The Implementation of Multiple Information Security Governance (ISG) Frameworks Strategy and Critical Success Factors in Indonesia's Oil and Gas Industry: Case Study of PT X

Bob Hardian Syahbuddin
Faculty of Computer Science,
Universitas Indonesia
Depok, 16464, Indonesia
hardian@cs.ui.ac.id

Fatimah Azzahro[*]
Faculty of Computer Science,
Universitas Indonesia
Depok, 16464, Indonesia
azzahro.fatimah@cs.ui.ac.id

Wachid Yoga Afrida
Faculty of Computer Science,
Universitas Indonesia
Depok, 16464, Indonesia
wachid.yoga@.ui.ac.id

Achmad Nizar Hidayanto
Faculty of Computer Science,
Universitas Indonesia
Depok, 16464, Indonesia
nizar@cs.ui.ac.id

Kongkiti Phusavat
Department of Industrial Engineering,
Kasetsart University
Bangkok, 10900, Thailand
fengkkp@ku.ac.th

Abstract

The oil and gas industry is one of the largest contributors to Indonesia's foreign exchange. Many people believe that information technology plays an important role in the oil and gas industry's success. However, implementing information technology to support the corporate business process brings vast information security risks. There is a need for comprehensive information security governance that can comply with information security standards and regulations. This research is conducted to evaluate the use of multiple ISG frameworks for implementing information security governance in a multinational oil and gas company. In detail, we evaluate the effectiveness of such a framework, assess its implementation maturity level, and identify the success and inhibiting factors for implementing ISG frameworks. This study shows that framework XYZ, as a multiple ISG framework, is effective to cover the controls of ISO 17799, COSO, and IT Risk Framework at once. Meanwhile, the observed case study indicated a lack of compliance of Framework XYZ followed by the invention of the gap between current ISG implementation efforts and company visions. Lastly, several success and inhibiting factors are identified in the ISG framework implementation at PT X.

Keywords: Information security, governance, multiple ISG frameworks, ISO 17799, COSO, IT Risk Framework, Framework XYZ

[*] Corresponding Author

Introduction

The oil and gas industry has a very significant contribution to Indonesia's economy. So far, oil and gas have contributed to the country's foreign exchange and has become an important source of state revenue besides taxes (Baskoro 2019). In its implementation, the oil and gas industry rely heavily on seismic data. Seismic data provides information on the position and depth of drilling, oil and gas content, and other essential information related to oil and gas. This data will determine the amount of production and the sustainability of the company. Therefore, seismic data can be considered as the most important asset of an oil and gas company and must be guarded so that it does not fall into the hands of competitors.

On the other hand, technological developments play a very vital role in improving the business process in the oil and gas industry. The use of information technology such as GPS, ERP, and SCM can help companies make decisions regarding the drilling locations and estimation of oil and gas content more accurately and quickly. Despite providing benefits and conveniences, the increasing use of information technology in the oil and gas industry also comes with huge risks. Data processing failure, communication network problems, data inaccuracy, and data theft are some examples of problems that can occur while using information technology. To reduce this risk, the oil and gas industry has several regulations such as the Sarbanes Oxley Act (SOX), Payment Card Industry (PCI), Gramm Leach Bliley Act (GLBA), and Health Insurance Portability and Accountability (HIPPA).

Compliance with regulation is needed to minimize business risks. To do so, one should implement proper information security governance. Information security governance (ISG) involves developing and integrating management structures and organizations with a reporting process that covers all aspects of successful security programs and provides assurance to business management that risks can be defined and managed appropriately (Ferguson et al 2012). ISG consists of several aspects, namely, leadership, organizational structure, processes, supervisory mechanisms, and technology (Solms 2007). ISG needs to be implemented to secure the confidentiality, integrity, and availability of the organization's electronic assets (data, information, software) from risks and threats (Solms 2007).

To achieve effective information security governance, management must establish and maintain a framework to guide the development and maintenance of a comprehensive information security program. There are several ISG frameworks that can be used as a reference, including ISO / IEC 17799, COSO, GMITS Guidelines, COBIT, and ISM3. However, often, the use of a single framework is not sufficient to meet regulations in the industry. On the other hand, implementing a combination of ISG frameworks can potentially sacrifice their effectiveness.

PT X is a subsidiary of PT X Group, the fifth-largest integrated energy company in the world based in France. In managing its information security, PT X created a distinct ISG framework called the XYZ framework, which adopts and combines several ISG frameworks at once. This study will examine the adoption of the XYZ framework as multiple ISG frameworks in the oil and gas industry, particularly at PT X, by focusing on three research questions as follows:

- Evaluate the effectiveness of adopting multiple ISG (XYZ framework) and its compliance with information security regulations
- Assess the maturity levels of multiple ISG frameworks implementation and identify gaps between the current maturity level and the expected maturity level
- Identify the factors that support and hinder the successful implementation of ISG

Literature Review

Information Security and Threats

Information security is defined as all matters relating to the protection and maintenance of confidentiality, integrity, authenticity, availability, and reliability of information (Calder 2012). Information security can also be defined as the steps required to detect, document, and counter threats to information (Boiko and Shendryk 2016). The prior definitions imply that information security is not only a technical problem but also related to management problems consisting of processes and people (Albert 2016). The purpose of implementing information security is to minimize threats that come internally or externally. The threat is defined as anything that has the potential to cause loss and damage to information (Pfleeger and Pfleeger 2012).

Information Security Governance Frameworks and Standards

Information Security Governance (ISG) is part of corporate governance that produces a strategic direction, ensures that each goal is achieved, manages risks appropriately, uses organizational resources responsibly, and monitors the success or failure of corporate information security programs (Caballero 2014). ISG is implemented to ensure the confidentiality, integrity, and availability of an organization's electronic assets (data, information, software) and protect it from risks and threats (Solms 2007). To achieve effective information security governance, it is necessary to adopt a proper information security framework. The ISG framework can provide guidance in implementing a successful information security program, risk management, and monitoring. In addition, the ISG framework can also recommend controls needed to protect information as well as being used as an assessment tool for evaluating the implementation of information security. There are several ISG frameworks that are popularly used in the world of information security, including ISO 17799:2005, COSO, and the IT Risk Framework.

ISO 17799:2005, Code of Practice for Information Security Management is intended as a single point of reference in identifying the range of control required in situations where information systems are used in industry and commerce. ISO 17799 states that information is an asset that must be protected because it has the same position as other important business assets. ISO 17799 divides information security control into 11 areas, namely security policy, organization of information security, asset management, human resources security, physical and environmental security, communications and operations management, access control, information systems acquisition, development, and maintenance, information security. incident management, business continuity management, and compliance.

The COSO framework describes an integrated approach to evaluate management's internal control systems for achieving business objectives. COSO requires a formal risk assessment to evaluate the internal and external factors that affect organizational performance. The results of the risk assessment will determine the controls to be carried out by the organization. COSO focuses on financial controls that have implications for information security. COSO is divided into three dimensions, namely the control component, internal control objectives, and activities towards the organization. The control component consists of 5 aspects, namely risk assessment, control environment, control activities, information and communications, and monitoring.

The IT Risk Framework is one of the ISG frameworks published by ISACA in 2009 which focuses on risk management. The IT Risk Framework is a complement to COBIT which provides a series of controls for identification, governance, and management of IT risks. The IT Risk Framework consists of 3 domains, namely risk governance, risk evaluation, and risk response. The IT Risk Framework describes the IT risks that allow users to integrate IT risk management into the company's Enterprise Risk Management (ERM), thus enabling companies to re-evaluate risk management policies. In addition, the IT Risk framework can help to communicate decisions regarding risks level, the likelihood of risk, and tolerance for risk, as well as understanding how to handle IT risks.

Methodology

To answer the proposed research questions in this study, the authors carried out several stages described in Figure 1. First, an ISG multiple framework adoption strategy will be identified together with information security regulations. The analysis includes information security regulations that must be fulfilled and the ISG framework that will be used in ISG implementation. To find out how effective the implementation of this strategy is, we measure the effectiveness of ISG implementation based on four aspects, namely: organizational dependence on information technology, risk management, people and organizations, and information security program processes. After obtaining the effectiveness of the ISG application in the oil and gas industry, the maturity level of the ISG framework is then measured.

Finally, an analysis of the supporting and inhibiting factors of ISG implementation is studied based on human, organizational, and technological aspects.

Study Case: PT X

PT X is a subsidiary of the fifth-largest integrated energy company in the world based in France. PT X Group is a multinational energy company operating in 130 countries employing 130,000 staff. The scope of PT X's business is upstream operations which focus on exploration and production activities. The tight competition in the oil and gas industry both in the domestic and international markets has encouraged PT X to formulate a strategy in developing its business. The use of information technology is one of the critical factors for achieving the company's success.

PT X utilizes information technology to connect and exchange data and information between sites as well as with its Asia Pacific branch located in Singapore. The exchange of data and information takes place in real-time. To support all these business activities, an enormous investment in information technology has been made. To ensure the running of business processes and manage its investment in information and communication technology, PT X set up an Information System and Telecommunication division. Information System and Telecommunication division consists of several departments that handle specific aspects of information technology such as IT governance, telecommunications, and IT support. To protect data and information that constitute company assets, PT X has an information security organization controlled and managed by the Head Quarter of PT X Group. PT X Group has a commission responsible for information security called the Information Security and Control Committee (CSIC) based in France. CISC is responsible for formulating any policies related to information security, including determining ISG framework that needs to be followed throughout the organization.

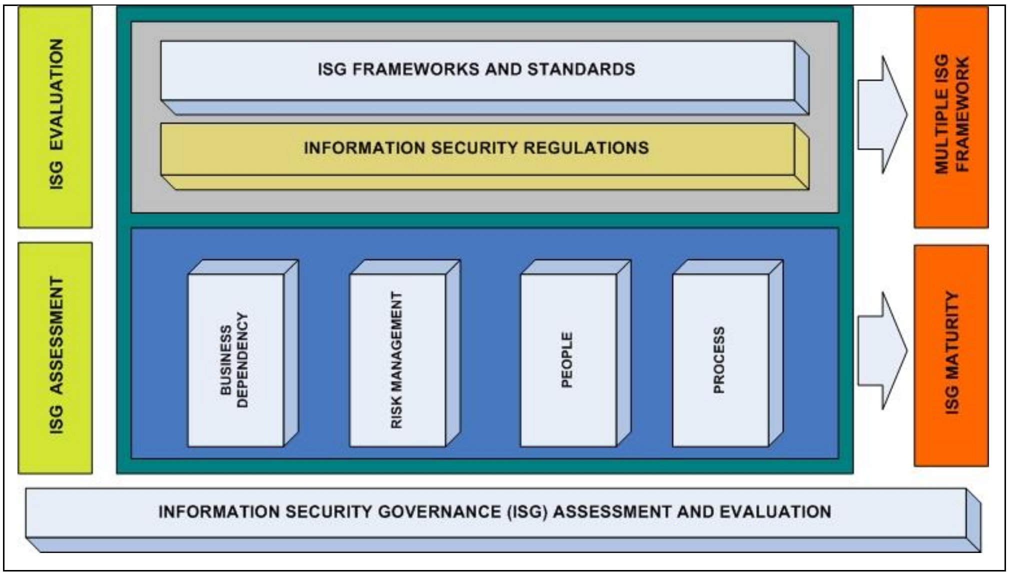
ISG EVALUATION
ISG ASSESSMENT
ISG FRAMEWORKS AND STANDARDS
INFORMATION SECURITY REGULATIONS
BUSINESS DEPENDENCY
RISK MANAGEMENT
PEOPLE
PROCESS
MULTIPLE ISG FRAMEWORK
ISG MATURITY
INFORMATION SECURITY GOVERNANCE (ISG) ASSESSMENT AND EVALUATION

Figure 1. The Conceptual Framework – ISG Assessment and Evaluation

Research Instruments

As qualitative research, this study uses a list of interview questions as the research instruments. The questions are developed in semi-structured and open-ended question styles. The author divides the list of questions into three parts, namely, a list of questions to identify the application of multiple ISG frameworks along with information security regulations, a list of questions related to the evaluation of ISG implementation, and a list of questions related to supporting and inhibiting factors for ISG implementation. The author also conducts pilot testing before starting to collect the data. Pilot testing is conducted to ensure that the questions are easy to understand and do not have multiple meanings.

Data Collection

Data collection for this study was carried out in two ways, namely in-depth interviews, and literature study. In-depth interviews are one of the qualitative research approaches used to deeply understand one's point of view on the topics being discussed. This method was chosen because the research objective was to determine the adoption of multiple ISG Frameworks, practices, and maturity levels of ISG implementation, as well as supporting and inhibiting factors for ISG implementation in the oil and gas industry in Indonesia. This study uses primary data and secondary data. The primary data were obtained by making direct observations in the field and conducting interviews with several key persons that manage information security at PT X. Meanwhile, secondary data were obtained through literature studies from journals, books, and the internet to collect data related to research on ISG implementation as well as supporting and inhibiting factors for ISG implementation. The secondary data used to support and strengthen the analysis of the research.

Data Analysis

1) Evaluating the Effectiveness of Multiple ISG Framework Implementation

The author measures the effectiveness of multiple ISG framework strategies by looking at the framework's ability to meet the information security regulations that must be followed. Comparisons were made using information security control variables from COSO, ISO 17799, and the IT Risk Framework. The three frameworks are used as a comparison because they have a control focus which includes information security management, risk management, and internal controls. The fulfillment of the comparative variables will show how effective the strategy used in covering information security regulations is.

Each framework will be compared and assessed based on 18 comparison variables. The scoring is conducted by evaluating two dimensions, which include the completeness of ISG process and the detailed standards in technical and operational terms. The horizontal dimension shows the completeness of the fulfillment of the 18 variables used as comparison variables for the ISG framework. The assessment is conducted by analyzing whether each framework has appropriate control for each variable. Meanwhile, the vertical dimension shows the extent of details of each procedure related to the technical and operational aspects. The assessment is carried out by analyzing the details of the technical and operational procedures of the variables. Table 1 and Table 2 show the scoring system for the first dimension and second dimension, respectively.

Table 1. ISG Process Compliance Level

Low	High	Compliancy
0	3	Very low
4	7	Low
8	11	Medium
12	15	High
16	18	Very high

Table 2. The Level of Technical and Operational Detail

Deepness	Score	Criteria
Low	1	Only a small number of controls can be fulfilled
Medium	2	Most of the controls can be fulfilled
High	3	All controls can be fulfilled

The total score for the technical and operational level of detail will be added up and the average value is sought to describe in general the results of the assessment so that it can be mapped into the low, medium, and high levels with the average value formula which can be seen in Equation 1. After obtaining the average value, based on the results of the assessment of 2 dimensions which include: the completeness of the ISG process and the level of technical and operational detail of each control, the mapping of the result is developed as shown in Figure 2.

$$\overline{x} = \frac{\sum x_i}{n} \quad (1)$$

Xi : the value of the level of technical and operational detail

n : number of comparison variables

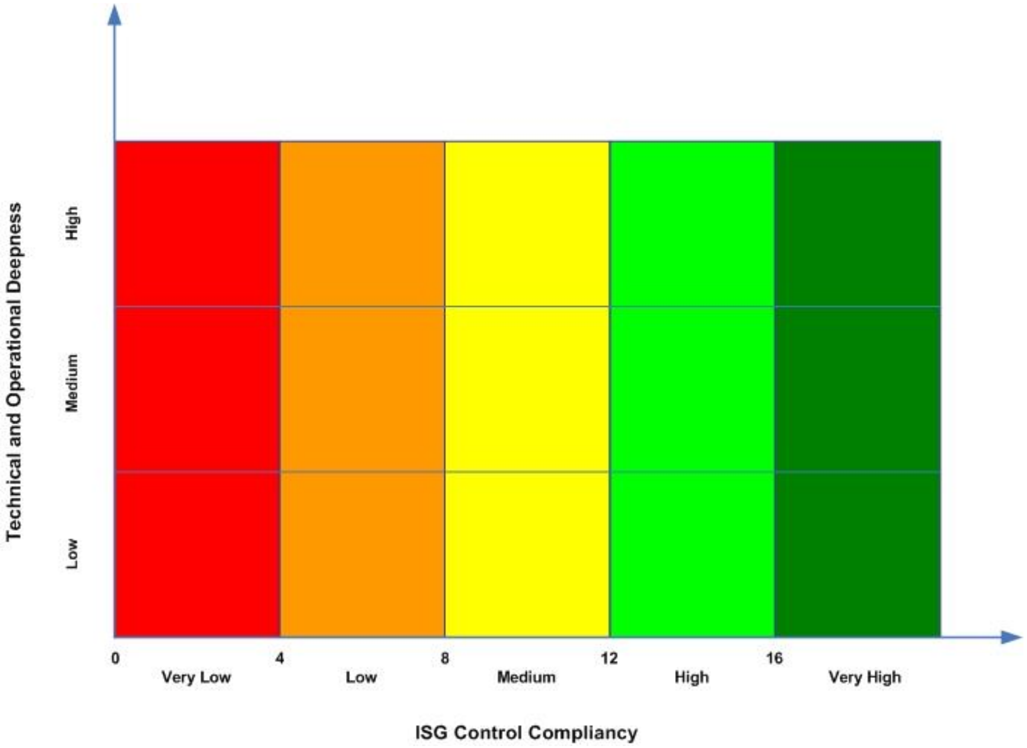

Figure 2. Mapping of ISG Process Completeness and ISG Technical and Operational Detail Level

2) *Evaluating the Maturity Level of ISG Implementation*

Data related to ISG implementation practices obtained from interviews were then analyzed using the ISG Assessment Tools published by the Corporate Governance Task Force to obtain a maturity level for ISG implementation. The Maturity level of ISG implementation is based on the answer to the interview question. Maturity level determination is divided into 4 parts, namely: Business Dependency Evaluation, Risk Management, People, and Processes. Table 3 shows an example of the maturity level scoring for each component.

3) *Identifying of the Supporting and Inhibiting Factors for ISG Implementation*

Data related to supporting and inhibiting factors for successful ISG implementation were obtained from interviews and then analyzed by conducting in-depth discussions between the authors and key persons. The author proposes a list of factors that influence the success of ISG implementation which is acquired from previous studies related to ISG. Then, the authors discuss each factor with the key persons to determine which factors play essential role. In the discussion, the key persons give arguments and evidence related to the critical factors for the successful implementation of ISG. Next, authors and key persons jointly formulate the factors that greatly influence or inhibit the successful implementation of ISG. The formulation of the factors is based on the existing evidence which is highly experienced by the company.

Table 3. Level of Technical and Operational Detail

Aspect	Rating Ranges	Maturity Level	State
Risk Management	0 – 6	0	Not Implemented
	7 – 13	1	Planning Staged
	14 – 20	2	Partially Implemented
	21 – 27	3	Close to Completion
	27 – 36	4	Fully Implemented
People	0 – 9	0	Not Implemented
	10 – 19	1	Planning Staged
	20 – 29	2	Partially Implemented
	30 – 39	3	Close to Completion
	40 – 48	4	Fully Implemented
Processes	0 – 27	0	Not Implemented
	28 – 55	1	Planning Staged
	56 – 83	2	Partially Implemented
	84 – 111	3	Close to Completion
	112 – 136	4	Fully Implemented

Results

Evaluating the Effectiveness of Multiple ISG Framework Implementation

To comply with regulations related to information security in the oil and gas sector, PT X is trying to combine several ISG frameworks that are tailored to its business needs. PT X has a framework developed by the Information Security & Control Committee (CSIC), the highest structure of the PT X Group information security organization. This framework is called the XYZ Framework and applies globally to PT X Group. The author compares the XYZ Framework with ISO 17799, the IT Risk Framework, and COSO by mapping the controls of each framework against the comparison variables. There are 18 information security controls used in this study, as can be seen in Table 4.

Next, an evaluation of the completeness of the ISG processes is carried out from two dimensions (Knapp et al. 2011). The vertical dimension describes the level of detail or standard depth in technical and operational terms. Meanwhile, the horizontal dimension sees the compliancy of the ISG process, using a score scale of 1 to 18 which has been divided into 5 parts, namely very low, low, medium, high, and very high which have been described in the methodology chapter. The results of the 2-dimensional evaluation are then depicted in matrix form as can be seen in Figure 3.

Based on the matrix in Figure 3, it can be concluded that the XYZ Framework which is developed based on a combination of COSO, IT Risk, and ISO 17799 has compromised horizontal and vertical dimensions, but still better among other ISG frameworks. The XYZ framework as a tailored framework has a broader and more detailed spectrum of ISG processes. Conversely, ISO 17799 only focus on the detail and depth in defining ISG processes that are technical and operational in nature. Meanwhile, COSO has superficial details, despite the broad spectrum of ISG compliancy. Finally, the IT Risk Framework lacks a spectrum of compliance with ISG controls because it is only focused on risk management. The effectiveness of implementing the XYZ Framework as a multiple ISG framework is considered very high because it is able to cover more controls and meet several information security regulations and business interests at once. Therefore, the use of multiple frameworks such as the XYZ

Framework is considered better than adopting a single framework such as COSO, ISO 17799, and the IT Risk Framework.

Table 4. Results of Compliance Assessment of ISO 17799, COSO, IT Risk, and XYZ Framework

Information Security Control	ISO 17799		COSO		IT Risk Framework		Framework XYZ	
	Compliancy	Score	Compliancy	Score	Compliancy	Score	Compliancy	Score
Security Policy	High	3	Medium	2	Medium	2	High	3
System Access Control	High	3	Low	1	-	0	High	3
Communication and Operation management	High	3	Medium	2	-	0	High	3
System Development and maintenance	High	3	Low	1	-	0	High	3
Physical and Environmental Security	High	3	Medium	2	Medium	2	High	3
Compliance	High	3	High	3	Low	1	High	3
Human Resource Security	High	3	High	3	Medium	2	High	3
Security Organization	High	3	Medium	2	-	0	High	3
Asset Management	High	3	-	0	High	3	High	3
Business Continuity management	High	3	High	3	Medium	2	High	3
Information Security Incident Management	High	3	Medium	2	High	3	High	3
Risk Governance	-	0	-	0	High	3	Medium	2
Risk Evaluation	Medium	2	Medium	2	High	3	Medium	2
Risk Response	Medium	2	Low	1	High	3	High	3
Control Environmet	Medium	2	High	3	Medium	2	High	3
Control Activities	High	3	High	3	Medium	2	High	3
Information and Communication	Medium	2	High	3	-	0	High	3
Monitoring	Medium	2	High	3	Low	1	High	3
TOTAL	**17**	**46**	**16**	**36**	**13**	**29**	**18**	**52**
AVERAGE		**2.55**		**2**		**1.66**		**2.89**

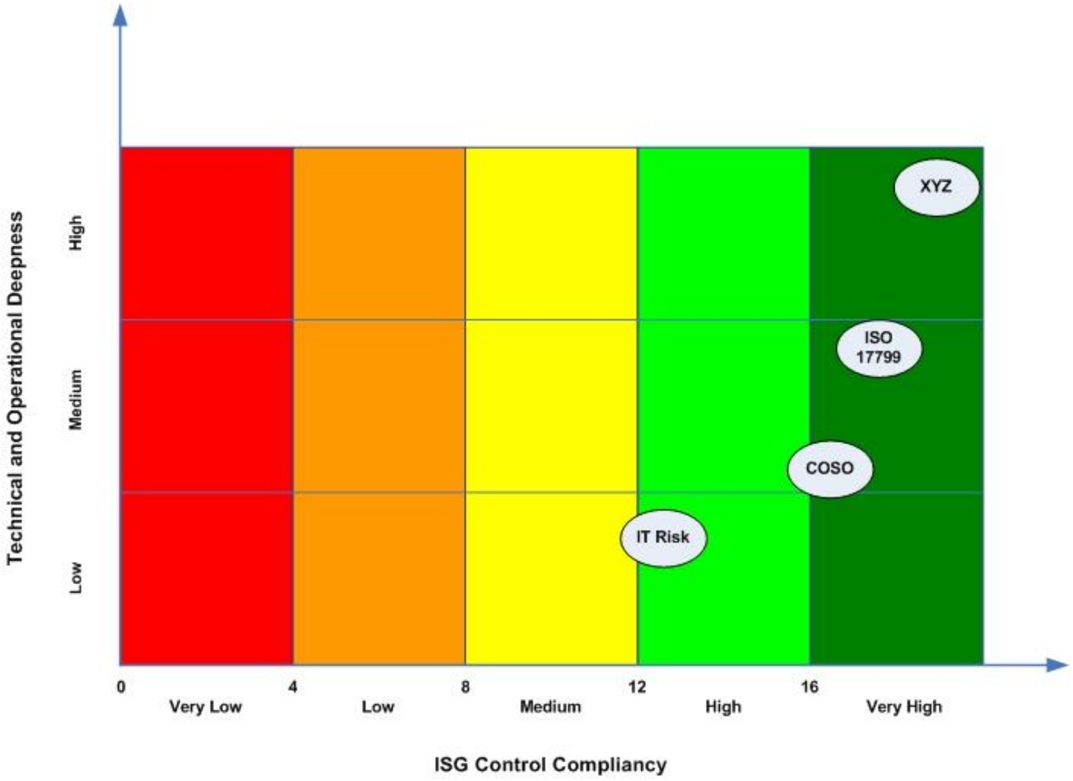

Figure 3. The Comparison of ISG Frameworks' Effectiveness

Evaluating the Maturity Level of ISG Implementation

The analysis of the ISG implementation maturity level can be used to determine the compliance of PT X with the XYZ Framework as a guideline for implementing the ISG. To find out the status of ISG implementation conducted at PT X, a level of maturity measurement was carried out which included (1) identification of business dependence on IT, (2) identification of risk management implementation, (3) identification of human aspects, and (4) identification of processes.

As previously explained, the measurement of maturity levels is carried out by adopting the ISG Assessment Tools issued by the Corporate Governance Task Force. Based on the evaluation results on the aspects of Business Dependency Evaluation, Risk Management, People, and Processes, the following results were found.

1) *Business dependency aspect*
PT X's dependence on the use of information technology in supporting and serving its business processes is included in the "High" criteria with a value of 49. With its high dependence on IT use, information security occupies an important position in company policy.
2) *Aspects of risk management, people, and processes*
Risk management, people, and processes as part of the aspects assessed and evaluated by the author are very important parts of a series of ISG controls. The fulfillment of these three aspects shows the effort of fulfilling the ISG implementation. The results of the evaluation and assessment of the aspects of risk management, people, and processes can be seen in Table 5. Based on the evaluation that has been done, it can be concluded that the aspects of risk management, people, and processes are included in the criteria "Needs Improvement" with a value of 169.

Table 5. Results of the Assessment of Risk Management, People, and Processes Aspects

Aspect	Current Maturity	Expected Maturity
Risk Management	22	36
People	40	48
Processes	107	136
TOTAL	**169**	**220**

Next, an analysis of the gap between the current maturity level and the expected maturity level is carried out in the aspects of risk management, people, and processes as can be seen in Figure 4. From the results of this evaluation, it can be concluded that PT X needs to make improvements and improvements to its ISG efforts. Additionally, the gap between the current maturity level and the expected maturity level shows that PT X does not comply with what has been established as an information security procedure in the XYZ Framework. Therefore, PT X must make improvements and reduce the maturity level gap by complying with and adhering to the XYZ Framework in implementing ISG.

Identifying of the Supporting and Inhibiting Factors for ISG Implementation

The existence of gaps in the expected maturity level and current maturity level in ISG implementation indicates that it is necessary to make improvements to the health of ISG implementation at PT X. Improvements should be supported by strengthening supporting factors and removing inhibiting factors for ISG implementation. Therefore, at the final stage of the research, the supporting and inhibiting factors of ISG implementation were identified at PT X by looking at 3 aspects, namely human aspects, organizational aspects, and technological aspects. Identification is done by conducting interviews and comparing the supporting and inhibiting factors for the implementation of the ISG adapted from previous research. The comparison results can be seen in Table 6.

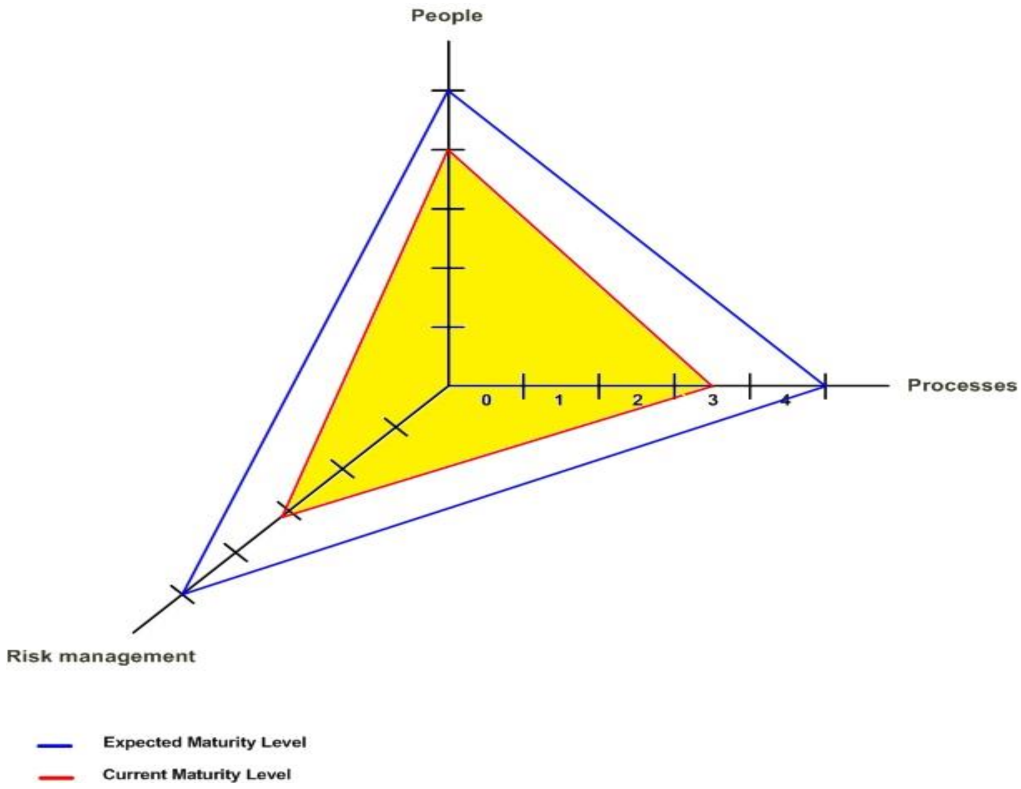

Figure 4. The Gap between Current and Expected Maturity Level

Table 6. Results of the Assessment of Risk Management, People, and Processes Aspects

Aspects	Related Research	Factors from Prior Research	Confirmed Factors	Remarks
Human	(Abu-zineh 2006; Furnell et al. 2009)	• Awareness and training programs • Motivation of employee • Culture • Communication of security issues	• Awareness and training programs	• Supporting factors for ISG implementation
Organization	(Abu-zineh 2006; Furnell et al. 2009; Kankanhalli et al. 2003)	• Risk estimation • Open environment and academic freedom • Top management support • Information Security Policy (ISP) • Job responsibility • Compliance with the information security standard • Business relationship with other organizations • Using service of information security external advisor	• Risk estimation • Top management support • Information Security Policy (ISP) • Job responsibility • Compliance with the information security standard	• Inhibiting factors for ISG implementation • Supporting factors for ISG implementation
Technology	(Furnell et al. 2009)	• Complexity of systems • Mobility and distributed access • Vulnerabilities (systems and application)	• Complexity of systems • Mobility and distributed access	• Inhibiting factors for ISG implementation

Based on the results of interviews and discussions between the author and the informants, it was concluded that the supporting and inhibiting factors for the implementation of ISG in PT X were influenced by the following:

1) *The human aspect*
Awareness and training programs are supporting factors for the implementation of ISG at PT X.
2) *Organizational aspects*
There are four determinants of ISG implementation which include: (1) risk estimation, (2) management support, (3) application of Information Security Policy (ISP), (4) division of job responsibilities, and (5) compliance with information security standards. Of the five factors, risk estimation is an inhibiting factor for the successful implementation of ISG at PT X, while management support factors, implementing ISPs, distribution of job responsibilities, and compliance with information security standards are supporting factors for the successful implementation of ISG at PT X.
3) *Technological aspects*
There are two factors that greatly influence the implementation of ISG at PT X. These two factors are challenges and obstacles to ISG implementation which include: (1) complexity of information systems and applications and (2) mobility and distribution access.

Discussion

Based on the results of the evaluation of the ISG implementation, it was found that PT X's dependence on information technology was very high and still needed improvements in implementation efforts. Therefore, PT X should have made several improvements, especially in the aspects of risk management and security administration programs. Improvements can be made by adhering to the five bases of effective ISG implementation which consists of an alignment of strategies with business needs, resource management, risk management, performance measurement, and value delivery (Caballero 2014).

Meanwhile, the alignment between the ISG strategy and business needs must be made considering the high dependence of businesses on information technology. ISG's position as part of corporate governance shows the importance of ISG's position, for this reason, the ISG strategy should be aligned with the company's business needs. Furthermore, the management of resources owned by PT X has shown very good efforts. First, the classification of security and physical security are used in protecting company assets. Despite the goof efforts, improvements are still needed, especially in human resources aspects. For example, information security staff training must be carried out in order to improve the skills and qualifications of the staff, so as to increase work productivity.

Risk management is considered as an appropriate step to manage and reduce risk and the potential threats on information resources towards an acceptable level (Purser 2004). Increasing risk management efforts can be done by implementing the classification and identification of company information and assets. High dependence on the use of information technology should be followed by excellent risk management. The classification and identification of a company's critical assets can be used as a reference for decision making on ISG's efforts and for business impact analysis. The XYZ Framework has clearly defined risk management and classification of company critical information and assets, therefore it is time for PT X to comply with the procedures and guidelines in the XYZ Framework.

The implementation of security administration program efforts which include evaluation, review, and audit of information security programs on a regular basis is part of the performance measurement step. Performance measurement and evaluation is one of the bases for effective ISG implementation (Albert 2016; Bowen et al. 2006; Caballero 2014). The security administration programs at PT X are still very weak and are still in the planning stage. Security administration programs are very important in knowing the status of ISG implementation and measuring the extent to which the efforts that have been made are used as a basis for making improvements.

Value delivery is an important part that must be implemented in the application of ISG. Value delivery is enhanced by optimizing information security investments in support of organizational goals. In the case of PT X, it is appropriate for PT X to carry out a cost estimation of information security efforts and to have a strategy in calculating the cost-effective risk and investment in information security to an acceptable level. With improvements in the five aspects above, especially for the aspects of risk management and performance measurement, the implementation of ISG as part of corporate governance at PT X can be done optimally to protect company information security and in line with business needs.

Conclusion

This study evaluates the effectiveness of implementing the multiple ISG framework strategies when compared to the application of a single ISG framework. Effectiveness is measured by looking at the completeness of ISG processes and the level of compliance with information security regulations in the oil and gas industry. Based on the evaluation results, it was found that the multiple ISG framework XYZ strategy has better effectiveness compared to the adoption of a single ISG framework. This is because the implementation of the XYZ Framework as a strategy for multiple ISG frameworks is able to cover the requirements of the three ISG frameworks, namely ISO 17799, COSO, and the IT Risk Framework in meeting information security regulations and standards.

An assessment of the practice and adherence to the ISG implementation strategy shows that PT X has a high dependency on the use of information technology. With these criteria, ISG as part of corporate governance occupies an important position in company policy considering the importance of protecting information security as a company asset. Meanwhile, the overall evaluation results from the aspects of risk management, people, and processes are included in the "Need Improvements" criteria. The results of the evaluation of the ISG framework implementation maturity level show a significant gap between the current maturity level and the expected maturity level. This gap reflects the inequality between ISG implementation efforts and company expectations of ISG implementation. Therefore, it is time to increase information security efforts considering the importance of information and data as company assets and the position of ISG as part of corporate governance.

Finally, this study has identified the supporting and inhibiting factors for the application of ISG at PT X, as a company engaged in the oil and gas industry. The identification of supporting and inhibiting factors is carried out by looking at three aspects, namely human aspects, organization aspects, and technology aspects. In the human aspect, security awareness and training programs are factors driving the implementation of ISG at PT X. The implementation of security awareness and training programs is deemed to be very helpful in the implementation of ISG because it forms the character of users who are aware of the importance of information security. In the organizational aspect, there are five factors that determine the successful implementation of ISG. Management support factors, implementation of Information Security Policy (ISP), division of job responsibilities and compliance with information security standards and guidelines are all supporting factors for ISG implementation. Risk estimation is an inhibiting factor for the implementation of ISG in organizational aspects. Risk estimation is an inhibiting factor because this business is still reactive, marked by the absence of information classification and critical asset data collection. In the technological aspect, the complexity of information systems and applications as well as mobility and distribution access are inhibiting factors for ISG implementation. The challenges and obstacles in this technological aspect are caused by the geographical conditions of PT X's operational areas which are scattered and located in areas that are difficult to reach.

This research has limitations. First, the limited number of case studies is one of the constraints and limitations of the research. This causes the research findings to be imperfect and requires additional data and analysis so that generalizations can be made to the research results. Furthermore, this study relies on interviews as a data collection method. Future research is expected to combine the results of the interview with the questionnaire (mixed method) to reduce the subjectivity of the processing and analysis results of the interview. Finally, this study only compares multiple XYZ frameworks with the ISO 17799 framework, COSO, and the IT Risk Framework. In the future, it is hoped that further research can enrich the framework that will be compared, such as COBIT and ITSM.

References

Abu-zineh, S. 2006. “Success Factors of Information Security Management - A Comparative Analysis between Jordanian and Finnish Companies,” *The Swedish School of Economics and Business Administration*. (http://www.pafis.shh.fi/graduates/samabu04.pdf, 2006, accessed 01 June, 2020).

Albert, K. 2016. “Computer Security Tools and Concepts for Lawyers,” *SSRN Electronic Journal*.

Baskoro, A. H. 2019. “Migas Penyumbang Pendapatan Kedua Terbesar Setelah Pajak,” *Suarasurabaya.Net*. (https://www.suarasurabaya.net/ekonomibisnis/2019/Migas-Penyumbang-Pendapatan-Kedua-Terbesar-Setelah-Pajak/, accessed 01 June, 2020).

Boiko, A., and Shendryk, V. 2016. “System Integration and Security of Information Systems,” in *Procedia Computer Science* (104:1), pp. 35–42.

Bowen, P., Hash, J., Wilson, M., Gutierrez, C. M., and Jeffrey, W. 2006. “Information Security Handbook: A Guide for Managers,” *NIST Special Publication 800-100* (October), pp. 137.

Caballero, A. 2014. “Information Security Essentials for IT Managers,” in *Managing Information Security*, pp. 1–45.

Calder, A. 2012. “ISO 27001 and ISO 17799,” in *Governance, Risk, and Compliance Handbook: Technology, Finance, Environmental, and International Guidance and Best Practices*, pp. 169–179.

Ferguson, C., Green P., Vaswani R., and Wu G. 2013. " Determinants of Effective Information

Technology Governance," *International Journal of Auditing* (17:1), pp. 75-99.

Furnell, S. M., Clarke, N., Werlinger, R., Hawkey, K., and Beznosov, K. 2009. “An Integrated View of Human, Organizational, and Technological Challenges of IT Security Management,” *Information Management & Computer Security* (17:1), pp. 4–19.

Kankanhalli, A., Teo, H. H., Tan, B. C. Y., and Wei, K. K. 2003. “An Integrative Study of Information Systems Security Effectiveness,” *International Journal of Information Management* (23:2), pp. 139–154.

Knapp, K. J., Marshall, T. E., Rainer Jr., R. K., and Ford, F. N. 2011. “Information Security Effectiveness,” *International Journal of Information Security and Privacy* (1:2), pp. 37–60.

Pfleeger, C., and Pfleeger, S. L. 2012. *Analyzing Computer Security: A Threat/Vulnerability/Countermeasure Approach*, Massachusetts: Prentice Hall.

Purser, S. 2004. *A Practical Guide to Managing Information Security*, Norwood: Artech House.

Solms, V. 2007. *The Relationship between Corporate Governance, Information Technology (IT) Governance and Information Security Governance and ICT Risk Management System to Support Information Security Governance*, Johannesburg: University of Johannesburg.

How to cite:
Syahbuddin, B. H., Azzzahro F., Afrida W. Y., Hidayanto A. N., and Phusavat, K. 2020. “ The Implementation of Multiple Information Security Governance (ISG) Frameworks Strategy and Critical Success Factors in Indonesia’s Oil and Gas Industry: Case Study of PT X ,” *Jurnal Sistem Informasi (Journal of Information System)* (16:2), pp. 43–56.