reaching the objectives, raising the awareness of opportunities and threats, and improving the ability to effectively allocate and use resources for risk treatment.

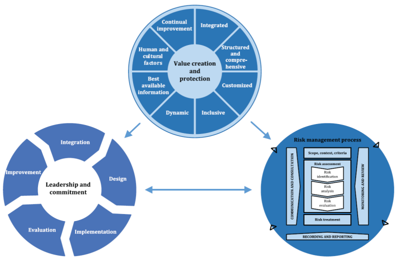


Figure 2. ISO 31000:2018 Risk Management Principles, Framework, and Process.

ISO 31000 has been used multiple times by global organisations to help them managing risks effectively. It applies to the strategic level as well as the unit level. Integrating it into the entire business process will support the objectives that should be achieved in the organisation. ISO 31000 consists of three elements: principles, framework, and process.

The principles of ISO 31000 have a primary mission, that is, to create and protect values of the organisation. It means that risk management put forward the ability to improve organisation's performance, promote innovation, and support target achievement. Moreover, the other eight characteristics that support the management are; Integrated, Structured and Comprehensive, Customized, Inclusive, Dynamic, Best Available Information, Human and Cultural factors, and Continual Improvement. In implementing those principles, it should be noted that ISO 31000 requires strong leadership and commitment at the top-level of management in the organisation. Besides, the organisation needs to have a robust risk management process.

Conclusion

In facing the future, global organisations need to build good governance, enterprise architecture, and also develop security and resilience. By fulfilling these aspects, the enterprise will be able to achieve their objectives and gain more profit. In order to reach the organisations' objectives, they need to adopt a global standard which improves the possibility of success and reduces the prospect of failure.

A global standard enhances the organisations' performance sustainably. ISO 31000 is a global standard that helps the enterprise in anticipating risks and reaching opportunities. Thus, if the organisations are adopting and applying the ISO 31000, they will be able to embrace future risks with more confidence.

Written by Andre Pangestu

THE NEW DIGITAL WORLD

OPPORTUNITY AND COMPLEXITY TO ENHANCE GRC

SPEAKER
Bryan Whitefield
Director of Risk Management Partners Australia
Former Director of Risk Management Institution of Australasia (RMIA), Australia

HOST
Fadjar Proboseno
Board of IRMAPA
Former Head of Audit Department - Astra International

The New Digital World: Opportunity and Complexity to Enhance GRC

SPEAKER
Bryan Whitefield
Director of Risk Management Partners Australia
Former Director of Risk Management Institution of Australasia (RMIA), Australia

HOST
Fadjar Proboseno
Board of IRMAPA
Former Head of Audit Department - Astra International

The new digital world presents unique opportunities for organisations with ways of technology utilisation. For instance, they are using technology as a current application to provide real-time data. To optimise its utilisation, the use of technology should be in-tune with governance, risk management, and compliance (GRC). This is essential for the organisation to deal with digital changes in the business environment, and define all information which is intertwined with business risks and opportunities.

The Blockages on Introducing GRC

In figure 1, Mr. Whitefield explained the blockages in introducing GRC in the organisations. The obstruction consists of a poor framework, bad experience, and sporadic engagement.

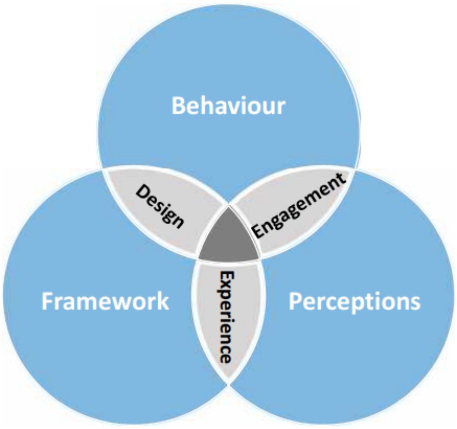


Figure 1. The blockages on introducing GRC

Poor framework. The risk manager's knowledge is an advantage for the advancement of the risk management subject, but it could also backfire. They provide an understanding to develop the standard for risk management, yet the result is often too complicated to concede in the business.

Bad experience. Some managers in the organisation perceive the implementation of risk management in the organisation as a form of bad experience for them. They have to spend much time to identify, assess, evaluate, and monitor the risks as pressure and additional workload mount on them.

Sporadic engagement. In implementing risk management, risk managers and other staffs are often involved in identifying and assessing the risks outside their context or job responsibilities. They do it for boards or committees as a compliance requirement or request.

The three blockages can be solved by creating simple framework design, great experimental learning, and continuous engagement. The framework has to drive good behaviour and create a better perception among risk managers as well as staffs. The framework, behaviour, and perception should be appropriately linked in the organisational risk model.

The New Challenges to Perform GRC in the Digital World

The implementation of GRC in the digital environment is a challenge for the organisations. Various perspectives should be considered concerning three pillars: governance, risk management, and compliance; one should also relate them to the organisation's objectives. The organisation should not only think about the three pillars, but also other challenges in the form of perceptions, comfort, and complexity.

Perceptions. It relates to people's understanding of role and function, and the existence of Enterprise Risk Management (ERM). In some organisations, managers have an impression that ERM only provides advantages to the Risk and

Compliance departments and boards, and not to themselves or their departments. Therefore, ERM, as part of GRC, cannot be applied optimally.

Conformity. It relates to the experts' function in the organisation. They assume that they must perform governance, manage the risks, and comply with some behavioural rules to comfort the Risk Committee. The experts should have a value-added leadership for the organisation, and become the advisors for boards and committees instead of only providing for risk compliance.

Complexity. It relates to the business environment today. Businesses today govern everything, ranging from technology, regulation, process, security, and many other issues. These are too complicated for the organisation; furthermore, it creates an unwillingness to follow.

With regard to complexity, we can learn from the Texas City Refinery explosion in 2005 which occurred because of confounded complexity in the chemical plant. It involved the irrefutable laws of physics and chemistry which must be followed by the employees and other stakeholders. They failed to grasp the complexity of the laws, so that evoked the risk of explosion. Another instance is the chess game. Chess is a twisted game that concerns moving pieces such as soldier, king, queen, and horse, and has its separate set of rules. The complexity of it is found in the Shannon number; the number of lower limits which have ten to the power one two three combinations. It reflects that chess has difficulties in predicting what happens next.

The strategy of the organisations is similar to designing a game in such a situation which only serves to add complexity. The organisations allow complexity in the process of decisions making from the frontline, support functions team, and the senior executive team every time. So, what are the factors which make it more complicated?

"Digital" means mobility, devices and data, and people are drivers of complexity. Based on the data, in 2015 – 2020, the number of devices which connected to the Internet is estimated to be growing from 15 billion to 30 billion, and the one-third of it is driven by the Internet of Things (IoT) industry. However, some companies do not know how to deal with these conditions; consequently, they invest some resources without comparing it to the value obtained.

Behind the complexity, there are always opportunities. The digital environment makes everything more straightforward and solves people's problems with automation, the use of real-time data, Artificial Intelligence (AI), and machines. The organisations crave to avail of digital opportunities; so, they must not only have insight regarding the use of digital technology, but also the objectives of the organisation for the coming year.

Conclusion

A poor risk management framework, bad experiences of risk managers and staffs, and their sporadic engagement turn out to be blockages in introducing GRC in the digital environment. The obstructions can be solved by developing a simple framework for risk management which supports better behaviour and perceptions of risk management. If the organisation succeeds in establishing it, it will become an excellent value risk management.

Written by Chandra Wijaya

GOVERNANCE, RISK MANAGEMENT, AND COMPLIANCE (GRC)

FROM CONCEPT TO PRACTICES

SPEAKERS

Ricardo Saludo
Managing Director, Center for Strategy, Enterprise & Intelligence (CenSEI)

Michael Webb
Barrister and Board Director, New Zealand

Dr. Refly Harun, S.H., M.H., LL.M
President Commissioner of PT Pelindo I, Indonesia

HOST

Leo J. Susilo, SH., MBA
Principal at CRMS Indonesia

Governance, Risk Management, and Compliance (GRC) – From Concept to Practices

SPEAKERS

Ricardo Saludo
Managing Director, Center for Strategy, Enterprise & Intelligence (CenSEI)

Michael Webb
Barrister and Board Director, New Zealand

Dr. Refly Harun, S.H., M.H., LL.M
President Commissioner of PT Pelindo I, Indonesia

HOST

Leo J. Susilo, SH., MBA
Principal at CRMS Indonesia

At present, we are experiencing a transition from the traditional era to the digital age where all activities are connected by technology. This provides various benefits to the organisation in terms of accelerating the production process. Moreover, this also presents some challenges for them, such as new risks in the digital age.

To mitigate the risk, organisations need to implement a risk management framework. However, it is considered insufficient in defeating any uncertainties, since the organisations also require the governance and compliance aspect which is supported by the Board of Directors (BOD) and top management. Thus, to deal with the digital transformation, every organisation needs to implement a framework of governance, risk management, and compliance (GRC).

The Concept of Governance, Risk Management, and Compliance (GRC)

Governance, risk management, and compliance (GRC) is a term that covers an organisation's approach in order to assure an organisation's reliability to achieve its objectives, address uncertainty, and act with integrity. These three components in GRC have their particular focus and differences that must be faced by each organisation, but they have interrelated relationships which are as follows:

Compliance. The first is a determination of compliance requirements through applicable regulations. It refers to the mandated boundaries such as laws and regulations, and voluntary terminations including the company's policies and procedure. Compliance is affected by organisation objectives; for instance, the banking sector is precepted by Bank Indonesia and Otoritas Jasa Keuangan (OJK).

Risk Management. As the second component in GRC, risk management focuses on managing non-compliance risks which affect organisations objectives. By implementing proper risk management, it can help the organisation to achieve its goals in an assured manner. As shown in Table 1, every organisation has different risks, depending on their business objectives.

Table 1. Risk in Government and Private

Type	Government Risk	Private Risk
Political/ Security	1. Loss of mandate and overthrow 2. Political and/or sectoral pressure 3. National security and criminal threats	1. Loss of management control 2. Public and/or government pressure 3. Company security and integrity threats
Economic /Financial	1. Economic hardship and slow growth 2. Fiscal and external imbalances 3. The global recession and inflation	1. Sluggish or declining sales/ profits 2. Loss of markets and market share 3. Rising costs and competition
Social/ Cultural	1. Loss of public trust and approval 2. Critical news and social media 3. Inefficiency, graft, and staff resistance	1. Damage to reputation and brands 2. Shifts in market trends and tastes 3. Staff deficiencies, industrial action
Technol ogical	1. Job losses due to new technology 2. Compromised information systems 3. Mission failure due to inferior technology	1. Sales losses due to new tech 2. Hacking damage to image operations 3. Product problems and failure
Environ-mental	1. Calamity and pollution damage to both government and public 2. Public/media/ global green pressures 3. Hunger and/or disease outbreak	1. Damage to assets, staff, and operations 2. Green pressures on operations industry 3. Losses due to power or transport issues

Legal & Others	1. Disruptive laws and rulings 2. Legal loopholes, poor enforcement 3. Intimidation, assassination of officials	1. Disruptive laws and rulings 2. Closed loopholes, tighter enforcement 3. Family meddling, quarrels, and abuse

Governance. It reflects an organisations' structure which manages and leads them toward their goals achievement, and shows control structures of the risk management program in the organisation.

The governance in organisations was substantiated in the three lines of defence (3LD) model. The 3LD model distinguishes business functions such as who manages the risks, who oversees the risks, and functions that provide independent assurance. These play an essential role in the Enterprise Risk Management (ERM) platform in both private and public organisations.

The Three Lines of Defence (3LD)

The implementation of the 3LD model has some differences in each organisation. In private organisations across Indonesia, the context of implementing the 3LD model is explained in figure 1. It shows that the three layers of defence are under the accountability and coordination of directors. In public organisations, the 3LD model applies to the perspective of governance structure that adheres to the two-board system, i.e. the Board Directors handle executive accountability while the Board of Commissioners handle oversight accountability.

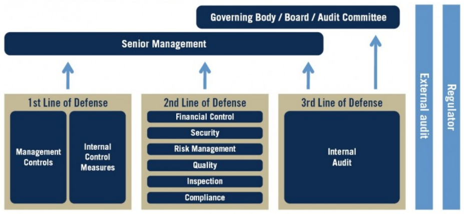


Figure 1. Three Lines of Defence Model; Source: ECIIA/FERMA

The difference between private and public organisations affects the efforts of the Board of Directors in achieving objectives, addressing uncertainty, and behaving with integrity. Mr. Saludo explained that the public organisation's objective is to provide services to the society. To achieve these objectives, the public sector needs to implementing the 5W system: Watch, Warn, Work Out and Whistle and Whip.

Watch means monitoring risk factors constantly, systematically, and strategically. Its purpose is to put priority in every sector, indicator, and report that monitors the different frequencies. While Warn is a warning which has a significant impact on outcomes, so that the organisation can – Work out – to define solutions and build capacity and readiness to tackle consequences. Ultimately, the organisations learn from perfective risks, and how to manage it, so it does not happen twice. That learning process is called a Whistle and Whip.

On the other hand, Mr. Webb explained that the solution which can be applied to the Board of Directors of private organisations is the IoD. IoD is the Mentoring Diversity Program and Future Directors Initiative. The purposes of the Mentoring Diversity Program are as follows:

1. Enhance mentees' governance knowledge and skills to assist the board in achieving director appointments, particularly in large organisation environments.

2. Increase mentees' understanding of how the listed and the large organisations' boards work.

3. Enhance connectivity between senior directors and chairs, attach the director-pool in diversity, and make board-ready talent more visible.

Meanwhile, the Future Directors Initiative aims at providing young talents the opportunity to observe and participate in an organisation' board for a period of 12 to 18 months, while providing exposure to these talents and benefits to their mind which would be eventually delivered to the boardroom.

Conclusion

Governance, Risk Management, and Compliance (GRC) are related to the three facets which help the board and the entire organisation structure achieve the objectives, address the uncertainties, and perform with integrity. Governance is the combination of processes which are established and executed by the Board of Directors, whereas risk management is a process of managing the risks that affect objectives. Moreover, the final factor is compliance that refers to adhering to mandated boundaries which include laws and regulations, and voluntary boundaries such as organisational policies and procedures.

From the three components, there are differences which need to be considered by organisations, both public and private. They have differences in the risks, 3LD models, and rules and regulations that affect the action of the Board of Directors, such as Mentoring Diversity Program and Future Director Initiatives in the private sector, and Watch, Warn, Work Out, and Whistle and Whip in the public sector.

Written by Taracandra Yahitadewi, S.E.

INTEGRATED GRC
DIGITAL CULTURE TRANSFORMATION

SPEAKERS
Rob Logie
President and CEO of PT. AIG Insurance Indonesia

Troy Steve Kipuw
Head of Risk Management of PT. Manulife Asset Management

HOST
Rachmadi Gustrian
Senior Vice President of Risk Management at PT Pelabuhan Indonesia Investama

Integrated GRC – Digital Culture Transformation

SPEAKERS

Rob Logie
President and CEO of PT. AIG Insurance Indonesia

Troy Steve Kipuw
Head of Risk Management of PT. Manulife Asset Management

HOST

Rachmadi Gustrian
Senior Vice President of Risk Management at PT Pelabuhan Indonesia Investama

Building an integrated GRC in a digital world has become a major topic among the business organisations today, since it is closely related to the organisations' culture transformation. Mr. Logie confirms that if organisations do not have a good culture transformation, then the systems, processes, and the designs of GRC would not be adequately delivered. These are essential elements that could protect and enhance GRC, especially in the digital world.

Culture transformation in the digital world is changing faster than ever before. Thus, the organisations need to not only have the culture to manage, but also mitigate the turbulence to sustain their business. Some instances of digital changes which affect the company are cryptocurrencies and blockchain, Internet of Things (IoT), Artificial Intelligence (AI), financial technology, big data, robotics, social media, and others which have been developed to improve the effectiveness and speed of business processes.

These digital changes related to the new technologies could escalate the risks and the organisations' need to adopt a high-risk strategy to face them, such as building an integrated GRC across entire business lines. On the contrary, the new technologies also bring opportunities to the business; Mr. Logie pronounced that the technological approach makes a better system for the organisations today and supports the advancement of GRC in the future.

Building an Integrated GRC: The Challenges in the Insurance Company

In this digital era, technological developments affect people’s behaviour such as high public demand for information, fast and accurate real-time responses, and desire to obtain easy access and services. It raises the technology risk which affects the industry, such as the insurance sector. Therefore, the insurance industry requires to develop an integrated GRC as a form of transformation in the digital era.

There are two challenges to build an integrated GRC in the insurance industry. The first challenge is related to technology and the second is related to culture. The hurdles related to technology are as follows:

1. New economic workers. Technology facilitates individuals who do not have a full-time job by providing them with an advantage of flexibility. Thus, there is a significant increase in the number of freelancers. However, this phenomenon has its advantages and disadvantages. It helps the economy to reduce unemployment and improve people’s well-being. On the contrary, the company loses the opportunity to obtain qualified human resources.

2. Big Data. It provides useful information and organised sources to the companies, which help them to gain prominent opportunities.

3. Aggregators, commoditisation vs customisation. In the future, everyone will get services and products to fit their needs. Aggregators compare the prices, features and products that satisfy the customers and also provide them efficiently.

4. Insurance technology; legacy IT issue. Digitalisation moves aggressively, precisely, and continuously. That situations are forcing companies to explore new technologies to sustain their businesses.

As mentioned above, the insurance sector is facing challenges related to culture. Culture is the most challenging issue to manage, since it covers entire systems in companies. Below are the difficulties associated with culture:

1. Committed CEO and ethical leadership. Everything that happens in the companies starts with the leader. If there is a leader that lacks excellent leadership skills or unethical behaviour, the company will not be able to deal

with any transformation, especially in the digital era.

2. Hiring for culture. Nowadays, when the companies hire new employees, they should consider leadership skill, visionary minded, people's attitude, and other soft skills as critical points besides technical skills. It is required to accelerate the cultural revolution in the companies.

3. Continuous improvement at the board level. Compared to employees, sometimes members of the board are determined by experience. In fact, the backgrounds may not necessarily prove adaptability to transformation. Therefore, the boards should possess excellent soft skills and technological knowledge to face any challenge related to digital changes.

4. Retraining employees. It is a challenging part of the companies to rebuild skills, both soft and technical, and knowledge. It is required to develop the critical thinking analysis of the employees, so they are able to deal with every change in the companies.

Digital Transformation and GRC in PT. Manulife Asset Management Indonesia

Manulife Asset Management Indonesia (MAMI) is a mutual funds company in Indonesia which has the following vision: "a decision made easier, lives made better". Behind the thought, MAMI desires to help people in making easy decisions to lead better lives.

MAMI is facing the era of digitalisation which influences the behaviour of the current society actively. It is proven by the rising number of smartphones used by MAMI's customers. Moreover, the usage of the Internet and social media is increasing aggressively. These factors are affecting MAMI to digitalise their products.

MAMI utilised technology to develop a digital product, which covered the entire country of Indonesia, called KlikMAMI. KlikMAMI is an online application transaction for mutual funds which can be accessed using a mobile phone or computer. It provides products and services to everyone, even in distant areas such as Papua.

KlikMAMI is a strategic initiative that is a part of the digital transformation by means of business incubation, digital laboratory or sandbox, and digital business enablement. MAMI's initiatives do not stop at its product only, as they develop other efforts with regard to building the digital transformation framework, as a pilot project for implementing the integrated Governance, Risk Management, and Compliance (GRC).

The integrated GRC touches the entire aspect of MAMI and becomes building blocks for any initiative in the company. It also helps management in setting and achieving the company's objectives by aligning them to the entire business process. GRC implements risk management at each point of the process and emphasises compliance with every applicable regulation. Eventually, it enhances MAMI's ability and capability in sustaining the business and satisfying the stakeholders.

Conclusion

The integrated GRC, as a part of the process of digital transformation, becomes essential in order to be implemented in a business organisation. For instance, in MAMI, GRC becomes the building blocks to develop strategic initiatives and create successes in the future. However, in its implementation, there are several challenges related to technology and culture.

The technology challenges are new economic workers, big data, aggregators, and technology itself. Meanwhile, the cultural difficulties include committed CEO and ethical leadership, hiring for culture, continuous in the boards level, and retraining employees. The hurdles need to be taken care of and solved by the company so that they gain continuous achievement in the future.

Written by Devina Kurniawan

IMPLEMENTING INTEGRATED GRC IN INDONESIA

AN INSIGHT ON THE ONGOING INITIATIVES AND CHALLENGES FACED BY INDONESIAN STATE-OWNED ENTERPRISES

SPEAKER
Dr. Gatot Trihargo, Ak., MAFIS., CA., QIA., CFE.
Deputy Minister for Financial Services, Survey, and Consultancy
Ministry of State-Owned Enterprises (MSOEs), Indonesia

HOST
Maulana Ibrahim
Former Deputy Governor of Indonesia Central Bank
Industry Expert Advisory Board at Center for Risk Management Studies

Implementing Integrated GRC in Indonesia; an Insight on the Ongoing Initiatives and Challenges Faced by Indonesian State-Owned Enterprises

SPEAKER
Dr. Gatot Trihargo, Ak., MAFIS., CA., QIA., CFE.
Deputy Minister for Financial Services, Survey, and Consultancy
Ministry of State-Owned Enterprises (MSOEs), Indonesia

HOST
Maulana Ibrahim
Former Deputy Governor of Indonesia Central Bank
Industry Expert Advisory Board at Center for Risk Management Studies

The digital transformation in recent years has experienced rapid progress. This is indicated by the industrial changes from 3.0 to 4.0 where most business processes are related to technology now. The changes make every process more manageable and carry out of activities easier; yet, it also brings new risks that require to be anticipated by every stakeholder in the organisation.

Digital Era: The Industry 4.0

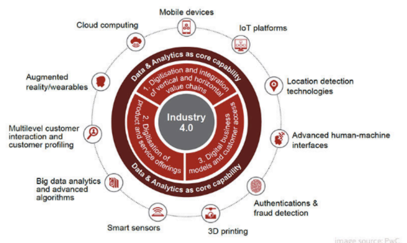

Mobile devices
Cloud computing
IoT platforms
Augmented reality/wearables
Location detection technologies
Multilevel customer interaction and customer profiling
Advanced human-machine interfaces
Big data analytics and advanced algorithms
Authentications & fraud detection
Smart sensors
3D printing
Data & Analytics as core capability
1. Digitisation and integration of vertical and horizontal value chains
2. Digitisation of product and service offerings
3. Digital business models and customer access
Industry 4.0
Data & Analytics as core capability

image source: PwC

Figure 1. The industry 4.0 framework and contributing digital technologies; Source:PWC

In the industrial revolution, technology 4.0 is a big leap for the industrial sector, where the information and communication technology is completely utilised not only in the production process but also in the industry value chain. Thus, it brings forth new business models with digital bases for achieving high efficiency and better quality products.

Based on PWC's 2016 Global Industry 4.0 survey, as shown in figure 1, the industry 4.0 is driven by three aspects: digitisation and integration of vertical and horizontal value chains, digitisation of product and service offerings, and digital business models and customer access.

Digitisation and integration of vertical and horizontal value chains. The industry 4.0 digitises and integrates processes vertically across the entire organisation, from product advancement and purchasing through manufacturing, logistics and service. All data concerning operations processes, process efficiency and quality management, as well as operations planning are accessible real-time, backed by augmented reality, and optimised in an integrated network. Horizontal integration spreads beyond the internal processes, from suppliers to customers and all key value chain partners. It includes technologies from track and trace devices to real-time integrated planning with execution.

Digitisation of product and service offerings. The digitisation of products includes the expansion of existing products, such as adding smart sensors or communication devices that use data analytics tools, as well as the conception of new digitised products that focus on wholly integrated solutions.

Digital business models and customer access. Managing industrial companies also develop their offerings by providing disruptive digital solutions such as complete, data-driven services and integrated platform solutions. Disruptive digital business models focus on generating additional digital revenues and optimising customer interaction and access. Digital products and services continuously look to serve customers with complete solutions in a sharp digital ecosystem.

However, the industrial revolution presents some hurdles for the business in Indonesia, for example:

1. New economy; the existence of digital transformation brings forth a new market called E-Commerce.

2. New customer behaviour; demanding customers, who want to serve faster and better, and tend to get affordable prices and greener services.

3. New regulatory; designed to support innovation while maintaining customer protection and financial stability.

4. New risks; IT risk, cyber risk, operational risk, reputation risk, and other risks which relate to the industry itself.

Agile GRC as a New GRC concept in the Digital Era

To face the new digital era called the industry 4.0, the GRC, which uses many tools and solutions, dynamic updates, unintegrated processes, and ineffective quality control, cannot be implemented anymore. Based on this situation, many practitioners are required to build a new concept of GRC called Agile GRC.

Agile GRC is considered as a new GRC concept to deal with industry 4.0 which is designed with structured guidelines and procedures, and empowers people by technology and analytical capabilities. Hence, it becomes a solution that helps executives to manage governance, risk, and compliance issues effectively.

Figure 2 is the Agile GRC Framework that was developed by Ernest & Young (EY). The framework consists of purpose-led risk, adaptive governance, optimised process, and digitally infused.

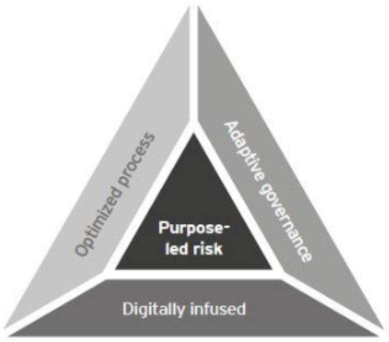


Figure 2. Agile GRC Framework; source: E&Y

Purpose-led risk. It requires the company to define the risks by looking at the velocity of risk and opportunities in order to provide timely information and forecasting on key business drivers and values beyond the financial impact.

Adaptive governance. Governance plays an essential role in improving performance and risk management in organisations. Thus, governing performance and risk requires transparency, active collaboration, and business-centric elevation.

Optimized process. It is a process to manage compliance effectively in a predetermined time, so it can encourage the organisations to maintain it smartly by securing the integrity of the organisation and its people. The optimised process also governs risk-based steering using holistic control optimisation to concede and defend relationships in a performance-based manner.

Digitally infused. Companies are required to turn data into multispeed action to keep up with the digital world. It will undoubtedly provide pre-eminence through transparency, which is rooted in a GRC approach and based on digitalised and intelligent applications and services. Technologies such as blockchain and machine learning is the first glimpse into the future of farsighted risk and compliance solutions.

The discussion above shows that practically all areas of an organisation are affected by Agile GRC. Thus, the rapid advancement of the digital world requires organisations to implement Agile GRC.

GRC Implementation in Indonesia's State-Owned Enterprises (SOE)

SOEs in Indonesia have adopted COSO for implementing the GRC. COSO consists of five components: control environment, risk assessment, control activities, information and communication, and monitoring.

Control environment is related to governance which is set by the organisation and reflects the entire level of attitudes in controlling management. Control environment consists of the integrity and ethical values, commitment to competence, Directors' and Audit Committees, management philosophy and operating styles, organisational structures, and human resource policies and procedures.

Risk assessment, as a set of identifying and analysing actions to manage the risks. It encompasses broad organisation goals, process level objectives, risk identification and analysis, and managing change.

Control activities include policies and procedures, security, management of application changes, business continuity or backup, and outsourcing.

Information and communication consist of records, processes, and report activities of the appropriate transaction to maintain accountability. It assures quality of information and effectiveness of communication.

Monitoring is a process to evaluate the internal quality control and ensure that the entire organisational process aligns to its objectives. The monitoring consists of ongoing monitoring, separate evaluations, and reporting deficiencies.

Based on the previous explanation, the implementation of COSO is evaluated under the conditions of GRC in Indonesia, since SOE governance in Indonesia possesses different characteristics in comparison to other countries. In Indonesia, the executive of the Board of Commissioners is different from the Board of Director. It certainly increases ineffectiveness of communication among them, and finally poses a challenge to the compliance or internal control processes. By implementing COSO, they achieve an effective way to communicate with each other properly, which has the potential to seize the objectives.

SOE's Indicators	2015	2017
Total Asset	375	526
Total Profit	10	13
Total Equity	89	179
Capex Amount	24	29
SOEs Contribution	16	25

Table 1. GRC contributions SOEs in Indonesia in USD Billion

Source: The Ministry of Finance

Table 1 shows the effectiveness of implementing GRC using the COSO standard. It presents SOE's contributions to national development from 2015 to 2017. SOEs increased their contribution from 16 to 25 in USD billion which was assessed by the aspect of total assets, total profits, total equity, and the amount of capital expenditure. In details, the total assets from 2015 to 2017 increased USD 151 billion, from 375 to 526. Also, total profit increased USD 3 billion from USD 10 billion in 2015 to USD 13 billion in 2017. Furthermore, total equity grew USD 90 billion from 2015 to 2017; the last aspect is capital expenditure which also gained USD 5 billion from 2015 to 2017.

By implementing the GRC, SOEs are encouraged to seize positive impact in the future. Nevertheless, another challenge for Indonesia SOEs is performing GRC in the digital world with the help of Agile GRC. It should draw particular attention to them in order to begin the newest venture.

Conclusion

Digital transformation changes rapidly. It can prove to be an opportunity or risk for SOEs in Indonesia. It becomes opportunities if they can embrace the innovation heading the transformation, such as developing a new technology to sustain their business and building an integrated business process. However, it additionally raises new risks if they fail to conform themselves to the changes.

SOEs succeed to manage their organisation by implementing GRC using the COSO standard. They provide a significant contribution to Indonesia; yet, they cannot stop at this moment since the world goes digital. They have to develop Agile GRC to dare many changes and achieve a long story success ahead of them.

Written by Taracandra Yahitadewi, S.E.

PRACTICE SHARING OF GRC IN PUBLIC SECTOR

SPEAKERS
Lim Tong Kang
Chief Risk Officer (CRO) of Tenaga Nasional Berhad, Malaysia

Mostafa Ramzy
Senior Enterprise Risk Management Expert of Emirates Nuclear Energy Corporation (ENEC), United Arab of Emirates (UAE)

Ti-Pin Teo
Head of Risk and Governance of SMRT TRAINS Ltd., Singapore

HOST
Prof Dr. Sonny Prijarsono, ERMCP, CERG, QRGP.
The lead of Public Risk Management Standard Development - Komtek 03-10, Indonesia
Advisory Board of Center for Risk Management Studies, Indonesia
Professor at Institute of Agriculture, Indonesia

Practice Sharing of GRC in Public Sector

SPEAKERS

Lim Tong Kang
Chief Risk Officer (CRO) of Tenaga Nasional Berhad, Malaysia

Mostafa Ramzy
Senior Enterprise Risk Management Expert of Emirates Nuclear Energy Corporation (ENEC), United Arab of Emirates (UAE)

Ti-Pin Teo
Head of Risk and Governance of SMRT TRAINS Ltd., Singapore

HOST

Prof Dr. Sonny Prijarsono, ERMCP, CERG, QRGP.
The lead of Public Risk Management Standard Development - Komtek 03-10, Indonesia
Advisory Board of Center for Risk Management Studies, Indonesia
Professor at Institute of Agriculture, Indonesia

The digital world changes periodically. It is reflected in the industrial revolution from 3.0 to 4.0 or the Internet of Things (IoT), where the role of technology dominates all the business processes. Besides, the advancement of technology interconnects the activities with each other. The changes certainly have an impact on organisations in every industry sector, including the public sector.

SMRT is a public sector in railway transportation which detects that the digital transformation poses a challenge for the organisation because of its impact on the quality of service. The railway industry is a highly mechanical and engineering-intensive business. In SMRT, IoT becomes big data which should be renewed continuously, especially in the safety and reliability systems. They must also intensify the use of social platform as customer service media that can enhance SMRT's reputation.

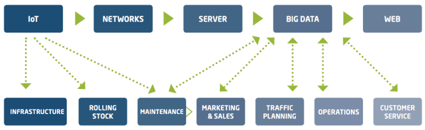


Figure 1. The development of digital railway

Figure 1 describes the implementation of IoT as big data in SMRT, which indicates that the entire system of rail stations is ‘intelligent’. It connects the whole infrastructure to create rail providers who notify the passenger occupancy in real-time. Also, analysing passenger movements to forecast the transportation demand, so that the operators can provide additional services.

IoT is also connected to the train sensors which provide signals to the other trains and control rooms for managing trajectories and avoiding accidents. For example, a track’s sensors might detect an extra weight or vibration on the paths which notifies that two trains are running on the same line. The sensor will automatically connect to both trains as well as the operator’s control room to maintain the tracks. Besides the advantages, the implementation of IoT also leads to disadvantages in relation to SMRT, one of them is cyber risk.

Cyber risk is defined as financial loss and disruption or damage to the reputation of the organisation which is caused by the breakdown of information technology systems. It is categorized as a massive disruption since entire technologies connect with each other throughout the systems. Examining the enormous consequences of cyber risk, SMRT placed an earnest effort to mitigate it. SMRT develops the governance system at two levels, macro and micro level.

The macro level. The implementation of the four pillars that are generated by the Singapore government, includes:

1. Building a resilient infrastructure.

2. Creating a safer cyberspace.

3. Developing a vibrant cybersecurity ecosystem.

4. Strengthening international partnership.

The micro level. It is the readiness of the top management level or Board of Directors (BOD) to undergo digital transformation. In digital evolution, technology is surging. It requires the leaders to be able to keep up with the circumstances. However, in reality, , an average of 63.1% of board members are uncomfortable with IT supervision since they have no IT background, according to the Harvard Law School Forum survey.

The BOD’s role to support the performance of GRC shows in its concept. It explains that governance is not something that stands alone, but is highly dependent on the implementation of internal control and risk management. According to Mr. Ramzy, if the organisations require to attain an excellent GRC, they need to focus on the second layer of defence. That is the stage where the Board of Directors perform an essential role in Enterprise Risk Management (ERM) and ensure that the organisations have a robust risk management framework which is applied to achieving objectives effectively.

Besides, Mr. Kang also confirmed that organisations will obtain a good GRC if they use a risk management standard such as ISO 31000 which converges on the objectives of the organisations. By applying it, management could concentrate on managing, mitigating, monitoring, and evaluating the risks that stem from the organisations' goals.

Conclusion

Digital transformation involves risks and the opportunities for the public sector. For example, in SMRT, digital evolution possesses both advantages and disadvantages. The advantage of digitalisation is that it improves the capability of managing the railway system, particularly enhancing customer satisfaction and advancing trajectories systems. On the contrary, the disadvantage lies in being exposed to cyber risk which has a significant impact on the organisation.

For managing the risk, SMRT is developing the governance system that involves the government at the macro level and the BOD at the micro level. SMRT is not only strengthening the governance system, but also risk management and compliance to accomplish the organisation's objectives.

Written by Taracandra Yahitadewi, S.E.

PRACTICE SHARING OF GRC IN FINANCIAL SERVICE INDUSTRY - BANKING ENVIRONMENT

SPEAKERS
Aurelie Saada
VP of Risk Management of Credit Suisse Asia Pacific, Singapore

Ahmad Siddik Badruddin
Chief Risk Officer of PT Bank Mandiri Tbk

Chairil Tarunajaya
Partner at PWC Consulting SEAC

HOST
Paul C G Gwee
Secretary-General of ASEAN Bankers Association

Practice Sharing of GRC in Financial Service Industry - Banking Environment

SPEAKERS

Aurelie Saada

VP of Risk Management of Credit Suisse Asia Pacific, Singapore

Ahmad Siddik Badruddin

Chief Risk Officer of PT Bank Mandiri Tbk

Chairil Tarunajaya

Partner at PWC Consulting SEAC

HOST

Paul C G Gwee

Secretary-General of ASEAN Bankers Association

Nowadays, many organisations have shifted from the business mindset, product-centric to customer-centric, to meet customers' changing needs. That also happens in the financial services industry, as is shown when they shift from conventional banks to digital banks. Increasingly, banking is going digital and attempting to synchronise all experience in one synergy. For instance, many conventional banks are beginning to switch to digital banks by offering a single product that helps the customers meet their needs, such as investing, borrowing, saving, protecting, and spending money. This shift was strongly supported by the development of technology such as machine learning, chatbots, or virtual assistant by using Artificial Intelligence (AI) which makes integrations with core component systems.

The Chatbot technology is utilised by Bank Mandiri, Mandiri Capital Indonesia (MCI), and other internal information technology teams in many companies. It functions as a 24-hour customer service using AI. On the other hand, Machine Learning technology helps to accelerate and facilitate customer interaction with banks. This proves that technology innovation has advanced significantly and developed many advantages for companies.

However, technology always has its downsides. New risks might emerge when utilising AI services. These risks are continually changing and evolving; and companies have to develop strategies to combat and face these challenges by aligning the Governance, Risk Management, and Compliance (GRC) in order to create an integrated GRC environment.

GRC: Scope and Benefits

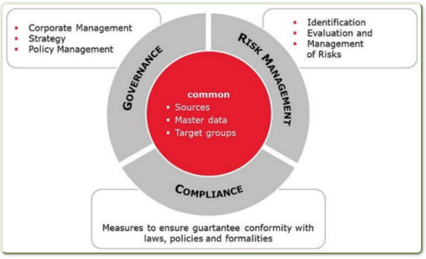


Figure 1. Scope of Governance, Risk Management, and Compliance (GRC)

The Integrated GRC is the collaboration and synchronisation of all information and activities required by the company in relation to risks. These things will help stakeholders predict and exploit the risks accurately; moreover, help them to take the right decisions. Figure 1 shows the scope of the Integrated GRC which consists of the three primary pillars of Governance, Risk Management, and Compliance. These three pillars should equal, balance, and integrate with each other; most importantly, break the silos in every part of the GRC scope.

Governance. The highest level of the company manages the company in the areas of mechanisms, processes and relationships, which enable smooth allocation and understanding of the rights and responsibilities of various decision-makers in the business.

Risk Management. Every aspect of every business has potential risks, whether it is reputation risk, health and safety, financial security, compliance, strategic, investment, or any other issue. It is challenging to manage it while achieving success, therefore risk management function is the answer to tackle the challenges. It is the set of processes that identify, analyse, and respond appropriately to each potential risk.

Compliance. Handling several risks at the same time can be conflicting, leaving the business to choose between minimising the risk to safety or minimising the risk to profits, so it is necessary to ensure that the right decisions are made. That is the role of compliance; businesses should comply with various standards, laws, and regulations to avoid penalties resulting from non-compliance.

The Integrated GRC provides some benefits for organisations, especially the financial industry. Below are eight main benefits that can be derived from it.

1. Continuous collaboration across assurance functions, creating a holistic vision of risk to take up the issue to make better actions

2. Effective compliance programs to address constant changes in regulations, technology, and the business

3. A "single version of the truth" is provided

4. Ability to respond proactively to risks by breaking down restrictive, functional business, and organisational silos

5. More accuracy of risk and control information that enables stakeholders to make fast and risk-informed business decisions.

6. A unified operating model for the business with the agility required to manage emerging risks

7. Consistency in GRC measure means comprehensive insights into the internal operating environment

8. Lower cost of assurance

GRC Implementation in Financial Industry

Bank becomes a financial industry that reaches out to the entire community to collect funds efrom the public. In sustaining the community as an ecosystem of the financial sector, the role of the government involves issuing Otoritas Jasa Keuangan regulations to be followed by the financial industry. Thus, not only maintaining the ecosystem, but also emphasising the regulations to manage the risk in financial business.

Banks use strategic approach as a tool to manage the risks, build integrated risk management, compliance, controls, structures and guarantee processes, and intelligently utilise a data management structure which supports a robust organisational culture. Bank Mandiri could be one of the best practices for implementing integrated GRC in the Indonesia financial industry sector.

GRC Activities in Bank Mandiri

Corporate governance: a combination of processes which is established and executed by the BoC and BoD simultaneously within the team. This is indicated in the organisations' structure and reflected when the company is driven to achieve its objectives.

Risk governance as an Enterprise Risk Management is considered as an integrated risk management function, which connects strategic planning, risk appetite, business execution, risk assessment, and performance evaluation to optimise business growth and risk-adjusted return and maximise shareholder value.

Corporate compliance, applicable laws, regulations and policies: Conformity and adherence to the mandated boundaries include laws and regulations and voluntary borders such as risk appetite, policies, and procedures.

Bank Mandiri is one of the state-owned banks which has a GRC framework to support business processes in terms of managing GRC, which is reflected in Figure 2. It shows that at the top of the chart is Shareholder (Annual General Shareholder Meeting) which is the point of BoD and BoC. They supervise the committee to ensure the GRC is working adequately and managing the risk-taking activities as part of the compliance function in the 12 subsidiaries.

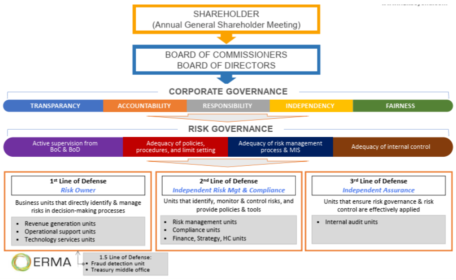

SHAREHOLDER
(Annual General Shareholder Meeting)
BOARD OF COMMISSIONERS
BOARD OF DIRECTORS
CORPORATE GOVERNANCE
TRANSPARANCY
ACCOUNTABILITY
RESPONSIBILITY
INDEPENDENCY
FAIRNESS
RISK GOVERNANCE
Active supervision from BoC & BoD
Adequacy of policies, procedures, and limit setting
Adequacy of risk management process & MIS
Adequacy of internal control
1st Line of Defense
Risk Owner
Business units that directly identify & manage risks in decision-making processes
Revenue generation units
Operational support units
Technology services units
2nd Line of Defense
Independent Risk Mgt & Compliance
Units that identify, monitor & control risks, and provide policies & tools
Risk management units
Compliance units
Finance, Strategy, HC units
3rd Line of Defense
Independent Assurance
Units that ensure risk governance & risk control are effectively applied
Internal audit units
ERMA
1.5 Line of Defense:
Fraud detection unit
Treasury middle office

Figure 2. GRC Framework in Bank Mandiri

BoD and BoC establish corporate governance policies based on five fundamental principles, including transparency, accountability, responsibility, independence, and fairness. With regard to strategic activities, BoD and BoC actively supervise the risk-taking activities and ensure bank business follow policies and procedures adequately. BoD and BoC also have an appropriate risk management process tool and Management Information System (MIS) to manage the risk-taking activities and sufficient internal control processes for covering the security systems of the risk-taking activities.

In supporting the integrated GRC, Bank Mandiri has modified the structure of the three Lines of Defence model. There are additions, namely, 1.5 Line of Defence which emphasises fraud detection unit and treasury middle office. The 1.5 Line of Defence was built to strengthen the GRC model in Bank Mandiri, especially to leverage the ability to prevent risks.

The First Line of Defence refers to business units that directly identify and manage risks in decision-making processes such as revenue generation units, operational support units, and technical services units. The second and third lines of defence in Bank Mandiri are regulated by Otoritas Jasa Keuangan (OJK) and Bank Indonesia (BI). For instance, risk management is regulated in Peraturan Otoritas Jasa Keuangan (POJK) No. 18 /POJK. 03/2016: Penerapan Manajemen Risiko Bagi Bank Umum. Compliance is regulated in Peraturan Otoritas Jasa Keuangan (POJK) No. 46/POJK.03/2017: Pelaksanaan Fungsi Kepatuhan Bagi Bank Umum. Internal Audit is regulated in Peraturan Bank Indonesia (PBI) No.1/6/PBI/1999: Penerapan Standard Pelaksanaan Fungsi Audit Intern (SPFAIB).

Besides modifying the structure of the Three Lines of Defence model, Bank Mandiri also developed the GRC model to respond to digitalisation banking which is illustrated in Figure 3.

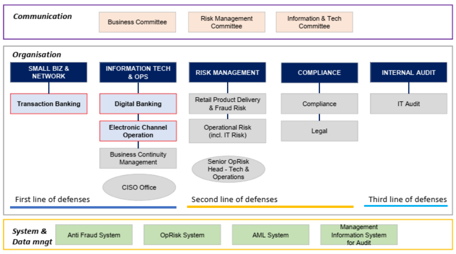


Figure 3. Digitalisation in Banking: GRC Response in Bank Mandiri

The figure above describes the development processes of a robust capability in managing risks in the IT of digital banking products at Bank Mandiri. In this process, human resources become critical in managing information security in IT risk management to ensure business growth in digital banking. The primary human resource in Bank Mandiri is the Chief Risk Officer (CRO), the Chief Compliance Officer (CCO), and the Chief Information Officer (CIO) or Chief Information Security Officer (CISO).

In the organisational structure, Bank Mandiri has a risk management function to perform in accordance with the four-eye principle. With respect to the risk-taking function, the CRO assists the Senior Executive Vice Presidents in charge of the Wholesale and Retail segments. Risk management in Bank Mandiri focuses on managing the risks in periodic business operations and capital management. It is supported by excellence systems, processes, and tools. Bank Mandiri has developed basic ERM processes to cover the end-to-end risk-taking activities, such as the modelling function to ensure sufficiency of capital to cover unexpected events and losses.

As a holding, Bank Mandiri requires to sustain GRC at the subsidiary level by integrating and harmonising the entire business process among them, including business evaluation, risk management, reporting, and culture. Based on the need to build robust GRC, Bank Mandiri prepares some strategies as follows:

(1) setting up a concept of GRC Maturity Model,

(2) developing an enterprise-wide GRC program to support strategic vision and objectives,

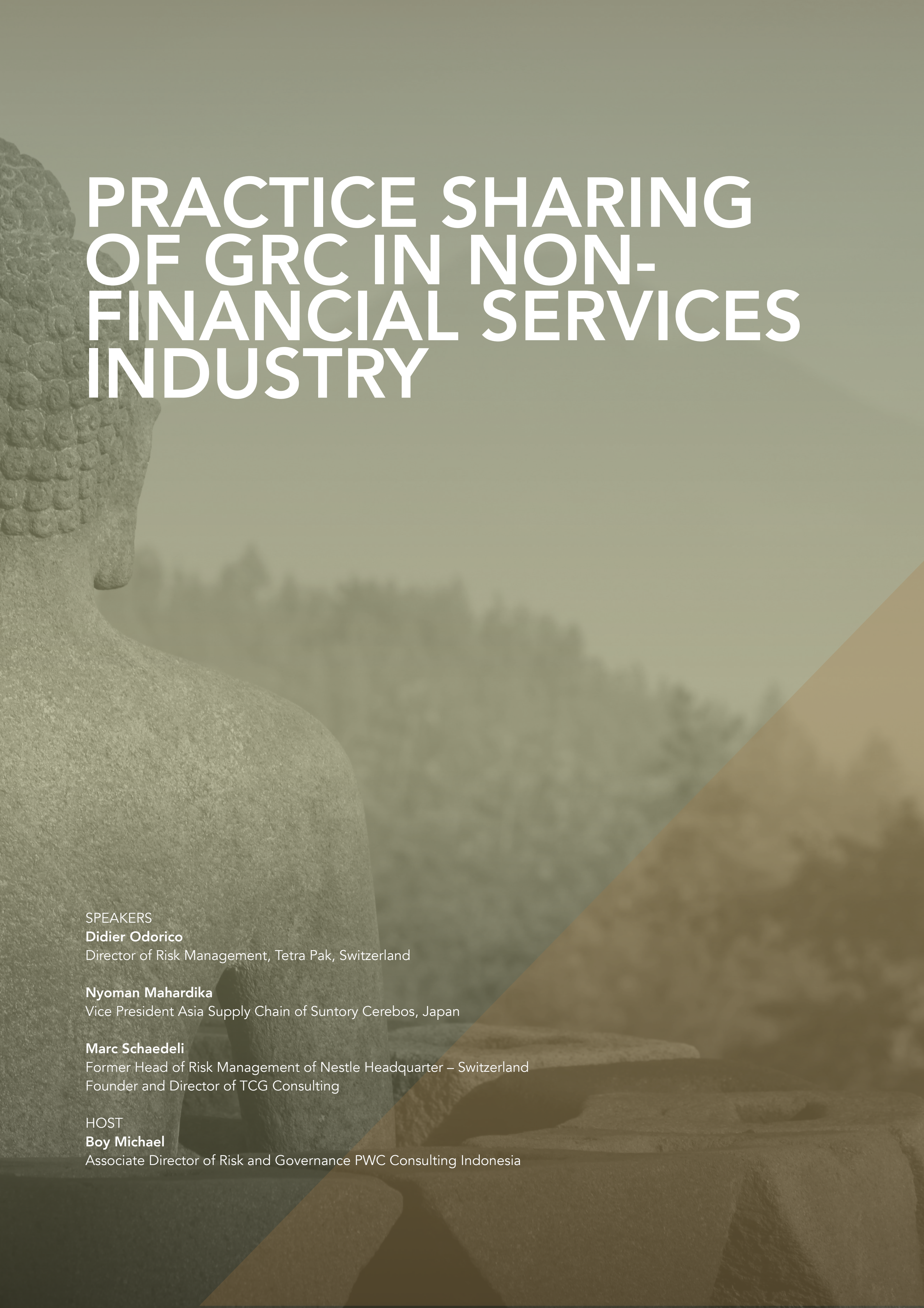
(3) designing and delivering specific GRC function and process, and pointing to the GRC solution as a tool to leverage its capability for particular events and situations.

Conclusion

In dealing with ecosystem changes in the industrial sector, every company requires to change perspective in the digital era. It happens to all industries, especially in the financial sector.

Banks are targeted by the government to build an integrated ecosystem and an integrated GRC which are regulated by POJK. The integrated GRC will help banks to predict risk sharply, exploit the opportunity, and take appropriate decisions. In conclusion, a well-planned GRC establishes transparency, strengthens collaboration across business units, and helps banks to achieve exceptional performance.

Written by Chandra Wijaya



PRACTICE SHARING OF GRC IN NON-FINANCIAL SERVICES INDUSTRY

SPEAKERS
Didier Odorico
Director of Risk Management, Tetra Pak, Switzerland

Nyoman Mahardika
Vice President Asia Supply Chain of Suntory Cerebos, Japan

Marc Schaedeli
Former Head of Risk Management of Nestle Headquarter – Switzerland
Founder and Director of TCG Consulting

HOST
Boy Michael
Associate Director of Risk and Governance PWC Consulting Indonesia

Practice Sharing of GRC in Non-Financial Services Industry

SPEAKERS
Didier Odorico
Director of Risk Management, Tetra Pak, Switzerland

Nyoman Mahardika
Vice President Asia Supply Chain of Suntory Cerebos, Japan

Marc Schaedeli
Former Head of Risk Management of Nestle Headquarter – Switzerland
Founder and Director of TCG Consulting

HOST
Boy Michael
Associate Director of Risk and Governance PWC Consulting Indonesia

In today's environment, organisations are facing an unknown future which is rich in opportunities but filled with many exposures such as the development of technology at the same time. Companies need to be aware of every aspect which is related to their business processes, policies, and regulations. As a response to handle it, worldwide organisations need to implement an integrated Governance, Risk Management and Compliance (GRC) which could guarantee better sustainability.

The Implementation of GRC at Tetra Pak Company

According to Mr. Odorico, risk management is a pilot in the implementation of GRC since a company performance in business is deeply related to risks. However, implementing it in the business process is not a simple matter. This session discussed the crucial points that organisations need to consider in adopting risk management to achieve GRC, best practice at Tetra Pak Co, which is described in figure 1.

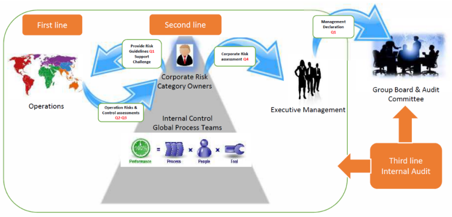

First line
Second line
Provide Risk Guidelines Q1 Support Challenge
Corporate Risk assessment Q4
Management Declaration Q1
Corporate Risk Category Owners
Operations
Operation Risks & Control assessments Q2-Q3
Internal Control Global Process Teams
Performance
=
Process
×
People
×
Tool
Executive Management
Group Board & Audit Committee
Third line Internal Audit

Figure 1. Three Lines of Defence at Tetra Pak Company

In Tetra Pak Company, the units are responsible for the First Line of Defence. They are required to understand every aspect of the system's performance and should have a sufficient understanding of the risks in the company. They need to have simple, tangible, and integrated processes to collect and complete the data and information, making it into a straightforward story. Data and information are vital for them because it could be the indicators of risk or the type of risk that requires to be managed. It also could be the method for mitigating the risk. However, to make it into a piece of useful information, all of the data needs to be combined together to provide insights.

The Second Line of Defence at Tetra Pak is called executive management. They act as corporate risk owners who are a part of a group of specialists that defines and controls the risk management framework, measures risk impact, and determines risk control and other activities. They also compose the report by compiling risk analyses from external parties, which is submitted for CSR or environmental regulation. The executive management also reports to the boards regarding the action plan which is executed by them. Besides the internal audits as the Third Line of Defence, they also perform as observers and challengers for the executive management, and representatives for the boards.

Another thing related to the data and information administration, as part of risk management, is that the Tetra Pak Company enforces the effectiveness of the information channel, using meeting dashboard in figure 2. It constructs various information obliged to control the risks. It also provides data such as the company's locus to monitor and mitigate the risks. By implementing the dashboard method, the activities in Tetra Pak become more dynamic, real, and practical to employ in various sections.

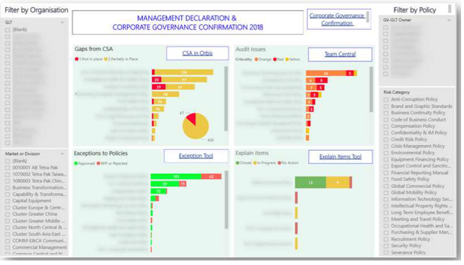

Filter by Organisation
GLT
(Blank)
MANAGEMENT DECLARATION & CORPORATE GOVERNANCE CONFIRMATION 2018
Corporate Governance Confirmation
Filter by Policy
GV-GLT Owner
Gaps from CSA
CSA in Orbis
● 1.Not in place ● 2.Partially in Place
124
20
97
29
63
58
26
25
67
424
Audit issues
Team Central
Criticality ● Orange ● Red ● Yellow
26
5
6
8
7
5
Market or Division
(Blank)
0010001 AB Tetra Pak
1070002 Tetra Pak Taiwa...
1080003 Tetra Pak Chin...
Business Transformation...
Capability & Transforma...
Capital Equipment
Cluster Europe & Centr...
Cluster Greater China
Cluster Greater Middle ...
Cluster North Central & ...
Cluster South Asia East ...
COMM-E&CA Communi...
Commercial Management
Common Central and N...
Exceptions to Policies
Exception Tool
● Approved ● WIP or Rejected
185
42
59
15
32
Explain items
Explain Items Tool
● Closed ● In Progress ● No Action
12
Risk Category
Anti-Corruption Policy
Brand and Graphic Standards
Business Continuity Policy
Code of Business Conduct
Compensation Policy
Confidentiality & IM Policy
Credit Risk Policy
Crisis Management Policy
Environmental Policy
Equipment Financing Policy
Export Control and Sanctio...
Financial Reporting Manual
Food Safety Policy
Global Commercial Policy
Global Mobility Policy
Information Technology Sec...
Intellectual Property Rights ...
Long Term Employee Benefi...
Meeting and Travel Policy
Occupational Health and Sa...
Purchasing & Supplier Man...
Recruitment Policy
Security Policy
Severance Policy

Figure 2. Example of Tetra Pak meeting Dashboards

Ultimately, Mr. Odorico emphasised another crucial thing with regard to changes embedded in every line of management. They should not only have exceptional knowledge and procedures to tackle transformation, but also be capable of making better decisions.

GRC as Tools in Facing Global Changes

Similar to Mr. Odorico, Mr. Schaedeli also stated that risk management is crucial in achieving business objectives. There are considerable numbers of risk management models as part of identification and quantification of GRC. These will be able to support a business environment, although companies should consider and determine a model which helps them to face global changes holistically.

In this interconnected world, a company will be faced with exposure to incidents which arise in a country. For example, the arrestment of Huawei CFO in Canada had a significant impact on the global technology supply chain as well as the world stock market. This case showed that an incident might indirectly affect the companies in other countries. For anticipating the implication of it, the company should possess a robust system which considers risk exposures and also capable be of uniting the aspects of GRC in the business. It becomes standard and requires sustainable improvement, since the companies grow in environments which continually change.

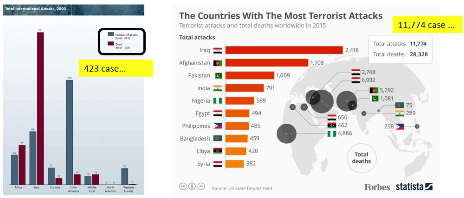


Figure 2. Number of 'Terrorist' cases (2000-2015) – US State Department

Another issue which escalates the exposure of risk in companies is terrorism. Based on the US State Department data, it shows that the number of terrorist attacks had increased dramatically from 423 cases in 2000 to 11,774 cases in 2015 globally and caused more deaths as well. The data indicates that the world has become insecure and more exposed to numerous risks.

These conditions are forcing global companies to make exceptional efforts and place additional resources into risk management. Companies are encouraged to compose extensive reports and establish rapid and competent communication, as part of GRC. Then, they create efficiency in resource planning, prevent duplication in reporting, and also break the silos in them. In GRC, Enterprise Risk Management (ERM) is placed as a framework which fundamentally supports exposure-related planning. It helps to determine a better risk analysis model, equalise perceptions about the risks, and evaluate the availability of resources for specific purposes.

GRC in Infant Formula Industry – The Case of Mead Johnson Nutrition

In this session, Mr. Mahardika shared a real case of how a multi-national company could fail in implementing GRC and what it cost them. The case describes what happened to Mead Johnson Nutrition in previous years.

Mead Johnson Nutrition primarily focused on the Infant Formula. It is a very lucrative business as it increases quality of life and mothers' hope for the health of her child. The market became a snowball in Asia, mainly in China, as it became a leader and attracted more players. Below is a summary of what the Infant Formula industry looks like.

1. It is a highly regulated industry (World Health Organization code)
2. Have a powerful push from breastfeeding activists
3. Healthcare professionals are a source of influence
4. Going through premiumisation
5. Have loyal consumers who are also easily affected and relentless
6. Touched by the China industry.

As a lucrative business, Mead Johnson Nutrition faced several incidents recently and on a frequent basis which affected the company. These are several examples of the events that took place in the company:

1. Mead Johnson has been facing a melamine crisis in China where a baby died and triggered panic buying to Hongkong and Australia which affected the infant formula business. It also forced some retail chains to remove infant formula from the market.

2. Mead Johnson has been fined 12 million dollars due to accusations of fraud and an undisclosed practice bribery case. WHO principles prohibit infant formula to be marketed explicitly in advertisements including print advertisements.

3. Mead Johnson Nutrition has been sanctioned 33 million dollars because of price fixing.

These cases triggered the company to revamp and review their governance, risk assessment, and compliance. The company successfully made some corrective actions and identified five high-risk areas. These include the following:

1. Medical sales representative practices: No sponsorships for doctors, no support to attend a medical convention, and no product sampling at clinics and hospitals.

2. Below the line promotion: No free sampling and no special gondola.

3. Advertising – promotion and marketing practices: No TV commercial, no print ads, and no branding in any commercial.

4. Third party agreement: No contract with third-party connected with any public officials.

5. Government and external affairs: Strictly enforce US Foreign Corrupt Practices Act (FCPA) of 1997.

The company also reviewed and revised all contracts, work instructions, manuals and SOPs in the high-risk areas. It also simplified them to make them sharp and easy to execute by every stakeholder in the company.

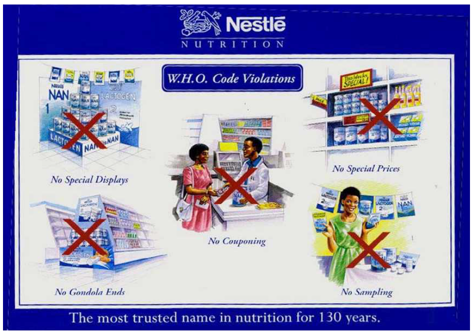


Figure 3. Example of violations intended for employees

Mead Johnson Nutrition also made an additional effort to ensure members of the company to follow the rules and prevent previous mistakes. The simple actions are shown in figure 3, where the company re-train and re-certify every employee in the company. The employees need to pass the test every six months to ensure their capability to always meet the standard.

Furthermore, Mr. Mahardika explained that the company must calibrate the risk appetite both strategically and industrially, which is essential to determine the areas which is exposed to potential risks.

Moreover, companies require to develop tactical actions to mitigate risk and effective ways to fight GRC fatigue, so that GRC practices would no longer stay still at the mandated level.

Conclusion

Worldwide organisations should always strive to improve better GRC in their businesses. Some options which can be carried out by the company are enhancing and simplifying the method of data and information transfer to create transparency and objectivity in decision making. The organisations should be aware of the changes that occur globally and have an effect on themselves. Ultimately, the organisations should also construct a robust GRC for facing the unpredictably changing world.

Written by Andre Pangestu

PRACTICE SHARING OF GRC IN E-COMMERCE INDUSTRY

SPEAKERS
Lisa Widodo
Senior Vice President of Operations and Senior Vice President of Product Management of Blibli.com, Indonesia

Pawoot Pongvitayapanu
President of Thai E-Commerce Association CEO and Founder of TARAD.com
Chairperson of Thailand E-Commerce Association

Setiawan Adhiputro
Director of OVO (PT Visionet Internasional), Indonesia

HOST
Alan Simmonds
Founder and Director of GDPR360, UK
Key Contributor to COBIT 5 ISACA
IT Risk Expert

Practice Sharing of GRC in E-Commerce Industry

SPEAKERS

Lisa Widodo
Senior Vice President of Operations and Senior Vice President of Product Management of Blibli.com, Indonesia

Pawoot Pongvitayapanu
President of Thai E-Commerce Association CEO and Founder of TARAD.com
Chairperson of Thailand E-Commerce Association

Setiawan Adhiputro
Director of OVO (PT Visionet Internasional), Indonesia

HOST

Alan Simmonds
Founder and Director of GDPR360, UK
Key Contributor to COBIT 5 ISACA
IT Risk Expert

In the online world, the store of data moves to data box which is accessible by many people around the world and became a phenomenon. That condition has a severe impact on the data owners concerning their privacy and any confidential information about them. On the other hand, the data users need updated information from the owner to use data analytics, particularly in the e-commerce industry.

E-commerce is one of the big data users, as they use the information from their customers to analyse customer behaviour and experiences. Not only do they analyse the information, but also use them to build a relationship with the customer in relation to the product. The use of data and information by the e-commerce industry should be protected sufficiently to reduce potential negative impact such as legal risks related to data protection. Hence, it is necessary for them to build an integrated system in order to protect the customer and the business itself; in other words, the GRC.

GRC in E-commerce Industry

The GRC practice amongst OVO Indonesia, Tarad.com, and Blibli explain that they have paid significant attention to the business and concerns of customer satisfaction. OVO Indonesia is one of the most successful e-commerce platforms in the country which provides cashless convenience transactions using mobile phones, while operating their business in a complex environment. They build the GRC system within the entire ecosystem, not only focusing on the internal aspect but also on the whole stakeholders.

The GRC system in OVO manages collaboration and partnership with business partners and customers. It maintains a mutual relationship between them to gain sustainable relations; furthermore, it builds trust among partners. Whereas in risk management, as stated by Adhiputro, e-commerce is always open to the risks and completely taken to every threat. It becomes the way in which OVO manages risks. It is fascinating that e-commerce has a unique characteristic with the help of which it manages risks.

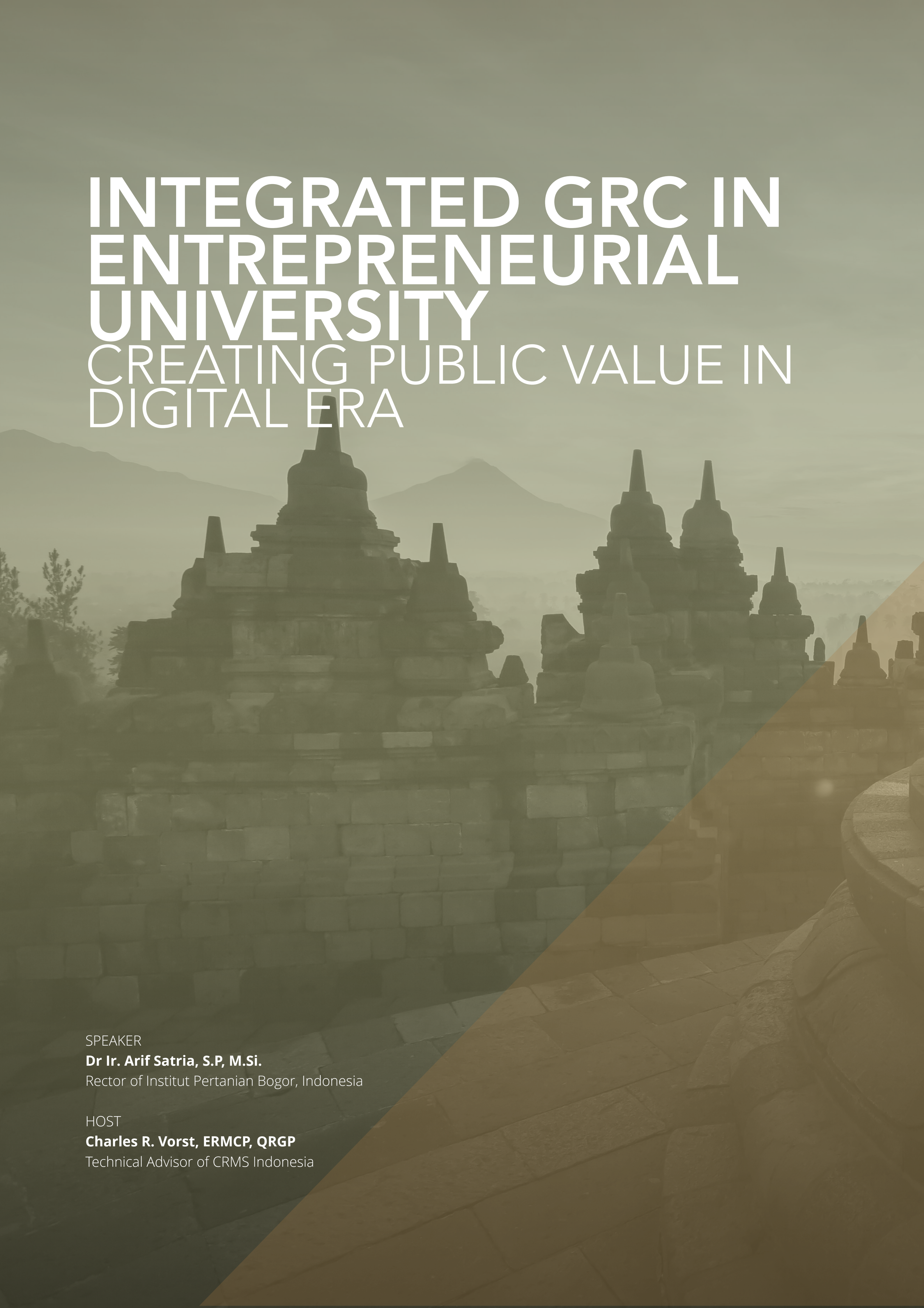
Tarad.com is a leading e-commerce platform in Thailand which also use the GRC system in managing their business society. Tarad emphasised the importance of the GRC system in maintaining and analysing digital risks as a part of organisation and customer data protection. Based on Tarad's viewpoint, the GRC system should be able to enhance the customer’s trust and strengthen the relationship with stakeholders.

Similar to OVO and Tarad.com, Blibli, as an excellent e-commerce platform in Indonesia, confirmed that the GRC system should enhance the stakeholders’ data and information protection. Although, it also preserves the organisations from fraudulent customers. According to Blibli, fraudulent customers negatively impact the organisation by way of loyalty loss, opportunity loss, and financial loss. To reduce the negative impact, Blibli develops a robust GRC capability which includes prevention, detection and mitigation to manage the processes and procedures of marketing and promotion that are commonly misused by the customers. A robust GRC system and capability could detect any fraudulent customers and protect the organisations’ values in a sustainable manner.

Conclusion

In this digital era, many people are facilitated by the technology around them. The technology simplifies their activities by helping them in fulfilling their needs, especially in buying and selling transactions on e-commerce platform. The process of e-commerce platform involves merely using cashless medium and registering consumer data and information with the data box. Due to many conveniences, of course, some problems arise, such as data privacy vulnerability and fraudulent customers. These are a challenge for e-commerce, and they should be able to handle every negative impact around them. Moreover, in order to reduce these impacts, they develop a robust GRC system which is capable of dealing with any risk in the e-commerce business.

Written by Devina Kurniawan



INTEGRATED GRC IN ENTREPRENEURIAL UNIVERSITY

CREATING PUBLIC VALUE IN DIGITAL ERA

SPEAKER
Dr Ir. Arif Satria, S.P, M.Si.
Rector of Institut Pertanian Bogor, Indonesia

HOST
Charles R. Vorst, ERMCP, QRGP
Technical Advisor of CRMS Indonesia

Integrated GRC in Entrepreneurial University; Creating Public Value in Digital Era

SPEAKER
Dr Ir. Arif Satria, S.P, M.Si.
Rector of Institut Pertanian Bogor, Indonesia

HOST
Charles R. Vorst, ERMCP, QRGP
Technical Advisor of CRMS Indonesia

Education in 4.0 has become popular in the current technological era, mainly driven by a smart society that always maximizes the use of innovative technologies to solve life issues, especially with respect to educational matters.

Institut Pertanian Bogor (IPB) is one of the universities in Indonesia which applies 4.0 educational systems as part of the IPB's vision to provide particular contribution to the nation. This vision has encouraged IPB to create and improve literacy capabilities among stakeholders, including students, lecturers, government, and other society members in the digital era. This is crucial for enhancing literacy capabilities to prepare their students as some jobs will disappear in the future. Therefore, IPB must have characteristics, dimensions, strategies, and policies to transform their educational system.

Transformation in Education 4.0: Characteristics and Strategies

As far as the transformation side is concerned, IPB has five characteristics and dimensions: The first is the dimension of learning. In this dimension, IPB wants to create a massive open online course for the students. The second is the dimension of a new profession that prepares the student for new business 4.0. The third dimension is new literacy to build and develop the data, and ICT (Information and Communication Technology) that can be read, analysed, and used for information (big data); science and technological literacy for understanding how the application works, and human literacy and culture for humanities, communication, and design. The fourth dimension involves skills; transformation requires soft skills such as millennium leadership and entrepreneurship. The last aspect is the dimension of the characters. IPB wants to make sure that their students possess integrity and social awareness.

Besides building a sound characteristic, IPB also sets up five strategies to prepare for the transformation process. The first strategy concerns producing a new curriculum 4.0, including integration of hard skills and soft skills. The second involves changing and aligning the current traditional learning process to online. The change in it can be afforded by the “blended learning” system: MOOCs (Massive Open Online Courses) and ODL (Online Distance Learning). The third strategy is about upgrading the lecturers’ skills by preparing virtual teaching material or e-learning; development of heutagogy for virtual learning, and development of assessment design virtual education which results in the perspective of LO (Learning Outcomes) achievement. The fourth strategy involves developing new sciences and new professions that are fulfilled by agrologistic, data science, cyberpsychology, cybersociology, and sustainability. Moreover, the final strategy is about restructuring the curriculum of the IPB vocational school 4.0 using a work-based curricula approach, which refers to the combined design of curriculum and system blocks 3-2-1.

Risk Identification in Implementing Education 4.0

Facing the transformation is not entirely effortless, as IPB must accept various risks to succeed in this transformation. The risks are in the form of HRD, culture, technology, and organisation. It will be a paradigm shift and mindset re-orientation for HRD. IPB’s risk treatment includes framing an intensive training program. Another threat is culture risk; IPB’s risk treatment for this is to create social engineering. For the technological risk, which relates to change management, IPB should deal with massive investment. A further challenge is the organisational risk as it influences a lack of corporate capacity. To mitigate the risks, IPB should develop the Three Lines of Defence.

Critical Success Factor for Implementing Education 4.0

Although IPB faces a variety of risks, IPB has the critical success determinants in dealing with them. The factors that are important to note are human and culture. Human is an essential element to achieve the organisational goals. As a central corporate part, people should be directed and managed adequately, so that they become the most significant advocates for every particular achievement in the organisation, whereas culture is the characteristic of the organisation, defined by everything from the processes, procedures, and strategic thoughts to the policies. In IPB, they build a culture which supports the implementation of Education 4.0 by prioritisinge technological aspects in every process, procedure, and decision-making system.

Beside human and culture, the system of risk management is also defined as one success factor for implementing education 4.0. The risk management system in the university is similar to other business organisations: it uses a top-down approach and strong leadership. The top-down approach means the direction, evaluation, and monitor of risk should come from a leader. Further, the organisations need a leader with strong leadership who can focus on managing the strategic risk to achieve the organisation’s purpose. IPB believes if they have a quality in human resource, robust culture and integrated risk management system, they can implement the education 4.0 favourably.

IPB in the Future

In the future, after the implementation of 4.0 education systems, IPB requires to make many transformations in research and community services, especially in using agriculture’s 4.0 data and technology. Regarding community service, IPB will make future farms small and smart. Drones will be utilized in the future to carry out precise farming by conducting surveys like infrared mapping to gather vital information such as crop condition and big data, so driven drone system can seamlessly integrate agricultural production and consumption, significantly decreasing waste. This makes future farm smallholders have better knowledge of what and when to produce, and whom to deliver. Consumers will also know well ahead of time where the food comes from and how it grew.

Another research program is the smart plan protection. This program will use the function of the Internet of Things (IoT) utilisation for integrated pest management, based on computer vision technology. This research program will require the application to access the digital library, collect data, and automate identification. Through the app, IPB will be able to monitor the program and create disease mapping for the smart plan protection.

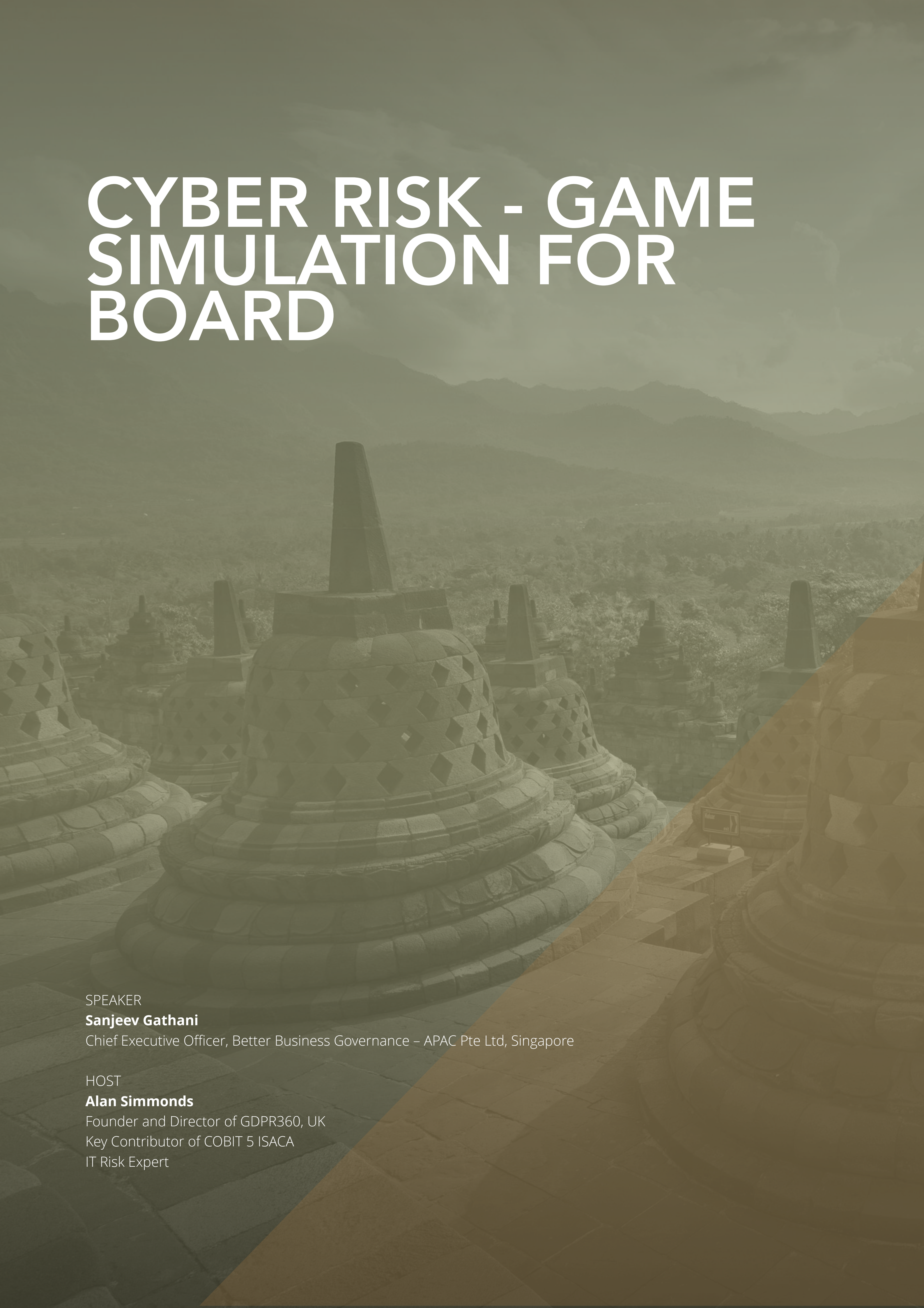
The final program that IPB desires to develop is the Tani Center for the farmer service centre. The users of the Tani Center are the farmers, small businessmen, and the citizens who live near the forest. The centre facilities will be able to provide knowledge related to agriculture throughout communication services such as online information centre, consultation centre, sharing centre, and training centre. On the other side, Tani center has facilities for harvesting farms and marketing.

Conclusion

IPB is a university which builds the system of education 4.0. It develops them as a contribution to the country by providing superior and qualified graduates. It is achieved by undergoing a transformation in the human and culture as well as the risk management system of the university.

Shifting the paradigm in human and culture management and building the proper risk management system helps IPB to deal with many risks in transformation, such as human resources risk, culture risk, technology risk, and organisational risk. Eventually, they can move forward and become the education 4.0-based university which contributes to Indonesia in an excellent manner.

Written by Devina Kurniawan



CYBER RISK - GAME SIMULATION FOR BOARD

SPEAKER

Sanjeev Gathani

Chief Executive Officer, Better Business Governance – APAC Pte Ltd, Singapore

HOST

Alan Simmonds

Founder and Director of GDPR360, UK

Key Contributor of COBIT 5 ISACA

IT Risk Expert

Cyber Risk - Game Simulation for Board

SPEAKER
Sanjeev Gathani
Chief Executive Officer, Better Business Governance – APAC Pte Ltd, Singapore

HOST
Alan Simmonds
Founder and Director of GDPR360, UK
Key Contributor of COBIT 5 ISACA
IT Risk Expert

Technology and cyber are evolving swiftly. This condition creates advantages and disadvantages to the community or organisation. The advantage of technological advancement is the technology-based data collection, which helps organisations in understanding their customers and markets accurately. High-grade data collection improves the performance of the investment, time, assignment, and other terms of an organisation. The disadvantage, for instance, is the use of public infrastructure facilities such as public Wi-Fi that poses a significant risk, such as malicious Wi-Fi service. It also monitors the activities through the computer or the other devices. Imagine if the companies connect to public Wi-Fi and expose confidential information.

Every company is susceptible to cyber threats because these lead to economic downfall, national security attack, and restraint of individual freedom. The company should build a commitment to secure cyberspace and retain the Internet safely. For instance, in 2017, the world was shocked by the cyber-attack led by ransomware Wannacry that attacked the Microsoft Windows Operating System by encrypting data and requesting ransom payments in bitcoin cryptocurrency. It happened because the technology was weak and obsolete which led to modifying inadequate processes in the software. Therefore, in a company, every business process and management function should be involved in avoiding things which lead to a cyber-attack by creating an effective cybersecurity management.

The cybersecurity management consists of three principal factors which are connected to each other: technology, business process, and human. Among the three elements, human is the weakest bond, therefore human needs to be trained adequately to create a powerful cybersecurity management.

Cyber Risk at All Levels

Digital governance involves the policies, processes, roles, responsibilities, and guidelines, supervised by the boards to help the organisation define business opportunities and risks associated with digital technologies.

The risks associated with cyber activity are relatively new, allowing the organisations a lack of understanding about the issues. To recognize the risks, the boards must realise that situations can change on a daily basis. Apart from being aware of the circumstances, the boards are also obliged to understand cybersecurity framework and template in order to Accept, Aware, Transfer, and Reduce (AATR) cyber risk. Moreover, establishing knowledge regarding cyber risk should be prepared in the organisations. Another approach to learning the cyber risks involves imbibing lessons learnt from a recent case of cyber-attacks, such as the SingHealth case study. In that case study, the hackers stole the personal details of 1.5 million patients, including the outpatient prescriptions of Singapore's Prime Minister, Lee Hsien Loong, and many other ministers. It occurred because of a breach of the SingHealth front-end workstation passed by malware download through websites or phishing email. This allowed malware access to the SingHealth database and obtain credentials such as usernames and passwords.

In the discussion above, it turns out that cyber security is one of the most important organisational issues. Moreover, cyber problem falls under the three core elements, namely, the board, corporate governance, and the business, as described in Figure 1.

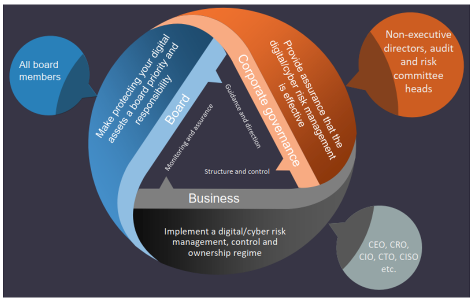

All board members
Make protecting your digital assets a board priority and responsibility
Board
Corporate governance
Provide assurance that the digital/cyber risk management is effective
Non-executive directors, audit and risk committee heads
Guidance and direction
Monitoring and assurance
Structure and control
Business
Implement a digital/cyber risk management, control and ownership regime
CEO, CRO, CIO, CTO, CISO etc.

Figure 1. Corporate governance of cyber risk

The company needs to prevent and mitigate cyber risk continuously to minimise the long-term effect of cyber-attacks which affect both the business process and the company's stakeholders. Cyber risks must be managed proactively by the boards, led by senior management, and guaranteed by corporate governance, an ethical culture in the entire business. The boards should provide assurance that the crucial information related to risks are appropriately assessed and prioritised. Also, information of such nature should be monitored regularly to define and alleviate the threats and vulnerabilities.

Besides, the boards should communicate cyber risks to whole stakeholders and secure the value of information assets, such as company pricing, business strategies, online services, and industrial process control systems.

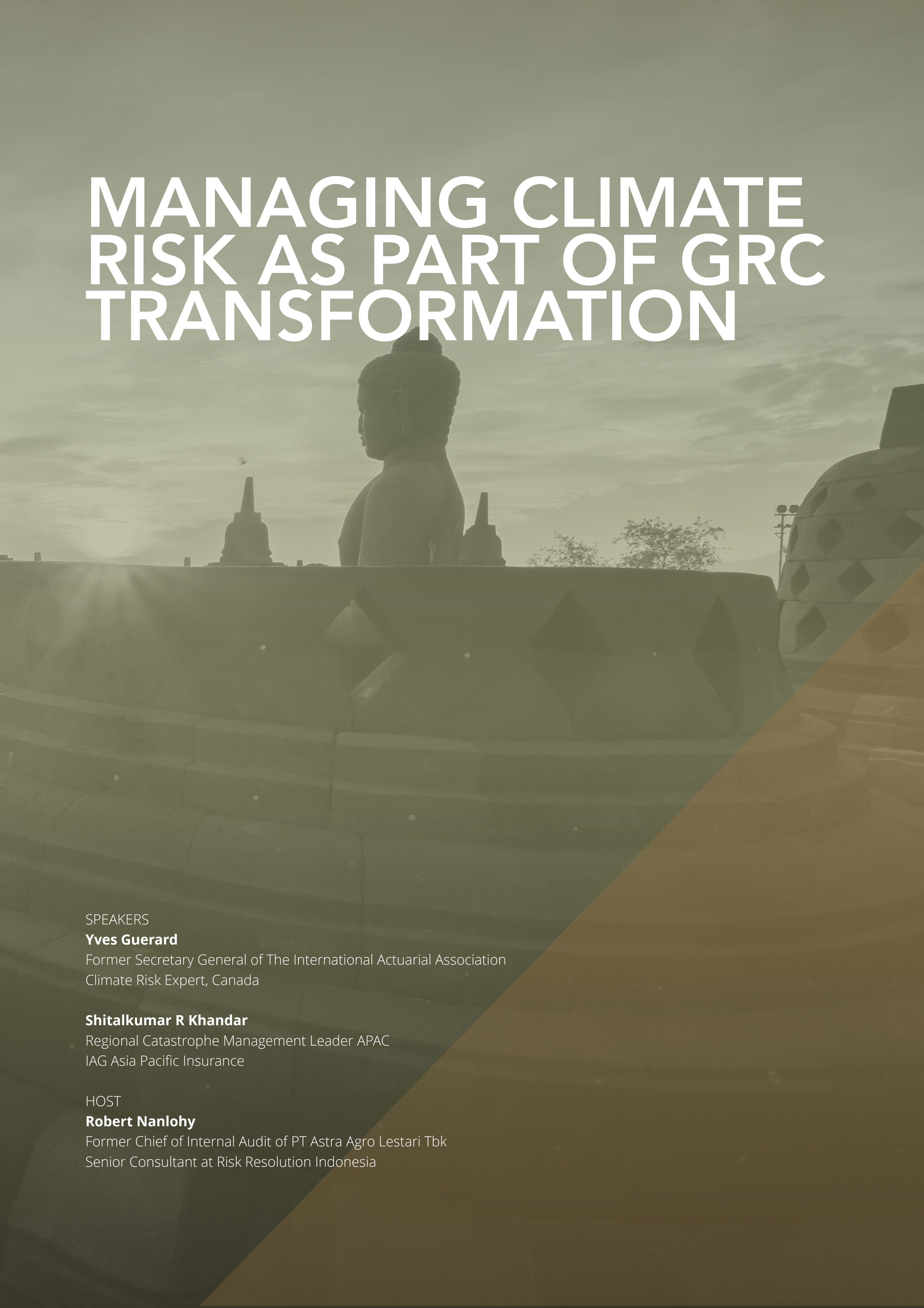
Conclusion

“Put cyber risk agenda before it becomes the agenda.”

This statement explains the importance of giving extra thought to cyber risks. Cyber threats are an organisation’s issue. It is because the perils could destroy the entire organisation. Hence, the boards are at the forefront of managing cyber risks. They should possess sufficient knowledge and be highly aware of the risks. Furthermore, they should be able to establish an adequate cybersecurity management system in the organisation.

Written by Chandra Wijaya

MANAGING CLIMATE RISK AS PART OF GRC TRANSFORMATION



SPEAKERS

Yves Guerard
Former Secretary General of The International Actuarial Association
Climate Risk Expert, Canada

Shitalkumar R Khandar
Regional Catastrophe Management Leader APAC
IAG Asia Pacific Insurance

HOST

Robert Nanlohy
Former Chief of Internal Audit of PT Astra Agro Lestari Tbk
Senior Consultant at Risk Resolution Indonesia

Managing Climate Risk as Part of GRC Transformation

SPEAKERS
Yves Guerard
Former Secretary General of The International Actuarial Association
Climate Risk Expert, Canada

Shitalkumar R Khandar
Regional Catastrophe Management Leader APAC
IAG Asia Pacific Insurance

HOST
Robert Nanlohy
Former Chief of Internal Audit of PT Astra Agro Lestari Tbk
Senior Consultant at Risk Resolution Indonesia

GreenHouse (GHG) emissions, also called Carbon emissions, are increasing each year and directly stimulate global warming all over the globe. In general, this condition has a tremendous impact on environmental performance, including socio-economic environments. It drives many countries to create regulations to reduce the number of GHG emissions through international conventions such as the Kyoto Protocol in 1997, and more recently the Paris Agreement in 2015.

These conventions have produced some regulations which emphasise firms, especially boards and top management, to measure, manage, and disclose their GHG emissions which affect the firms' financial performance. These things are necessary as a form of implementation of governance which put forward transparency, accountability, and responsibility to stakeholders, including investors, customers, creditors, governments, and employees.

GHG Emissions as an Agent of Climate Change

Climate change is defined as variability, statistical distribution, pattern, or dynamic alteration of the climate system, including the atmosphere, water cycle, land surface, ice and the existing components of the earth. It has occurred for a long time and gradually become a subject of concern for several researchers.

Some researchers revealed that climate change arose as a result of the accumulation of Carbon Dioxide and GHG emissions. They considered them as the principle causes of global warming. Joseph Fourier, on Fourier's Article of 1824, presented that the earthbound temperature was augmented by the interposition of the atmosphere and exposed to heat because of the GHG effect. Meanwhile, Svante Arrhenius, in 1896 expounded the science of global warming and claimed that fossil fuel combustions-Carbon emissions might eventually result in enhanced global warming. He claimed that there is a correlation between atmospheric Carbon Dioxide and temperature, called the natural GHG effect.

The natural GHG effect generates dangerous anthropogenic interference to the global climate system. The long-term impact of it will cause instability of environmental performance.

Climate Change: Key Metrics Limitation Target of GHG Emissions

The peril of climate change due to GHG emissions, to the environment, has been realised by both developed and developing countries, especially industrialised countries. Therefore, they declare to protect their environment and strengthen their ability to deal with the impact of climate change by developing a regulation to control GHG emissions. Furthermore, as a concrete action, in 1979, they held the first World Climate Conference in Geneva, and subsequently, the United Nations formed the Intergovernmental Panel on Climate Change (IPCC) in 1988; then, the Kyoto Protocol in 1997, and recently, the Paris Agreement in 2015.

The Paris Agreement, a new legally-binding framework for an internationally coordinated effort to solve climate change, has established the critical metrics for defining limitation target of GHG emissions as mentioned below.

1. Global warming reach below 2 degrees Celsius on pre-industrial average, post emissions should not

exceed 1,000 Gita Tons of Carbon Dioxide (CO2).

2. GHG emissions need to start decreasing to stabilise asymptotically near net zero emissions before the carbon budget is exhausted.

3. The limit creates the risks of losses from stranded assets, including fossil fuels that cannot be burnt and other related infrastructures such as power plants, refineries, and pipelines that become even higher for a 1.5 degrees Celsius target.

4. The carbon budget translates into a CO2 atmospheric concentration target of 450 ppm.

The limitation policies of GHG emissions has shifted the business behaviour of firms toward a low-carbon economy. However, it also increases the new risks and opportunities for exposure.

Climate Change: Risks, Opportunities, and Financial Impact

Mr. Guerard stated that climate change and its regulation create uncertainty in a business environment, and directly increase the risks for stakeholders and their firms. Although in reality, the risks always come along with opportunities, even in the climate change context.

The Task Force on Climate-Related Financial Disclosure (TCFD) has compiled risks and opportunities related to climate change which affect the firms' financial performance, as outlined in figure 1.

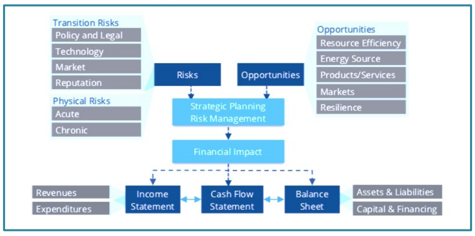


Figure 1 Climate-Related Risk, Opportunity, and Financial Impact

A. Climate-Related Risk

Based on TCFD, climate-related risks are divided into two major categories: 1) the risks related to transition to a lower-carbon economy and (2) the risks related to the physical impact of climate change.

As a consequence of the transitioning process toward a lower-carbon economy, the firms have to face transition risk which may generate financial and reputational risk to the firms. Transition risk may include policy and legal, technology, market, and reputation.

Climate change also drives irregular climate patterns such as storms and thunders; furthermore, in the long-term, chronic climate system will cause cyclones, hurricanes or floods. All these things cause havoc, directly induce physical risks, and impact firms' financial performance.

B. Opportunities

Strenuous attempt to manage climate-related risks also afford opportunities to firms. For instance, cost saving due to resources reduction, the use of renewable energy as a new energy source, developing new products or services, expanding to a new market, and establishing an extensive supply chain network.

C. Financial Impact

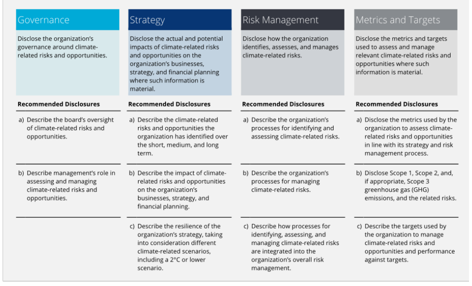
The risks and opportunities, in part, of managing climate change should be clearly addressed in the firms' strategic decision, since it will affect the current and future financial position of the firms, which is reflected in income statement and represented in revenue and expenditure, cash flow statement and balance sheet, described as asset and liabilities – capital and financing.

The impact of climate change to the firms' financial position was also confirmed by Mr. Khandar who stated that climate change could sustain momentum to generate future gain or losses for the firms, depending on the adaptability to control and mitigate climate change. Moreover, the firms could enhance the ability to adapt to the risks if they soundly identify the risks that affect them and communicates the risks adequately. Consequently, the firms have to disclose climate-related risks that interfere with the financial performance.

Financial Disclosure Related to Climate Change as A Part of GRC Transformation

Since climate change affects financial performance, many stakeholders such as investors, customers, creditors, governments, and employees become more concerned about encouraging firms to disclose climate-related risks and opportunities in their financial disclosure.

Financial disclosure related to climate change is considered a commitment of board and top management in implementing GRC in their organisations. Further, to provide a structured disclosure, TCFD recommends guidance for organisations to develop Climate-related Financial Disclosure which covers both financial sector industries and non-financial sector industries. It consists of four core elements' recommendations, namely, governance, strategy, risk management, and metrics and targets, as depicted in Figure 2.



Governance	Strategy	Risk Management	Metrics and Targets
Disclose the organization's governance around climate-related risks and opportunities.	Disclose the actual and potential impacts of climate-related risks and opportunities on the organization's businesses, strategy, and financial planning where such information is material.	Disclose how the organization identifies, assesses, and manages climate-related risks.	Disclose the metrics and targets used to assess and manage relevant climate-related risks and opportunities where such information is material.
Recommended Disclosures	**Recommended Disclosures**	**Recommended Disclosures**	**Recommended Disclosures**
a) Describe the board's oversight of climate-related risks and opportunities.	a) Describe the climate-related risks and opportunities the organization has identified over the short, medium, and long term.	a) Describe the organization's processes for identifying and assessing climate-related risks.	a) Disclose the metrics used by the organization to assess climate-related risks and opportunities in line with its strategy and risk management process.
b) Describe management's role in assessing and managing climate-related risks and opportunities.	b) Describe the impact of climate-related risks and opportunities on the organization's businesses, strategy, and financial planning.	b) Describe the organization's processes for managing climate-related risks.	b) Disclose Scope 1, Scope 2, and, if appropriate, Scope 3 greenhouse gas (GHG) emissions, and the related risks.
	c) Describe the resilience of the organization's strategy, taking into consideration different climate-related scenarios, including a 2°C or lower scenario.	c) Describe how processes for identifying, assessing, and managing climate-related risks are integrated into the organization's overall risk management.	c) Describe the targets used by the organization to manage climate-related risks and opportunities and performance against targets.

Figure 2 Recommendations and Supporting Recommended Disclosure

Every core element has substantial purposes which reflect how organisations measure, manage and mitigate climate-related risks, how climate-related risks and opportunities impact strategic decision making, and describe how board's and management's role carry out their function to manage climate-related risks and opportunities.

Regardless of the single purpose of these elements, the recommendations itself is made for two more important goals. First, it helps stakeholders and decision makers assess their risk exposure, which is a pre-requisite to controlling and managing risks at the single entity level. Second, it makes the strategic decision maker available to the global community, regarding the necessary information to facilitate convergence on pathways that offer cost-efficient mitigation of climate change. Eventually, even though these recommendations are not mandatory, they become a tool to desirably employ governance which puts forward transparency, accountability, and responsibility to tackle climate-related risks.

Conclusion

The regulation related to climate change, as an effect of GHG emission, has magnitude leverage on the firms' financial decision-making process. Thus, the boards and top management are required to have a qualified skill to measure, manage, and disclose the climate-related risks and opportunities adequately. It becomes necessary since it is considered the boards' commitment to implementing GRC.

The implementation of GRC related to climate change, in industrial sectors, could be conducted by adopting TCFD's recommendations framework for disclosing financial-related climate change information, as a tool to apply peer pressure through comparative analysis. Furthermore, in future, as an initiative of GRC transformation, TCFD's recommendations need to become the mandatory disclosure framework for both financial sector industries and non-financial sector industries.

Written by Intan Megafany

To find out more about ERMA, visit www.erm-academy.org

CONNECT WITH ERMA

info@erm-academy.org | www.erm-academy.org

@ERMAcademy erm-academy