ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 6, Issue 5, May 2021

Electronics Risk Management Practices of Selected Semiconductor Companies in Laguna: Inputs to Enhancement Program

Jason V. Dollente

MBA Candidate, Laguna College of Business and Arts
Email: dollente.jason@gmail.com

Abstract--- This study was conducted to determine the employees' awareness and effectiveness level of Electronics Risk Management Practices (ERMP) of selected semiconductor companies in Laguna. A descriptive correlational method was utilized as the research design. The researcher used G* Power analysis to determine the sample size of the study. Moreover, this study employed a stratified random sampling procedure for selecting the participants. The study was conducted in three manufacturing companies; American, Japanese, and Filipino-owned semiconductor firms situated at Cabuyao, Sta. Rosa, and Biňan respectively. The respondents were the rank and file employees who are the beneficiaries of risk management practices. Quantitative data were collected utilizing a technique of researcher-made structured survey as an instrument. Using the four-point Likert Scale and the simple mean, Analysis of Variance, and Pearson-r correlation coefficient, findings revealed that the respondents were aware in terms of the nature of electronic risk, risk vulnerability, and risk management. There was no significant difference in the level of awareness among the group of respondents in terms of the nature of electronic risk and risk management, while there was a significant difference in terms of risk vulnerability. The effectiveness level of ERMP in terms of risk identification, assessment, treatment, policy, and governance was effective as assessed by the respondents. Furthermore, the employees' awareness level has a significant relationship to the effectiveness level of ERMP. As an output of the study, an enhancement program that can address the needs of employees to maximize risk awareness towards maximum effectiveness of ERMP was proposed.

Key word--- Electronic Risk, ERMP, Risk, Risk Awareness, Risk Management

I. INTRODUCTION

Risk Management (RM) has been increasingly adopted in the industry, it builds a structure for individual operations to develop solutions to the risk faced based on the surrounding environment, condition, equipment, and personnel involved. Risk management is a technique that minimizes losses. The organization manages risk by identifying, analyzing, and then evaluating whether the risk should be modified by risk treatment in order to satisfy risk criteria (ISO 31000:2011).

The importance of risk management in the semiconductor and electronics industry is acknowledged. The industry faces unpredictable tastes on the demand side, disruptions on the supply side, and production challenges in the middle. How the company responds to the risks determines the severity of the impact.

The risks involved in the automation testing (ATE process) in the semiconductor industry are the primary focus of this research. The risk involves test scripts version control and safeguard of test data, compatibility of test automation systems with the test environment, and other software testing tools in the test environment, underestimation of human tester potential in some application environments, and vendor concerns such as; failure to provide technical assistance, inability to upgrade automation testing tools with improvements to the product testing platform and test environment, and liquidation of the distributor company. Semiconductor companies must have effective electronics risk management practice in order to mitigate uncertainties, survive, improve and grow.

The role of risk awareness as the basis of risk management is increasingly noted in the literature. The rapid, complex, and continually evolving nature of today's business and social environment is widely debated. Despite the existence of rich literature in the fields of risk management, there is inadequate information about Electronics Risk Management Practices (ERMP) of semiconductor and electronics industry in the Philippines as well as the inconclusive evidence with regards to the relationship of the employee's awareness and the effectiveness of ERMP in the semiconductor industry prompted the researcher to embark on this study.

Theoretical Framework

The study is anchored on the following theories: The Probability theory, Attribution theory, and Decision theory. The theory of probability has developed overages since

Galileo was first introduced as part of his experiments on the dice game (Maistrov, 1974). The objective of probability theory is to analyze and illustrate the sequence of randomized trials. The concept of risk could have a specific meaning under the condition of known probabilities which are classified into two distinctions, the subjective and objective interpretations. According to objective probability, the estimation of the likelihood that something will happen by using observations. Subjective probability, on the other hand, is a guess which is based on personal experience.

The Hale and Glendon model (1987) considers that danger is still present at the workplace and conceptualizes the role of human intervention in risk management. Attribution theory is concerned with how individuals interpret evidence to determine the causality of events.

Lastly, Decision theory is concerned with calculating the consequences of uncertain decisions (Peterson, 2013). Risk management is concerned with making decisions to manage uncertainties and their consequences. Decision theory is about evaluating choices people make. When information on the decision maker's risk-taking behavior is available, decision theory can prioritize risks and prescribe how to react to them numerically.

Conceptual Framework

Following the above cited theoretical framework, the proponent of the study conceptualized his research as shown in figure.

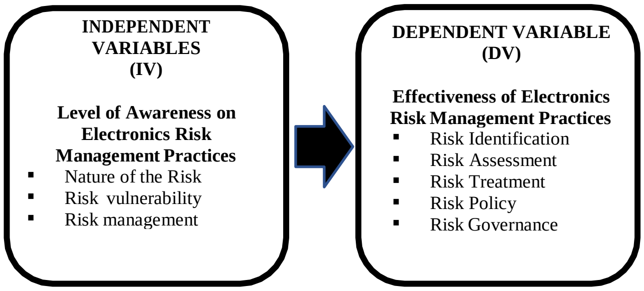

Figure 1. Research Paradigm

In this study, the researcher sought to investigate whether the level of employee's awareness (independent variable) has a relationship on the effectiveness of ERMP (dependent variable), as shown in Figure 1.

Statement of the Problem

The study assessed the current ERMP of the semiconductor industry. The analysis of the findings aimed to give practical implications for leaders on how they conceptualize accordingly to maximize the effectiveness of ERMP.

The research sought to answer the following questions:

1. What is the level of awareness on the current Electronics Risk Management Practices as perceived by the American, Japanese, and Filipino Semiconductor Company employees in terms of:

1.1. Nature of risk,

1.2. Risk vulnerability, and

1.3. Risk management?

2. Is there any significant difference among the responses of the American, Japanese, and Filipino company employees on the current Electronics Risk Management Practices in terms of the above-mentioned variables?

3. What is the level of effectiveness on Electronics Risk Management Practices of the selected semiconductor companies in Laguna in terms of:

3.1 Risk Identification,

3.2 Risk Assessment,

3.3 Risk Treatment,

3.4 Risk Policy, and

3.5 Risk Governance?

4. Is there any significant relationship between the level of awareness and effectiveness of the current Electronics Risk Management Practices of the selected semiconductor companies in Laguna?

5. Based on the results of the study, what inputs to enhancement program can be proposed?

Hypothesis

This study attempted to test the following null hypotheses at a 0.5 level of significance:

Ho 1. There is no significant difference among the assessments of employees of American, Japanese, and Filipino semiconductor companies on current Electronics Risk Management Practices.

Ho 2. There is no significant relationship between the level of awareness and effectiveness of the current Electronics Risk Management Practices in the selected semiconductor companies in Laguna.

Review of Related Literature

The researcher found the following literature and studies to be of great help in conceptualizing the study. All these resources and studies helped in the formulation and analysis of the findings.

The authors named Simota et al. (2017), Alseiari (2015), Renault et al.(2016), Kutsch (2015), and Rostami (2016), shared common insights that the reduction of incidents and achievement of operational discipline is based on the employee's awareness and sensitivity to the nature of risks that may occur in the workplace. They stressed out that risk awareness is a combination of vulnerability assessment and knowledge management, which provides critical input to the risk identification process within the overarching risk management framework of the organization.

In thoughts about the risks involved in automation testing in the semiconductor industry, Priya Sr. (2018), sighted the risks of automation testing. His journal focused on the benefits and disadvantages of automated testing equipment in terms of reliability, test scripts, test scenarios, valuation of time and effort, version control and compatibility, and vendor issues. While Spacey (2016) and Zurkus (2017), stressed out that these potential technology risks and vulnerabilities may disrupt business operations. Therefore, each enterprise must develop its awareness schemes and policies to identify and understand what could go wrong, and additionally develop crisis management strategies, particularly for unforeseen negative incidents.

Gaps Bridged by the Study

In most of the literature on electronics and technical risks, almost all of the impacts reported will be data loss, software breaches, but very minimal in terms of product safety and quality. In addition, conventional risk management methods generally prioritize risk by using the probability and impact of risk events. This approach appears to be imperfect because the risk is influenced by many additional factors. The aim of this study is to contribute to understanding or awareness of these electronics risks towards the effectiveness of risk management practices.

Lastly, only a few risk management practices about semiconductors are supported by a learning mechanism. This is due to the limited publications because of information security or nondisclosure to the public.

II. METHODOLOGY

Research Design

The study utilized the descriptive-correlational research in determining the employees' awareness and effectiveness level of Electronics Risk Management Practices of selected semiconductor companies in Laguna.

Descriptive Correlational Research is used to describe the relationship among variables rather than to infer cause and effect relationships. This is the most appropriate design for the study, as it assesses the relationship between the independent and dependent variables.

Research Instrument

The proponent utilized the researcher-made questionnaire as an instrument of the study. The questionnaire's constructs were developed to measure the level of employees' awareness and the effectiveness of risk management. The questionnaire in this research consists of two parts. The first part determines the awareness level of various employees of selected semiconductor companies based on the following variables: Nature of electronics risk, Risk vulnerability, and Risk Management. The second part of the questionnaire measures the effectiveness level of risk management practices in terms of the following: Risk Identification, Risk Assessment, Risk Treatment, Risk Policy, and Risk Governance.

The questionnaire uses 4-point Likert scales. A numerical score was associated with each response and this reflected the degree of attitudinal favorableness. After the researcher's questionnaires were checked, improved, revised, and validated, the researcher secured permission from the human resource department of each company to deploy the instrument where the target respondents are employed.

Respondents/Participants of the Study

The study was conducted in three manufacturing companies, American, Japanese, and Filipino semiconductor firms. The participants were the rank and file employees who are the recipients and implementers of risk management practices. The researcher utilized G*Power, a statistical software, in determining the respondents of the study. There were a total of one hundred forty-four (144) respondents. They consist of forty-eight (48) participants in each company representing thirty-three percent point three percent (33.3%) of the sample population.

Data Gathering Procedure

The researcher sought consent and approval from the human resource department of the selected manufacturing companies to conduct research in their firms. Following the affirmation, questionnaires were distributed to the target respondents. Participants were asked to answer the item honestly and properly. After completion, the questionnaires were collected, tallied, analyzed, and interpreted. Moreover, the researcher consulted a statistics expert for the treatment of the gathered information.

Treatment of Quantitative or Qualitative Data

The following are the statistical treatments applied to the study by the statistician using Statistical Package for Social Sciences (SPSS):

1. The mean and the four-point Likert Scale was used to describe the awareness level of the employees of semiconductor companies and the effectiveness level of ERMP.
2. To determine the significant difference of employees' awareness among selected semiconductor companies, the Analysis of Variance was used.
3. To determine the significant relationship between the awareness and effectiveness level of ERMP, The Pearson Correlation Coefficient (Pearson's r) was used.

III. RESULTS AND DISCUSSIONS

This presents the interpretation and analysis of data gathered in order to discuss the answers to the research problems of the study. The study attempts to determine the level of employee awareness and effectiveness of electronics risk management practices of the selected semiconductor companies in Laguna.

1. The Level of Awareness on the Current Electronics Risk Management Practices as Perceived by the Employees of Semiconductor Companies in terms of:

1.1 Nature of Risk

Table 1.1 shows the level of awareness on the current Electronics Risk Management Practices as perceived by the employees of semiconductor companies in terms of the Nature of Risk.

Table 1.1

The Level of Awareness on the Current Electronics Risk Management Practices as Perceived by the Employees of Semiconductor Companies in terms of Nature of Risk

Indicators	Composite	
	$\bar{X}$	VI
Employees are aware about electronic threats which compromise business information.	3.18	A
Employees are conscious on technical failures such as software/program bugs, computer crash or the complete failure of a computer component	3.15	A
Employees have knowledge about infrastructure failures which could interrupt business operations	2.77	A
Employees understand that human error is major threat on business	3.30	FA
Employees are well knowledgeable that physical threats also compromise not only business operations but also individual security.	3.30	FA
General Assessment	3.14	A

Legend: 3.26 - 4.00 Fully Aware (FA); 2.51 - 3.25 Aware (A); 1.76 - 2.50 Moderately Aware (MA); 1.00 - 1.76 Not Aware (NA)

This generates a general composite assessment of 3.14 and interpreted as Aware. The result indicates that the employees of semiconductor companies are aware and have an understanding in terms of the nature of electronics risk. That the employees were capable to identify sources of risks and threats in their workplace.

According to Cunha et.al, (2015) in their research entitled "Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance", threats can be anything that can take advantage of a vulnerability to breach security and negatively alter, erase, harm objects of interest. When it comes to electronics and business operation, employee mistakes can lead to serious breaches in your information security, breakdowns of your equipment, and much worse is the compromise of product quality.

1.2 Risk Vulnerability

Table 1.2 shows the level of awareness on the current Electronics Risk Management Practices as perceived by the employees of semiconductor companies in terms of Risk Vulnerability.

Table 1.2

The Level of Awareness on the Current Electronics Risk Management Practices as Perceived by the Employees of Semiconductor Companies in terms of Risk Vulnerability

Indicators	Composite	
	$\bar{X}$	VI
The biggest security vulnerability in any organization is its own employees.	3.04	A
The IoT (Internet Of Things) devices represent a massive opportunity to attackers and a massive risk for businesses	2.97	A
The most common form of electronic attack comes as an email mimicking the identity of one of your company's vendors or someone who has a lot of authority or access in the company.	3.27	FA
Programming bugs and unanticipated code interactions rank among the most common computer security vulnerabilities	2.95	A
The most basic tenets of managing software vulnerabilities is the access privileges of software users	2.69	A
General Assessment	2.98	A

Legend: 3.26 - 4.00 Fully Aware (FA); 2.51 - 3.25 Aware (A); 1.76 - 2.50 Moderately Aware (MA); 1.00 - 1.76 Not Aware (NA)

It exemplifies the level of awareness in terms of risk vulnerability has a composite mean of 2.98 interpreted as Aware. This implies that employees are cognizant of electronics vulnerabilities. That these vulnerabilities can be a big deal when there's a threat.

1.3 Risk Management

Table 1.3 shows the level of awareness on the current Electronics Risk Management Practices as perceived by the employees of semiconductor companies in terms of Risk Management.

Table 1.3

The Level of Awareness on the Current Electronics Risk Management Practices as Perceived by the Employees of Semiconductor Companies in terms of Risk Management

Indicators	Composite	
	$\bar{X}$	VI
A risk management plan includes the company’s processes for identifying and controlling threats to its digital assets, including proprietary corporate data, customers’ personally identifiable information (PII) and intellectual property.	3.08	A
The company fosters risk awareness by encouraging event reporting and looking into system design and human factors that contributed to events or errors.	2.94	A
There is clear flow of communication within the organization in case risk, hazard or incidents will be encountered.	3.08	A
Risk management training, coaching or educational programs are being practiced within the organization	3.10	A
Risk management is about taking steps to reduce both the likelihood and consequence of a risk so that the organization best meets its objectives.	3.15	A
General Assessment	3.07	A

Legend: 3.26 - 4.00 Fully Aware (FA); 2.51 - 3.25 Aware (A); 1.76 - 2.50 Moderately Aware (MA); 1.00 - 1.76 Not Aware (NA)

The composite mean is 3.07 which is interpreted as Aware. The result indicates that the employees of semiconductor companies have good adaptable behavior in terms of the risk management program of their company. A robust risk management strategy would permit an organization to develop procedures to prevent future risks. This capacity to consider and monitor the threats enables organizations to be more confident in their business decisions.

According to Renault et al., (2016), in their research paper entitled “A Theoretical Review of Risk Identification: Perspective of Construction Industry,” Risk management cannot be used as means to foresee the future, since this is quite unimaginable. Instead, it is defined by the authors as a means of making the project possible in order to make better decisions based on investment information. In this way, decisions based on poor information will be avoided, and this can lead to better performance.

2. The significant difference on the awareness level of current Electronics Risk Management among the selected semiconductor companies.

Table 2

Test of Significant Difference on the Awareness Level on Current Electronics Risk Management among the Selected Semiconductor Companies

Indicators		Sum of Squares	df	Mean Square	F	Sig.	Decision	Remarks
Nature of Risk	Between Groups	3.801	2	1.900	4.739	.010	Reject Ho	Significant
	Within Groups	56.542	141	.401				
	Total	60.342	143					
Vulnerability Risk	Between Groups	1.977	2	.989	2.856	.061	Accept Ho	Not Significant
	Within Groups	48.816	141	.346				
	Total	50.793	143					
Risk management	Between Groups	3.022	2	1.511	3.659	.028	Reject Ho	Significant
	Within Groups	58.216	141	.413				
	Total	61.238	143					

The respondents of the three companies have different assessments on the nature of risk and risk management. As shown in their probability values of .010 and .028 respectively, are all less than the level of significance at .05. On the other hand, the respondents of the three companies have similar assessments on the vulnerability risk probability values are greater than the level of significance. It implies that the level of awareness of the current electronic risk management practices in determining risk vulnerability has nothing to do with the classification of the group of respondents. However, the nature of risk and risk management have different assessments among the group of respondents.

3. The Effectiveness level of current Electronics Risk Management Practices of Selected Semiconductor companies in Laguna terms of:

3.1 Risk Identification

Table 3.1 shows the effectiveness level of Electronics Risk management practices of the selected Semiconductor companies in Laguna in terms of Risk Identification.

The general composite assessment is 3.12 and interpreted as Effective. This basically implies that the semiconductor companies have developed systems and tools to identify potential risks. Likewise, the company promotes a reporting system that allows employees to report hazards and risks; and propose solutions and improvements. Thinking beyond such incidents and hazard reporting will help the organization to benefit. This provides the data required to enhance decision-making capabilities at the executive and director levels and at other layers of management.

Table 3.1

The Effectiveness Level of Electronics Risk Management Practices of Selected Semiconductor Companies in Laguna in terms of Risk Identification

Indicators	Composite	
	$\bar{X}$	VI
The company publishes specific expectations and procedures for risk identification	3.17	E
The company promotes a reporting system that allows employees to report hazards and risks, issues, concerns, occurrences, and incidents; and propose solutions and improvements.	3.29	HE
The company clearly identifies the levels of management with the authority to make decisions regarding risk acceptance for the organization.	2.94	E
The company develops systems and tools to identify potential risks for electronic threats, technical failures, infrastructure failures, human errors, or physical threats.	3.02	E
Mandates putting up of signs, labels and warnings, to ensure that workers and visitors are aware of the risks before they are exposed to it.	3.15	E
General Assessment	3.12	E

Legend: 3.26 - 4.00 Highly Effective (HE); 2.51 - 3.25 Effective (E); 1.76 - 2.50 Moderately Effective (ME); 1.00 - 1.75 Not Effective (NE)

3.2 Risk Assessment

Table 3.2 shows the effectiveness level of Electronics Risk management practices of the selected Semiconductor companies in Laguna in terms of Risk Assessment.

Table 3.2

The Effectiveness Level of Electronics Risk Management Practices of Selected Semiconductor Companies in Laguna in terms of Risk Assessment

Indicators	Composite	
	$\bar{X}$	VI
The company develops and implements risk assessment plans	3.29	HE
The company identifies function responsible for developing the strategy and policy for monitoring, control and mitigation of the risk	3.28	HE
The likelihood and impacts of risks are quantified using technical performance or quality as a dimension for risk analysis	3.15	E
The company uses systematic methodology and sufficient controls to mitigate electronics and technological threats or vulnerabilities	3.20	E
The company executes different management strategies to deal with negative and positive risk	2.97	E
General Assessment	3.18	E

Legend: 3.26 - 4.00 Highly Effective (HE); 2.51 - 3.25 Effective (E); 1.76 - 2.50 Moderately Effective (ME); 1.00 - 1.75 Not Effective (NE)

The general composite assessment is 3.18 and interpreted as Effective. Semiconductor companies have established a process of identifying hazards and evaluating any associated risks within a workplace. Risk assessment plans should be reviewed periodically by the project team to prevent stalling the analysis.

3.3 Risk Treatment

Table 3.3 shows the effectiveness level of Electronics Risk management practices of the selected Semiconductor companies in Laguna in terms of Risk Treatment.

Table 3.3
The Effectiveness Level of Electronics Risk Management Practices of Selected Semiconductor Companies in Laguna in terms of Risk Treatment

Indicators	Composite	
	$\bar{X}$	VI
An early warning system is being used to track critical risks and decide on activating mitigation measures.	2.96	E
Installs programs or systems that activate alarms and other measures to signal the malfunctions, threats, and risks.	3.01	E
Treatment plans are comprehensive and includes all necessary information	2.95	E
The company practices is on hierarchy of control at all times	3.18	E
Top management support is carried throughout the entire life-cycle of the process.	3.16	E
General Assessment	3.05	E

Legend: 3.26 - 4.00 Highly Effective (HE); 2.51 - 3.25 Effective (E); 1.76 - 2.50 Moderately Effective (ME); 1.00 - 1.75 Not Effective (NE)

The general composite assessment is 3.05 and interpreted as Effective. Semiconductor firms have used systematic methodology and sufficient controls to mitigate risk in the workplace. Risk control measures are implemented in a hierarchy with a view to their effectiveness.

3.4 Risk Policy

Table 3.4 shows the effectiveness level of Electronics Risk management practices of the selected Semiconductor companies in Laguna in terms of Risk Policy.

Table 3.4
The Effectiveness Level of Electronics Risk Management Practices of Selected Semiconductor Companies in Laguna in terms of Risk Policy

Indicators	Composite	
	$\bar{X}$	VI
Risk policies are typically focused and tailored to the major risk types facing an organization	3.28	HE
The risk mitigation measures adopted by the company shall be effective in the long-term and embedded in the business processes of the company.	3.14	E
Tracking of error, issue and failure rates is used as a key performance indicator to track risks	3.11	E
The risk management policy is regularly reviewed and improved	3.17	E
The company develops specific business policies, procedures and code of conduct upon which electronics risk management program is based.	3.00	E
General Assessment	3.14	E

Legend: 3.26 - 4.00 Highly Effective (HE); 2.51 - 3.25 Effective (E); 1.76 - 2.50 Moderately Effective (ME); 1.00 - 1.75 Not Effective (NE)

The general composite assessment is 3.14 and is interpreted as Effective. The result implies that the risk policy of semiconductor companies includes basic guidance for risk management. Policies are usually focused and tailored to the major categories of risk. The aim is to provide guidance on risk control to promote the accomplishment of corporate objectives.

3.5 Risk Governance

Table 3.5 shows the effectiveness level of Electronics Risk management practices of the selected Semiconductor companies in Laguna in terms of Risk Governance.

Table 3.5
The Effectiveness Level of Electronics Risk Management Practices of Selected Semiconductor Companies in Laguna in terms of Risk Governance

Indicators	Composite	
	$\bar{X}$	VI
The company risk management framework sets out the core roles and responsibilities at strategic and operational level	3.06	E
Seeks external support from experts for implementation of risk management program	3.11	E
The company are establishing and practicing communication techniques and information management	3.09	E
Business Continuity Plan (BCP) and Recovery plan are in place	3.19	E
Each business unit or department monitors and ensures that risk management activities are in line with the Company's policy and framework approved by the Board of Directors.	3.11	E

General Assessment	3.11	E

Legend: 3.26 - 4.00 Highly Effective (HE); 2.51 - 3.25 Effective (E); 1.76 - 2.50 Moderately Effective (ME); 1.00 - 1.75 Not Effective (NE)

The general composite assessment is 3.11 and is interpreted as Effective. The result implies that risk governance defines the way in which the company undertakes risk management.

According to the International Risk Governance Council, risk governance covers all actors, rules, conventions, procedures, and frameworks, and is concerned with how appropriate risk information is gathered, evaluated, and transmitted, and how management decisions are made. Under this definition, organizations are required to explicitly identify how strategic decisions are made.

4. Test of Significant Relationship between the Awareness and Effectiveness Level of Electronics Risk Management Practices of Selected Semiconductor Companies in Laguna.

Table 4

Test of Significant Relationship between the Awareness and Effectiveness Level of Electronics Risk Management Practices of Selected Semiconductor Companies in Laguna

Awareness	Practices	r value	p value	Decision	Remarks
Nature of Risk	Risk Identification	.577**	.000	Reject Ho	Significant
	Risk Assessment	.644**	.000	Reject Ho	Significant
	Risk Treatment	.631**	.000	Reject Ho	Significant
	Risk Policy	.647**	.000	Reject Ho	Significant
	Risk Governance	.693**	.000	Reject Ho	Significant
Risk Vulnerability	Risk Identification	.605**	.000	Reject Ho	Significant
	Risk Assessment	.645**	.000	Reject Ho	Significant
	Risk Treatment	.606**	.000	Reject Ho	Significant
	Risk Policy	.646**	.000	Reject Ho	Significant
	Risk Governance	.661**	.000	Reject Ho	Significant
Risk Management	Risk Identification	.685**	.000	Reject Ho	Significant
	Risk Assessment	.677**	.000	Reject Ho	Significant
	Risk Treatment	.697**	.000	Reject Ho	Significant
	Risk Policy	.756**	.000	Reject Ho	Significant
	Risk Governance	.774**	.000	Reject Ho	Significant

Table 4 shows the significant relationship between the awareness and effectiveness level of Electronics Risk Management Practices of selected semiconductor companies in Laguna as assessed by the respondents. The probability values are all less than the level of significance.05 thus reject the null hypothesis. There is a significant relationship between the awareness and effectiveness level of Electronics Risk Management Practices of the selected semiconductor companies in Laguna. The resulting test implies that the employees' level of awareness perceived by semiconductor companies is very important to determine the effectiveness level of electronics risk management practices. An awareness of risk as the basis for identifying and managing risks has become an increasingly critical dimension of governance for modern organizations. Evidence shows that the presence of strong governance can significantly enhance risk awareness and communication, supporting an enterprise-wide culture of risk management. The correlation values between risk management to risk governance (r=0.774) and risk policy (r=0.756) show high and very high positive correlation results.

5. The proposed program to enhance the awareness and effectiveness of Electronics Risk Management Practices. As an output, an enhancement program was proposed on how to increase awareness of semiconductor employees and maximize the effectiveness of Electronics Risk Management Practices.

IV. CONCLUSIONS AND DIRECTIONS FOR FUTURE USE

Based on the aforementioned findings of the study, the following conclusions have been derived:

Semiconductor employees are aware of the nature of the risk posed by electronics. They are also conscious of the vulnerabilities of electronic risks. In addition, the company is taking measures to minimize both the probability and the consequences of the risk so that the enterprise can better achieve its objectives. The risk itself as well as the risk management differs with the culture, processes, and structures of every organization. However, the risk vulnerability has nothing to do with the classification of the group of respondents.

The company has developed systems and tools for identifying hazards and evaluating any associated risks. The risk policy provides general guidelines for risk management and implementation. Risk governance defines the way in which the company undertakes risk management. The higher the awareness level of ERMP, the higher the effectiveness level of risk management in semiconductor companies in Laguna.

The proposed enhancement program may be utilized by the implementing organizations for them to be guided accordingly with the learning and development needs of employees to maximize risk awareness towards maximum effectiveness of Electronics Risk Management Practices. Future researches may add other program tools that could be widely used by organizations in the semiconductor industry

The Proposed Enhancement Program

KEY RESULT AREA	OBJECTIVES	STRATEGIES/ACTIVITIES	SUCCESS INDICATORS	TIME FRAME	PERSONS INVOLVED
Employees Awareness	Raise level of experience	Simulation/Case Studies/Lessons Learned	Certification of at least 2 subject matter expert related to electronics risk management every quarter	Last month of every quarter	All employees, contractors, Risk consultants, concessionaires, suppliers & OEM onsite supports
	Increase technical skills	Mentorship/Coaching/Training such as Technical /communications/risk management	100% compliance training and 360 ° feedback		
	Increase Knowledge of Risk Management	Risk Identification meetings/status meetings/Hazard identification competitions/games/ incentives	At least 80% Employee engagement on KAIZEN, SGA,Quality and Safety activities		
	Enhance communication skills	Checklist/Questionnaires/ Definitions/signage's/ Adoption of e-learning and social media systems	100% utilization of e-learning , visualization aided tools and 80% on social media platforms		
	Normalize Risk Tolerance	Probability / Impact Matrix / engineering controls / poka yoke solutions	At least 20%-30% normalization of high risk		
Effectiveness of Risk Management Practices	Efficient Governance	Employee Engagement/Participation/ Survey/Transparency	100% employee participation on surveys	Last month of every quarter	All employees, contractors, Risk consultants, concessionaires, suppliers & OEM onsite supports
		Support and allocate resources for the promotion of risk awareness	Available regular budget/resources for promotions of risk		
		Make consistent and effective control, policies, procedures Adopt new technologies/benchmarking	Corporate policies and procedures are always updated and understood by employees		
	Strong Compliance	Continues information/up-to-date knowledge and trainings/	100% compliance training and zero internal findings related to compliance and infraction incidents		
		Monitor Audit Behavior			
		Enforcement of Code of Conduct and sanctions			

	Enterprise-Wide Risk Management	Innovate Incentive programs for Risk Identification, Risk Assessment, and compliance along with training & performance of employees	Zero Major Non-conformities and Less than 10 minor non-conformities during audits		
		Maintain efficient communications to organization in all aspect of information systems, platforms and methodologies	100% compliance training and zero internal findings related to compliance and infraction incidents Less than 2 operation downtime caused by electronics risk		

REFERENCES

[1] Alseiari, K.B. (2015). The Management of Risk Awareness in Relation to Information Technology (MERIT). (Doctoral Dissertation), University of Gloucestershire. Retrieved from http://eprints.glos.ac.uk/2739/ on March 23, 2020.

[2] AS/NZS ISO 31000:2009. Risk Management-Principles and Guidelines. Australian Standards Association/New Zealand Standards Council OB-007. Published November 20, 2009. Sydney, Australia and Wellington, New Zealand. Retrieved from http://www.finance.gov.au/sites/default/files/COV_216905_Risk_Management_Fact_Sheet_FA3_23082010_0.pdf on March 20, 2020.

[3] Cunha, M. & Portela, I. (2015). Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance. Published by Information Science Reference, USA.

[4] Kutsch, E., Browning, T. & Hall, M. (2015). Bridging the Risk Gap: The Failure of Risk Management in Information Systems Projects, Research-Technology Management, 57:2, 26-32, DOI: 10.5437/08956308X5702133.

[5] Priya Sr, F (2018). Benefits and Risk of Automation Testing. Retrieved from https://www.h2kinfosys.com/benefits-risks-automation-testing/ on July 12, 2020.

[6] Renault, B. Y., Agumba, J. N. & Ansary, N. (2016). A Theoretical Review of Risk Identification: Perspective of Construction Industry. 5th Applied Research Conference in Africa. (ARCA) Conference, 773-782, 25-27 August 2016, Cape Coast, Ghana.

[7] Rostami, Ali. (2016). Tools and Techniques in Risk Identification: A Research within SMEs in the UK Construction Industry. Universal Journal of Management 4.4 (2016) 203 - 210. Doi: 10.13189/ujm.2016.040406.

[8] Simota, J., Tupa, J., & Steiner, F. (2017). Risk Management to Enhance Performance in the Construction SME Sector; Theory and Case Study, Risk Management Treatise for Engineering Practitioners, Chike F Oduoza, IntechOpen, DOI:10.5772/intechopen.68798.

[9] Spacey, J. (2016). What is Technology Risk? Retrieved from https://simplicable.com/new/technology-risk-definition on March 23, 2020.

[10] Tchankova, L. (2002) Risk Identification—Basic Stage in Risk Management. Environmental Management and Health, 13, 290-297. http://dx.doi.org/10.1108/09566

[11] Zurkus, K. (2017). Vulnerability vs. risk: Knowing the difference improves security. Retrieved from https://www.csoonline.com/article/3211443/vulnerability-vs-risk-knowing-the difference-improves-security.html on March 23, 2020.