CONCEPCION
INDUSTRIAL CORPORATION

CLASSIFICATION

GENERAL

CIC-ERM-001

CIC ENTERPRISE RISK MANAGEMENT FRAMEWORK

CHANGE / AMMENDMENTS / MODIFICATION HISTORY

Version No.	Date Issued	Change		Author	Approved by
		Section	Particular		
01	June 2019	New document		Jose Marie L. Cariño	Ma. Victoria A. Betita

CONTENTS

1. POLICY INTRODUCTION

CIC Board of Directors and Management consider Risk Management as an integral part of the organization's strategic management. It is the process where CIC addresses the risks on activities related to the business, with the goal of achieving sustained benefit within various processes and across all businesses of CIC.

Risk Management is the culture, processes and structures that are directed towards realizing potential opportunities and managing adverse effects. It is a tool to help Management improve its decision-making process, minimize its losses, as well as maximize its profits. It offers a framework for managing uncertainties, responding to risks, and exploring opportunities as they arise to ensure that value is created, protected, and enhanced.

The purpose of this Framework is to provide reference to CIC leadership, management, and employees on the consistent application and comprehensive methodology of risk management which includes identification, analysis, evaluation and controlling of risks.

This Framework follows the Committee of Sponsoring Organization of the Treadway Commission (COSO) Enterprise Risk Management Framework. It is a continuous and developing process which runs throughout the organization's strategy and its implementation.

2. DEFINITION OF TERMS

Enterprise Risk Management (ERM) – a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

Risk Management – the identification, evaluation, prioritization of risks followed by application of resources to minimize, monitor, and control the probability or impact of unfortunate events, or to maximize the realization of opportunities.

Risk – defined as the possibility that an event will occur, which will impact an organization's achievement of objectives (The Professional Practices Framework 2004/2015).

Opportunities – potential beneficial effect towards the achievement of organization's objectives.

Control – any action effected by an entity's board of directors, management and other personnel, designed to manage risks, and increase the likelihood of achieving established business goals and objectives.

Inherent Risk – level of risk in place in order to achieve an entity's objective and before actions are taken to alter the risk's impact / consequence or likelihood / occurrence.

Residual Risk – remaining level of risk following the development and implementation of entity's response.

Risk Identification – process of finding, recognizing and describing risk, including the identification of risk source, events, cause, and potential impact / consequence and likelihood / occurrence.

Risk Analysis – process of identifying and analyzing potential issues that could negatively impact key business initiatives or critical projects in order to help organizations avoid or mitigate those risks.

3. OBJECTIVES

Risk Management is a responsibility of all CIC employees, with specific risk responsibilities allocated to different groups and levels within the organization. It is important to have complete and current risk information / profile available as this assists management to make more informed decisions around both strategic direction and operational objectives.

The objectives of the CIC ERM Framework are as follows:

a. Provide as a reference for a systematic approach to the early identification and management of risks;

b. Provide consistent risk assessment criteria;

c. Make available, accurate, and concise risk information that will aid towards informed decision and appropriate business direction;

d. Adopt risk treatment strategies that are cost effective and efficient in reducing risk to an acceptable level; and

e. Monitor and review risk levels to ensure that risk exposures remain within an acceptable level across all CIC entities / divisions.

4. BENEFITS

The application of a consistent and comprehensive risk management process will:

a. Increase the likelihood of achieving CIC's strategic and business objectives;

b. Encourage a high standard of accountability across CIC entities / divisions / business units;

c. Support towards more effective decision making through better understanding of risk exposures;

d. Create an environment that enables CIC to deliver timely and quality products and services, and meet performance objectives in an efficient and cost-effective manner;

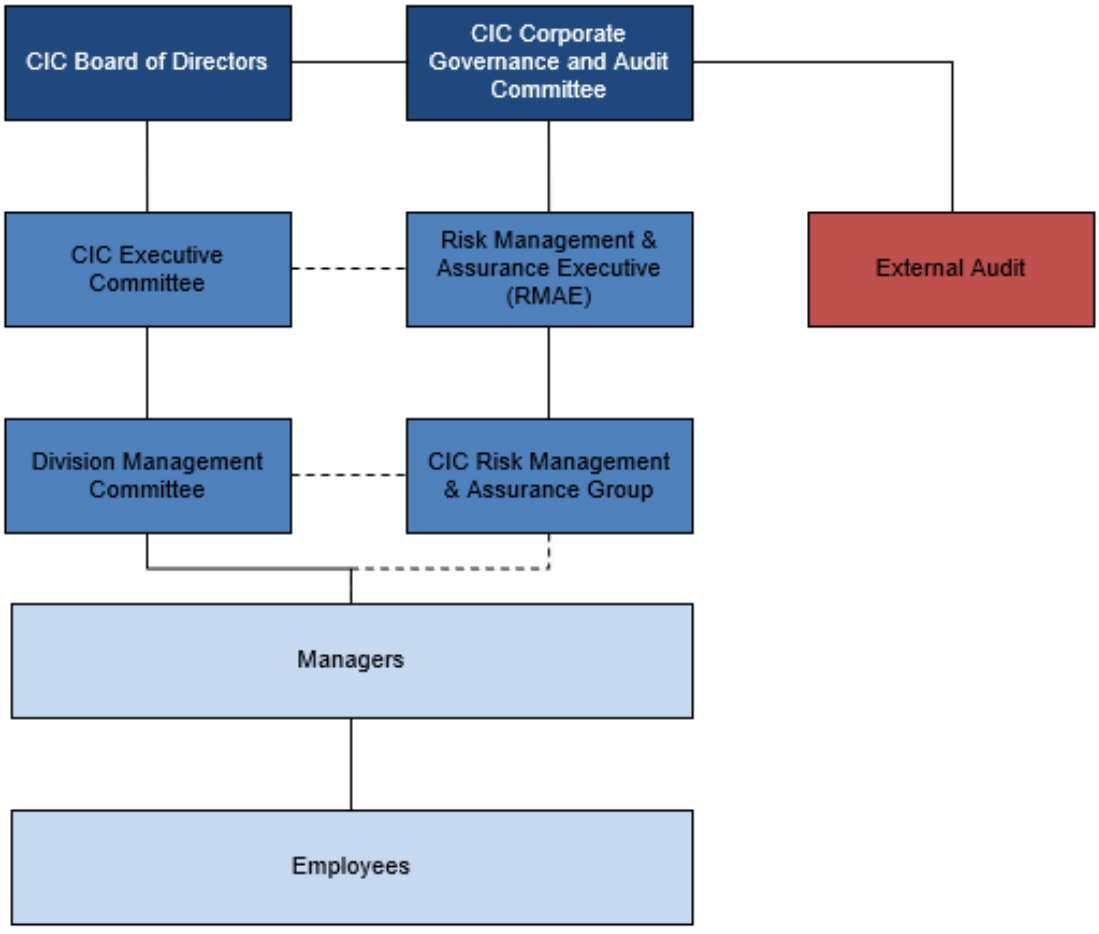
e. Safeguard CIC assets – human, property and reputation; and

f. Meet compliance and governance requirements.

5. ROLES AND RESPONSIBILITIES

CIC's ability to conduct effective risk management is dependent upon having an appropriate risk management structure and well-defined roles and responsibilities. It is important for each CIC employee to be aware of his or her individual and collective risk management responsibilities as it contributes towards well-defined and effective processes, and organizational culture.

Below is CIC's ERM Governance Structure. It illustrates that risk management function is not a sole responsibility of one individual, but are rather inherent and supported at all organizational levels.



CIC Board of Directors

The Board has the ultimate responsibility for over-seeing the performance of CIC including monitoring of risk management and internal control systems. To assist in discharging its responsibilities, the Board has established the CIC Executive Committee and the CIC Corporate Governance and Audit Committee which will aid in the implementation and oversight of controls and associated risks, respectively, toward the fulfillment of CIC's goals and business objectives.

CIC Executive Committee (CIC Excom)

The Chief Executive Officer (CEO), CIC Division Presidents, Chief Finance Officers (CFO), Chief Information Officer (CIO), and Chief Human Resources Officer (CHRO) collectively known as the CIC Executive Committee, together with the CIC Board of Directors created an environment for ERM to operate effectively and, at the same time, ensure that significant internal and external factors, including stakeholder interests, are considered in defining Risk Tolerance levels. The members of the CIC Excom act as:

a. The comprehensive Risk Executive of their respective Divisions and/or Functions.

b. The ultimate Accountable persons for risk management priorities, tolerance, policies, and strategies.

c. The Enforcer of risk management.

CIC Corporate Governance and Audit Committee

The CIC Corporate Governance and Audit Committee will assist the Board in the review of risks, risk management process, and significant risk facing CIC and its entities / divisions.

Moreover, the responsibility of CIC Corporate Governance and Audit Committee are as follows:

a. Review and approve CIC's ERM Framework for identification, assessment, monitoring and management of risks;

b. Regular review of the updated risk profile of CIC and its entities / divisions; and

c. Review (at least annually) CIC's implementation of the ERM Framework.

Risk Management & Assurance Executive (RMAE) and CIC Risk Management & Assurance Group (RMA)

The CIC RMA Group, led by the RMAE, will support CIC in performing its responsibility in institutionalizing a sustainable risk management process within the organization.

The overall responsibility of the CIC RMA Group are as follows:

a. Review, validate and confirm risk issues generated by Risk Management & Assurance Group;

b. Recommends risk management tolerances to the CIC Corporate Governance and Audit Committee;

c. Evaluates measurement methodologies;

d. Develop risk management policy, strategies, and initiatives for the approval of CIC Corporate Governance and Audit Committee;

e. Develop risk appetite strategy;

f. Develops and implement systems, policies, and procedures on the identification, collection, assessment, analysis and mitigation of risks;

g. Oversee the implementation of risk management strategies and initiatives in compliance with established risk appetite;

h. Assign owners of significant risk;

i. Determine risk management tools and training requirements of the CIC RMA Group and employees; and

j. Evaluates effectiveness of risk governance infrastructure for managing specific risks.

The CIC RMA Group likewise provides assurance to CIC Corporate Governance and Audit Committee on the appropriateness of the implementation of risk management strategies, and the effectiveness of risk management processes, methodologies, and internal controls.

In its audit function, CIC RMA is more specifically responsible for:

a. Development and implementation of CIC Internal audit plan following a risk-based audit approach.

b. Review of the effectiveness of risk management policy and processes.

c. Notification of new and emerging risks identified in the course of implementing the CIC Internal plan, and whenever necessary, modifying the plan to take account the impact of new risks.

d. Reporting to the CIC Corporate Governance and Audit Committee all relevant risks and compliance issues.

Division Management Committee

The Division Management Committees (per CIC Division and/or entity) has the overall responsibility for enterprise risk management at the enterprise level and business process level. They are in support to CIC Excom in the effective implementation of risk management across CIC. The Division Management Committees will be represented by various Division and Business Unit Heads responsible on various risk areas / concerns within the entity / division.

Managers

Operating and Line Managers are responsible for conducting a periodic risk assessment in their area of operations using the tools and methodology provided by CIC ERM Framework. Among other things, they are responsible for the following:

a. Supporting the risk culture of the organization / division / business unit;

b. Identification, communication and management of risks in their area of operations;

c. Managing risks on daily operations.

Employees

All CIC Employees must comply with the company's policies and procedures. They are responsible for:

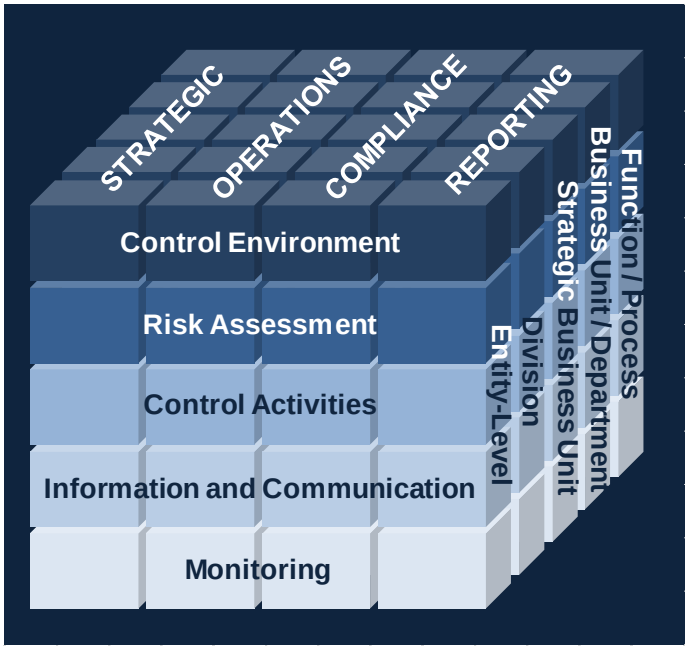
a. Identifying and reporting to appropriate level of authority new or emerging risks in their respective area of responsibilities that may affect CIC and its divisions' operations.

b. Report any real or perceived risk that CIC and its divisions' operations may impact on environment and / or community.

c. Identify opportunities to improve on operational efficiencies and optimize outcomes.

6. FRAMEWORK

Risk Management is a continual process that involves review and update of risk profiles of the enterprise at the entity, division, strategic business unit, business unit, and function / process levels. The scope of risk areas transcends from strategic, operations, compliance and reporting. CIC's ERM Framework is patterned from COSO's ERM Cube (Internal Control Integrated Framework).



The cube illustrates the link between: 1st dimension – Business objectives (Strategic, Operations, Compliance, and Reporting); 2nd dimension – Enterprise risk management Components (acceptable system of internal control) (Control environment, Risk assessment, Control activities, Information and Communication, and Monitoring); and 3rd dimension – Levels in the organization.

There is a direct relationship between business objectives, which are what an entity strives to achieve, the enterprise risk management components, which represent what is needed to achieve them, and the levels in the organization, which portrays the ability to focus on an entirety of CIC's enterprise risk management, or by objective category, component, entity, division, or other means.

Business Objectives

CIC ERM Framework is geared towards the achievement and realization of its goals and objectives as set forth in the following categories:

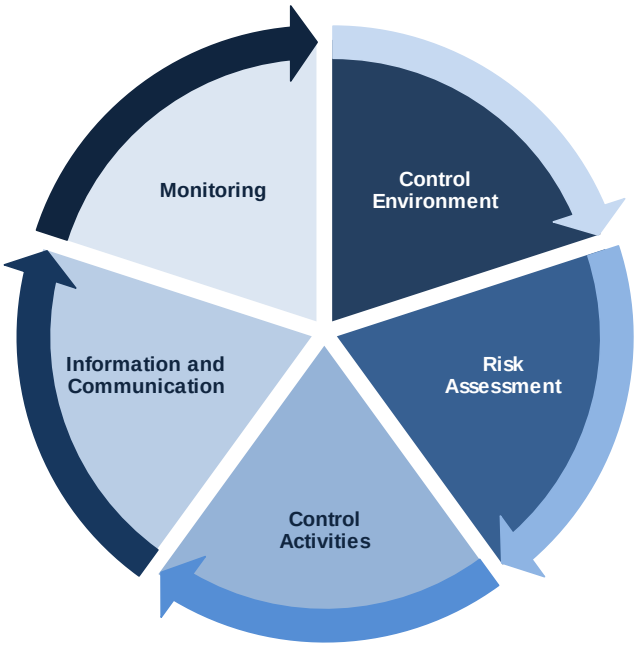
a. ***Strategic*** – high level goals, aligned with and supporting CIC's mission, vision and core values.

b. ***Operations*** – effective and efficient use of resources.

c. ***Compliance*** – compliance with applicable laws and regulations.

d. ***Reporting*** – reliability of financial reporting.

Components of Enterprise Risk Management



The CIC ERM Framework consists of five interrelated ERM components. These are derived form the way management runs an enterprise and are integrated with the management process.

a. ***Control environment*** – is the set of standards, processes and structures that provide the basis for carrying out internal control across CIC organization. The board of directors and senior management establish the tone at the top regarding the importance of internal control and expected standards of conduct. It consists of:

   1. *Internal Environment* – encompasses the tone of CIC organization, and sets the basis for how risk is viewed and addressed by CIC employees, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.

   2. *Objective Setting* – Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite.

At this phase, the following are defined by the CIC Excom and and/or Division Mancoms.

Risk Universe – is the full range of risks which could impact, either positively or negatively, on the ability of the organization to achieve its long-term objectives.

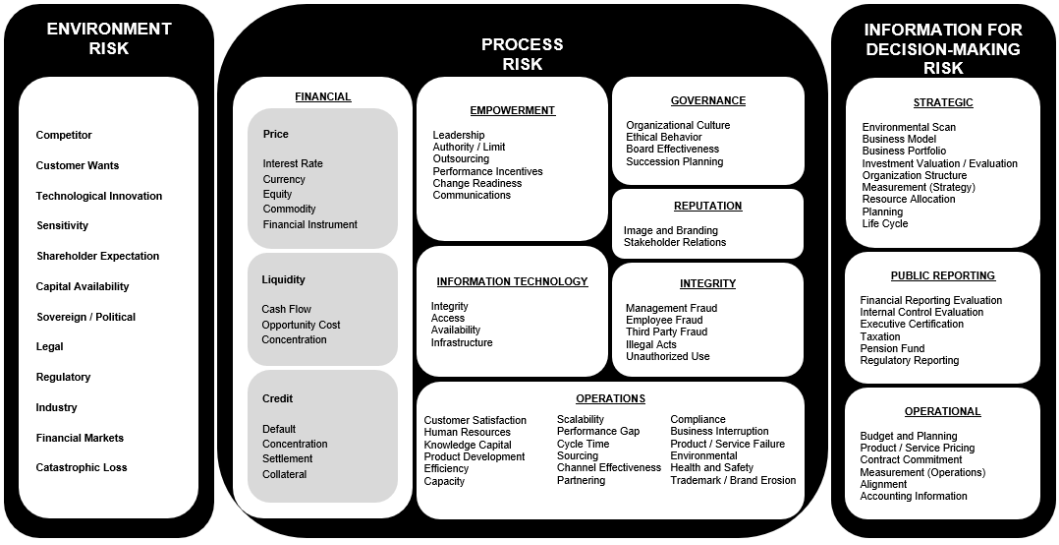
Risk Profile – the broad parameters an organization considers in executing its business strategy in its chosen market space. It outlines and provide guidance on the types of risks an organization is exposed to.

Risk Appetite – is the amount of risk that an organization is willing to seek or accept in the pursuit of its long-term objectives.

Risk Tolerance – acceptable levels of risks an organization is willing and able to keep in the execution of its business strategies

b. ***Risk Assessment*** – involves a dynamic and iterative process for identifying and analyzing risks to achieving the entity's objectives, forming a basis for determining how risk should be managed. Management considers possible changes in the external environment and within its own business model that may impede its ability to achieve its objectives. It consists of:

1. *Event Identification* – internal and external events affecting the achievement of CIC's objectives must be identified, distinguished between risks and opportunities. Opportunities are channeled back to management's strategy or objective setting process. For common risk language, it is suggested that CIC entities and divisions use the CIC Risk Model as adopted from Protiviti Risk Model [SM].



As shown in the table, risks are generally classified as follows:

1. *Environment Risks* – are risks arising from external forces that can affect the viability of CIC's business model, and CIC's performance including fundamentals that drive the overall objectives and strategies that define the model. These forces are generally outside management's ability to control.
2. *Process Risks* – are risks that business processes within CIC are not clearly defined, poorly aligned with business objectives and strategies, do not satisfy customer needs, dilute shareholders value, or expose assets and resources to misappropriation or misuse.
3. *Information for Decision-making Risks* – are risks that information used to support, strategic, operation and financial decisions is not relevant or reliable. This risk relates to the usability and timeliness of information that is either created or summarized by processes and application systems or a failure to understand information needs.

Definition of each specific classification of risks are provided in *Appendix A* of this framework.

Risks are analyzed, considering the risk impact / consequence and risk likelihood / occurrence, as a basis for determining how they should be managed. Risks are assessed on an inherent and residual basis. For common risk assessment methodology, it is suggested that CIC entities and divisions use the CIC Risk Assessment Matrix.

1. *Inherent Risk* – is the level of risk in place in order to achieve and entity's objective before actions are taken to alter the risk impact / consequence or likelihood or occurrence. Inherent risk is derived from the following:
   a. *Risk Occurrence / Likelihood* – this pertains to the degree of probability, within which risk is expected to occur or has occurred in the business. Risk occurrence / likelihood are rated as follows:

Assessment	Score	Definition
Almost Certain / Imminent	**5**	1. Expected to occur in most circumstances and has occurred several times; 2. >90% possibility of occurrence; 3. Has occurred in >90% of the time.
Likely / Probable / Frequent	**4**	1. Very likely to occur and has occurred several times; 2. >60% to 90% possibility of occurrence. 3. Has occurred in >60% to 90% of the time.
Possible / Occasional	**3**	1. Might occur sometime or has occurred in the business / operations; 2. >40% to 60% possibility of occurrence. 3. Has occurred in >40% to 60% of the time.

Unlikely / Infrequent	**2**	1. Could occur and has occurred in the industry to which the Company belongs; 2. 10% to 40% possibility of occurrence. 3. Has occurred in 10% to 40% of the time.
Remote / Rare	**1**	1. May occur only in exceptional circumstances and has never occurred in the industry; 2. <10% possibility of occurrence. 3. Had occurred ,10% of the time.

b. *Risk Impact / Consequence* – this refers to the level of consequence the risk might have upon or have affected the business. Risk impact / consequence are rated as follows:

Assessment	Score	Definition
Catastrophic / Critical	**5**	1. Significant impact on cash flow, assets and/or liabilities of the entity/division. 2. Sustained, serious loss on the company image/reputation 3. Business closure; Top management changes
Major / Severe	**4**	1. Material impact on cash flow, assets and/or liabilities. 2. Serious impact on company image/reputation over a long term. 3. Major censure which impacts customer activities and opportunities.
Moderate	**3**	1. Immaterial impact on cash flow, assets and/or liabilities. 2. Adverse impact on company image/reputation over a short term. 3. Major penalties and increased on going regulatory scrutiny.
Minor	**2**	1. Insignificant on impact cash flows, asset and/or liabilities. 2. Minimal impact on company image/reputation. 3. Minimal penalties and increased regulatory scrutiny.
Insignificant	**1**	1. No impact on cash flows, asset and/or liabilities. 2. No effect on company image/reputation. 3. Minor admonition or penalties.

Following the Risk Assessment Matrix, below will be the result of inherent risk assessment:

		Inherent Risk Rating				
Risk Likelihood / Occurrence	**Almost Certain / Imminent**	Moderate	High	Critical	Critical	Critical
	Likely / Probable / Frequent	Low	Moderate	High	Critical	Critical
	Possible / Occasional	Very Low	Low	Moderate	High	Critical
	Unlikely / Infrequent	Very Low	Very Low	Low	Moderate	High
	Remote / Rare	Very Low	Very Low	Very Low	Low	Moderate
		Insignificant	**Minor**	**Moderate**	**Major / Severe**	**Catastrophic / Critical**
		Risk Impact / Consequence				

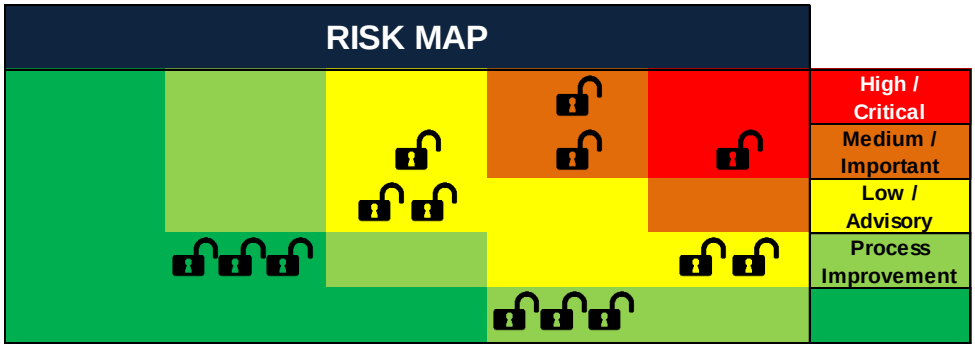
c. *Control Effectiveness* – this refers to the level of control effectiveness present to manage risks in the business. Inherent risk is affected by the degree of control effectiveness instituted in the organization. As control become effective, residual risk for the organization is lessened. Control effectiveness are rated as follows:

Assessment	Score	Definition
No Control	**5**	1. No Control(s) instituted. 2. Poses risk in any/all of the Business objectives/areas - Strategic, Operations, Compliance and Reporting.
Weak	**4**	1. Control(s) is/are not implemented as designed. 2. Poses risk in any of the Business objectives/areas - Strategic, Operations, Compliance and Reporting.
Inadequate	**3**	1. Control(s) is/are implemented but not formalized. 2. Poses risk in any of the Business objectives/areas - Strategic, Operations, Compliance and Reporting.
Adequate	**2**	Control(s) is/are adequate, implemented, and sufficient to manage risk(s) in any of the Business objectives/areas - Strategic, Operations, Compliance and Reporting.
Strong	**1**	Control(s) is/are adequate, implemented, and sufficient to manage risk(s) in all of the Business objectives/areas - Strategic, Operations, Compliance and Reporting.

2. *Residual Risk* – is the remaining level of risk resulting from the development and implementation of entity's response. Following the Risk Assessment Matrix, below will be the result of residual risk assessment:

		Residual Risk Rating				
Inherent Risk Rating	**Critical**	-	Process Improvement	Low / Advisory	Medium / Important	High / Critical
	High	-	Process Improvement	Low / Advisory	Medium / Important	High / Critical
	Moderate	-	Process Improvement	Low / Advisory	Low / Advisory	Medium / Important
	Low	-	-	Process Improvement	Low / Advisory	Low / Advisory
	Very Low	-	-	-	Process Improvement	Process Improvement
		Strong	**Adequate**	**Inadequate**	**Weak**	**No control**
		Control Effectiveness				

After each potential risk event are measured, those involved in the conduct of risk assessment process shall plot those risks in a Risk Heat Map. This will aid management in visualizing impact of various risks to one another, and will be used as basis for assessing and addressing such risks in accordance to their potential impact to the business. The need to prioritize risks is towards determination of important and critical to the organization towards the attainment of defined business goals are objectives.



For purposes of prioritization, risks are classified as follows:

a. RED – High / Critical Risks; as primary risks, these are of highest priority to be addressed; Urgent and Important.

b. ORANGE – Medium / Important Risks; secondary risks, these are next priority to be addressed; Urgent and / or Important.

c. YELLOW – Low / Advisory Risks; although not urgent and / or important, may cause elevated concern in the long term.

d. LIGHT GREEN – Process Improvement Opportunity; these are areas in which further improvement in the business is recommended (e.g., process efficiencies and effective of operations).

e. GREEN – No risk concern.

2. *Risk Response* – Management selects appropriate risk responses – Avoid (Terminate), Reduce (Treat), Share (Transfer) or Accept (Take) – developing set of actions to align risk within CIC's risk tolerance and risk appetite.

   a. *Avoid (Terminate)* – Change business process or objective so as to avoid the risk *(e.g., eliminate, prohibit, divest, etc.)*.

   b. *Reduce (Treat)* – Undertake actions aimed at reducing the cause and impact of risk *(e.g., process or control improvement, reorganization, redesign, etc.)*.

c. *Share (Transfer)* – Transfer risk of ownership and liability to a 3rd party *(e.g., insurance, outsourcing, hedging, etc.)*.

d. *Accept (Take)* – Do nothing, retain the risk and accept impact / consequence of the risk (e.g., self-insure).

When determining the preferred risk option, consideration should be given to the cost of risk treatment as compared to the likely risk reduction that will result (Cost benefit analysis). On selecting the risk option:

a. Cost of any actions should be incorporated into the relevant budget planning process;

b. Responsible person should be identified for delivery of the action, with this expectation being communicated to them;

c. A realistic due date should be set; and

d. Performance measures should be determined.

Risk response also involves:

a. Identifying controls currently in place to manage the risk by either reducing the consequence or likelihood of the risk;

b. Assessing the effectiveness of current control;

c. Identifying the likelihood of the risk occurrence; and

d. Identifying the potential impact or consequence that would result if the risk was to occur.

At this phase, the Risk Portfolio and Risk Map are co-developed by Division Management Committee, and Managers in consultation and with the assistance of RMAE and CIC RMA Group.

c. ***Control Activities*** – are the actions established by the policies and procedures to help ensure that management directives to mitigate risks to the achievement of objectives are carried out. Control activities are performed at all levels of the entity, at various stages within business processes, and over the technology environment. They may be preventive or detective in nature and may encompass a range of manual or automated activities such as authorizations and approvals, verifications, reconciliations, and business performance reviews. Segregation of duties is typically built into the selection and development of control activities. Where segregation of duties is not practical, management selects and develops alternative control activities. Controls are aimed at bringing the risks within acceptable levels. The evaluation of current controls can occur through several different processes including:

1. Process / Performance Review;
2. Control Self-Assessment;
3. Internal Audit; and
4. External Audit

At this phase, the Risks and Controls Matrix (RCM) are documented / updated to document corresponding controls in the management of risks. This is managed by the CIC RMA Group.

d. ***Information and Communication*** – Information is necessary for the entity to carry out internal control responsibilities in support of achievement of its objectives. Communication occurs both internally and externally and provides the organization with the information needed to carry out day-to-day internal control activities. Communication enables personnel to understand internal control responsibilities and their importance to the achievement of objectives. The risk management reporting process supports a formalized, structured, and comprehensive approach of the company to monitor and review its risks, thereby enhancing the entire enterprise risk management process.

e. ***Monitoring*** – Ongoing evaluations, separate evaluations, or some combination of the two are used to ascertain whether each of the five components of internal control, including controls to apply the principles within each component, are present and functioning. Findings are evaluated and deficiencies are communicated in a timely manner, with serious matters reported to senior management and to the board. The effectiveness of enterprise risk management framework as applied in CIC and its entities and divisions is also monitored and reviewed.

7. RELATIONSHIP WITH OTHER PROCESSES

Risk Management is not a stand-alone discipline. In order to maximize its benefits and opportunities, it needs to be integrated with existing business processes. Some of the key business processes with which risk alignment is necessary are:

a. Business planning (including budget)

Identifying risk during business planning process allows to set realistic delivery timelines for strategies / activities or to choose to remove a strategy / activity if associated risks are too high or unmanageable.

b. Performance Management

All risk responsibilities, whether a general responsibility to use the risk management process or specific responsibilities such as risk ownership or implementation of risk treatments should be included within the relevant individual / group's performance plans as Key performance indicators (KPIs) or Key result area (KRAs).

c. Internal Audit

Internal Audit reviews the effectiveness of internal controls. Alignment between the Internal Audit function and that of the controls within Risk Management process is critical. With risk management in place, Internal Audit will be able to optimize its operations through focused reviews of business activities or processes that are most important to the organization, or where critical risks exists or could occur.

8. RISKS AND CONTROLS MATRIX (RCM)

The RCM is a tool for documenting risks, and actions to manage each risk. RCM is essential to the successful management of risk. This is the live documentation and culmination of all enterprise risk management processes and activities performed.

RCM contains all the risks identified and summarizes or documents the results of the assessment performed including management actions to be undertaken to further mitigate the risks to an acceptable level. It also includes information as to whom (Risk Owner) specific risks are assigned and responsible for its mitigation. Among the details / information that should be included in the Register are as follows:

a. Entity, Division, Area, Process, Activity or Project with which risk is associated

b. Business objectives / goals to be achieved

c. Risk description

d. Business risk category

e. Business objective category

f. Risk reference

g. Assessment score for risk likelihood / occurrence

h. Assessment score for risk impact / consequence

i. Overall risk assessment

j. Value at risk or significance

k. Existing controls that mitigate the risks

l. Residual risk after existing controls

m. Future or action plan to further improve mitigation controls including timeline, responsible person, and status.

The Register shall be accomplished by each of the CIC entities / divisions, aligned with the requirements set forth in this Framework. This should be made available during annual risk review process, unless otherwise specifically requested by the CIC Board of Directors, CIC Corporate Governance and Audit Committee or CIC Executive Committee.

9. ERM FRAMEWORK ADMINISTRATION

The CIC ERM Framework will be administered by the Risk Management & Assurance Executive. The Framework shall be reviewed annually and revised as necessary. Changes to the Framework shall require approval from CIC Board of Directors and CIC Corporate Governance and Audit Committee.

APPENDIX A – Definition of CIC Risks

I	**Environment Risk** Environment risks arises from external forces that can affect the viability of CIC's business model, and CIC's performance including fundamentals that drive the overall objectives and strategies that define the model. These forces are generally outside management's ability to control.		
	A	**Competitor Risk**	Major competitors or new entrants to the market take actions to establish and sustain competitive advantage over the company or even threaten its ability to survive.
	B	**Customer Wants Risk**	The company is not aware that customer needs and wants change. Such needs and wants may apply to desired quality, willingness to pay and/or speed of execution.
	C	**Technology Innovation Risk**	The organization is not leveraging advancements in technology in its business model to achieve or sustain competitive advantage or is exposed to the actions of competitors or substitutes that do leverage technology to attain superior quality, cost and/or time performance in their products, services, and processes.
	D	**Sensitivity Risk**	Sensitivity risk results when management commits the company's resources and expected cash flows from future operations to such an extent that it reduces the company's tolerance for (or ability to withstand) changes in environmental forces that are totally beyond its control.
	E	**Shareholder Expectations Risk**	The risk of failing to manage shareholder expectations, resulting in a decline in investor confidence that may impair the company's ability to efficiently raise capital and reduce stock evaluations over time.
	F	**Capital Availability Risk**	The company does not have efficient access to the capital it needs to fuel its growth, execute its strategies, and generate future financial returns.
	G	**Sovereign / Political Risk**	The risk of adverse consequences through political actions in a country in which a company has made significant investments (a major project, for example), is dependent on a significant volume of business or has entered into an agreement with a counter party subject to the laws of that country.
	H	**Legal Risk**	The risk that a company's transactions, contractual agreements and specific strategies and activities are not enforceable under applicable law.
	I	**Regulatory Risk**	Changes in regulations and actions by national or local regulators can result in increased competitive pressures and significantly affect a company's ability to efficiently conduct business.

	J	**Industry Risk**		The risk that the industry will lose its attractiveness due to changes in the key factors for competitive success within the industry, capabilities of existing and potential competitors, and company's strengths and weaknesses relative to competitors.
	K	**Financial Markets Risk**		Financial markets risk is defined as exposure to changes in the earnings capacity or economic value of the firm as a result of changes in financial market variables (e.g., currency rates). These changes affect income, expense or balance sheet values.
	L	**Catastrophic Loss Risk**		The inability to sustain operations, provide essential products and services, or recover operating costs as a result of a major disaster.
II	**Process Risk** The risk that business processes are not clearly defined, are poorly aligned with business objectives and strategies, do not satisfy customer needs, dilute shareholder wealth, or expose assets to misappropriation or misuse.			
	A	**Financial Risk**		Financial risk can occur if the company fails to provide adequate liquidity to meet the firm's obligations or manages financial risks in a manner that is inconsistent with the firm's business objectives. Its severity depends on a number of factors, which include the firm's size, industry, financial position (e.g. public / private, leverage, free cash flow to equity, etc.), and the direction of the market as a whole.
		1 **Price Risk**		The exposure of earnings or net worth to changes in market factors (e.g., interest rates, currency rates), which affect income, expense or balance sheet values.
			a **Interest Rate Risk**	The risk that interest rates deviate from their expected value resulting in lower-than- expected investment yields, higher-than-expected borrowing or product costs, or deterioration of the firm's competitive position in its industry.
			b **Currency Risk**	The exposure to fluctuations in exchange rates may arise as a result of business activity in foreign markets and investment in securities, which are issued by overseas entities or are denominated in a foreign currency.
			c **Equity Risk**	The exposure to fluctuations in the income stream and/or value of equity ownership in an incorporated entity.

			d	**Commodity Risk**	This can be a financial market risk if a company chooses an investment as part of a diversification strategy for managing investment risk. From the industrial perspective, commodity risk is the exposure to fluctuations in prices of commodity-based materials or products (e.g., gold, energy, copper, coffee and etc.).
			e	**Financial Instrument Risk**	Financial market risk can vary depending upon the particular segment of the market to which the holder of a financial instrument is exposed, or the way in which the exposure is structured.
		2	**Liquidity Risk**		The exposure to loss as a result of the inability to meet cash flow obligations in a timely and cost-effective manner. Liquidity risk often arises as a result of an investment portfolio with a cash flow and / or maturity profile, which differs from the underlying cash flows dictated by the company's operating requirements and other obligations.
			a	**Cash flow Risk**	Actual losses incurred as a result of the inability to fund the operational or financial obligations of the business.
			b	**Opportunity Cost Risk**	The use of funds in a manner that leads to the loss of economic value, including time value losses, transaction costs due to inappropriate or inefficient management of cash flows and other causes of loss of value.
			c	**Concentration Risk**	Exposure to loss as a result of the inability to access cash in a timely manner due to the inability to liquidate exposures without moving the market, unusual market conditions, use of “proprietary” financial products, or excessive reliance on a small number of funding sources.
		3	**Credit Risk**		The exposure to actual loss or opportunity cost as a result of default (or other failure to perform) by an economic or legal entity (the debtor) with which the company does business.
			a	**Default Risk**	A counterparty will be unable to fulfill its obligations.
			b	**Concentration Risk**	Inappropriate emphasis of sales volume or revenues on a single customer, industry sector, or other economic segment leads to exposure to excessive loss.
			c	**Settlement Risk**	In financial terms, this risk arises when financial counterparties effect their payments to each other at different times or in different locations. In a non-financial context, settlement risk describes the risk of unexpected costs and / or administrative inconvenience associated with the failure to deliver payment in the right place at the right time.

			d	**Collateral Risk**	This is the risk that the value of an asset provided as collateral for a loan, receivable, or commitment to perform may be partially or totally lost.
	B	**Empowerment Risk**			The risk that managers and employees are not properly lead, do not know what to do (or how to do it) when they need to do it, exceed the boundaries of their defined authorities, do not have the resources, training and tools necessary to make effective decisions or are given incentives to do the wrong thing.
		1	**Leadership Risk**		The risk that the people responsible for the important business processes do not or cannot provide the leadership, vision, and support necessary to help employees be effective and successful in their job.
		2	**Authority / Limit Risk**		The risk that people either make decisions or take actions that are not within their explicit responsibility or control or fail to take responsibility for those things for which they are accountable. Failure to establish or enforce limits on personnel actions may cause employees to commit unauthorized, illegal or unethical acts or assume unauthorized or unacceptable business risks.
		3	**Outsourcing Risk**		Outside service providers do not act within their defined limits of authority and do not perform in a manner consistent with the values, strategies and objectives of the company.
		4	**Performance Incentive Risk**		Unrealistic, subjective or unclear performance measures may cause managers and employees to act in a manner that is inconsistent with the company's business objectives, strategies, ethical standards and prudent business practice.
		5	**Change Readiness Risk**		The people within the organization are unable to implement process and product/service improvements quickly enough to keep pace with changes in the marketplace.
		6	**Communications Risk**		Communication channels (top-down and bottom-up or cross-functional) within the organization are ineffective and result in messages that are inconsistent with authorized responsibilities or established measures.

	C	**Information Technology Risk**		The risk that the information technologies used in the business are not efficiently and effectively supporting the current and future needs of the business or threaten the company's ability to sustain the operation of critical business processes.
		1	**Integrity Risk**	The risk that the information technologies used in the business are not efficiently and effectively supporting the current and future needs of the business or threaten the company's ability to sustain the operation of critical business processes.
		2	**Access Risk**	Access risk includes the risk that access to information (data or programs) or systems will be inappropriately granted or refused. It encompasses the risks of improper segregation of duties, risks associated with the integrity of data and databases and risks associated with information confidentiality.
		3	**Availability Risk**	The risk that information will not be available when needed. This includes risks such as loss of communications (e.g., cut cables, telephone system outage, satellite loss and etc.), loss of basic processing capability (e.g., fire, flood, electrical outage) and operational difficulties (e.g., disk drive breakdown, operator errors).
		4	**Infrastructure Risk**	The risk that the organization does not have an effective information technology infrastructure (e.g., hardware, networks, software, people and processes) to effectively support the current and future needs of the business in an efficient, cost-effective and well-controlled fashion.
	D	**Governance Risk**		The risk that the organization's governance processes do not comply with legal requirements or stakeholder expectations and that the board of directors fails to provide adequate monitoring and oversight of executive management activities.
		1	**Organizational Culture Risk**	The organization's culture does not encourage managers to realistically portray the potential outcomes of transactions, deals, investments and projects and understand and portray the full picture for decision makers. The organization experiences dysfunctional behavior because managers are either risk averse or incented to take risks beyond the organization's risk appetite.
		2	**Ethical Behavior Risk**	The organization, through its actions or inaction, demonstrates that it is not committed to ethical and responsible business behavior.
		3	**Board Effectiveness Risk**	The board does not constructively engage management and provide anticipatory, proactive and interactive oversight of the company's activities and

				affairs, with integrity, vision, common sense and unquestioned independence.
		4	**Succession Planning**	Leadership talent within the organization is not sufficiently developed to provide for orderly succession in the future.
	E	**Reputation Risk**		The risk of loss of brand image such that the company will be unable to operate in the marketplace.
		1	**Image and Branding Risk**	The risk that a company may lose customers, key employees or its ability to compete, due to perceptions that it does not deal fairly with customers, suppliers and stakeholders, or know how to manage its business.
		2	**Stakeholder Relations Risk**	A decline in investor confidence may impair a company's ability to efficiently raise capital. The company will not have the same efficient access as competitors to the capital it needs to fuel its growth, execute its strategies, and generate future financial returns.
	F	**Integrity Risk**		The risk of management fraud, employee fraud, and illegal and unauthorized acts, any or all of which could lead to reputation degradation in the marketplace or even financial loss.
		1	**Management Fraud Risk**	Management issues misleading financial statements with intent to deceive the investing public and the external auditor or engages in bribes, kickbacks, influence payments and other schemes for the benefit of the company.
		2	**Employee Fraud Risk**	Fraudulent activities perpetrated by employees, customers, suppliers, agents, brokers or third-party administrators against the organization for personal gain expose the organization to financial loss.
		3	**Third Party Fraud Risk**	Managers and employees individually or in collusion commit illegal acts, placing the company, its directors and officers at risk to the consequences of their actions.
		4	**Illegal Acts Risk**	The company's employees (or others) use its physical and financial assets for unauthorized or unethical purposes.
	G	**Operations Risk**		The risk that operations are inefficient and ineffective in satisfying customers and achieving the company's quality cost and time objectives.
		1	**Customer Satisfaction Risk**	The company's processes do not consistently meet or exceed customer expectations due to a lack of focus on the customer.
		2	**Human Resources Risk**	The personnel responsible for managing and controlling an organization or a business process do

				not possess the requisite knowledge, skills and experience needed to ensure that critical business objectives are achieved and significant business risks are reduced to an acceptable level.
		3	**Knowledge Capital Risk**	Processes for capturing and institutionalizing learning across the organization are either nonexistent or ineffective, resulting in slow response time, high costs, repeated mistakes, slow competence development, constraints on growth and unmotivated employees.
		4	**Product Development Risk**	The productivity of the product development process is significantly less than more innovative competitors who are able to achieve higher productivity through a stronger customer focus, concentrating focused resources and faster cycle time.
		5	**Efficiency Risk**	The process is inefficient in satisfying valid customer requirements resulting in higher than competitive costs.
		6	**Capacity Risk**	The effective productive capacity of the plant is not fully utilized, resulting in spreading fixed costs over fewer units and creating higher unit costs and lower unit margins or the capacity does not fulfill customer needs resulting in a loss of business.
		7	**Scalability Risk**	The inability to operate differently and more efficiently at larger volumes or amortize costs over greater sales volume, resulting in diseconomies of scale that threaten the firm's ability to generate competitive profit margins.
		8	**Performance Gap Risk**	A business process does not perform at a world-class level because the practices designed into the process are inferior.
		9	**Cycle Time Risk**	Elapsed time between the start and completion of a business process (or activity within a process) is too long because of redundant, unnecessary and irrelevant steps.
		10	**Sourcing Risk**	The fewer the alternative sources of energy, metals and other key commodities and raw materials used in a company's operations, the greater the risks of shortages and higher costs. These risks can significantly affect the company's capability to provide competitively priced products and services to customers at the time they are wanted.
		11	**Channel Effectiveness Risk**	Poorly performing or positioned distribution channels threaten the organization's capacity to access current and potential customers/end users effectively and efficiently.
		12	**Partnering Risk**	Inefficient or ineffective alliance, joint venture, affiliate and other external relationships affect the

				organization's capability to compete. These uncertainties arise due to choosing the wrong partner, poor execution, receiving more value than is given (ultimately resulting in loss of a partner) and failing to capitalize on partnering opportunities.
		13	**Compliance Risk**	As a result of a flaw in design or operation or due to human error, oversight or indifference, the company's processes do not meet customer requirements the first time or do not comply with prescribed procedures and policies. Compliance risk can also result in failure to conform with laws and regulations at the international, country, state and local level that apply to a business process.
		14	**Business Interruption Risk**	The company's capability to continue critical operations and processes may be highly dependent on availability of certain raw materials, information technologies, skilled labor and other resources.
		15	**Product / Service Failure Risk**	The company's operations create risk of customers receiving faulty or nonperforming products or services.
		16	**Environmental Risk**	Environmental risks expose companies to potentially enormous liabilities. The exposure is twofold -- (1) liability to third parties for bodily injury or property damage caused by the pollution, and (2) liability to governments or third parties for the cost of removing pollutants plus severe punitive damages.
		17	**Health and Safety Risk**	These risks expose a company to potentially significant workers' compensation liabilities, financial loss, and negative publicity. Firms and their managers could find themselves criminally liable for failure to provide a safe working environment for their employees.
		18	**Trademark / Brand Erosion Risk**	The risk that a trademark or brand will lose its value. A trademark is a word, symbol or device (or any combination of these) that identifies a product or service and distinguishes that product or service from the products or services of competitors.
III	**Information for Decision-Making Risk** The risk that information used to support strategic, operational and financial decisions is not relevant or reliable. This risk relates to the usability and timeliness of information that is either created or summarized by processes and application systems or a failure to understand information needs.			
	A	**Strategic Risk**		
		1	**Environmental Scan Risk**	The failure to monitor and stay in touch with a rapidly changing environment resulting in obsolete business strategies.
		2	**Business Model Risk**	The organization has an obsolete business model and doesn't recognize it and / or lacks the information

				needed to make an up-to-date assessment of its current model and build a compelling business case for modifying that model on a timely basis.
		3	**Business Portfolio Risk**	The risk that a firm will not maximize business performance by effectively prioritizing its products or balancing its businesses in a strategic context.
		4	**Investment Valuation / Evaluation Risk**	Management does not have sufficient financial information to make informed short-term and long-term investment decisions and link the risks accepted to the capital at risk. Management and key decision-makers are unable to reliably measure the value of a specific business or any of its significant segments in a strategic context.
		5	**Organization Structure Risk**	The company's organizational structure does not support change or the company's business strategies.
		6	**Measurement (Strategy) Risk**	Occurs when overall organizational performance measures focus primarily on near-term financial results or are not consistent with and do not support business strategies.
		7	**Resource Allocation Risk**	The company's resource allocation process does not establish and sustain competitive advantage or maximize returns for shareholders.
		8	**Planning Risk**	The company's business strategies are not driven by creative and intuitive input or based on current assumptions about the external environment resulting in strategies that are out- of-date and unfocused.
		9	**Life Cycle Risk**	An organization's approach to managing the movement of its product lines and evolution of its industry along the life cycle (e.g., start-up, growth, maturity and decline) threatens the ultimate success of its business strategies.
	B	**Public Reporting Risk**		
		1	**Financial Reporting Evaluation Risk**	Financial reports issued to existing and prospective investors and lenders include material misstatements or omit material facts, making them misleading.
		2	**Internal Control Evaluation Risk**	Failure to accumulate sufficient relevant and reliable information to assess the design and operating effectiveness of internal control over financial reporting, resulting in inaccurate assertions by management in the internal control report.
		3	**Executive Certification Risk**	Failure to accumulate sufficient, relevant and reliable information to assess the design and operating effectiveness of disclosure controls and procedures, resulting in material information not being disclosed timely to certifying officers and in public reports.

		4	**Taxation Risk**	Significant transactions of the company have adverse tax consequences that could have been avoided had they been structured differently. Failure to comply with all tax regulations (e.g. payment and filing requirements) creates risks.
		5	**Pension Fund Risk**	Pension funds are not actuarially sound, e.g., they are insufficient to satisfy benefit obligations defined by the plan.
		6	**Regulatory Reporting Risk**	Reports of operating and financial information required by regulatory agencies are incomplete, inaccurate, or untimely, exposing the company to fines, penalties and sanctions.
	C	**Operational Risk**		
		1	**Budget and Planning Risk**	Budgets and business plans are not realistic, based on appropriate assumptions, based on cost drivers and performance measures, accepted by key managers, or used as a monitoring tool.
		2	**Product / Service Pricing Risk**	The company's price is more than customers are willing to pay or does not cover production and distribution costs.
		3	**Contract Commitment Risk**	The company does not have information that effectively tracks contractual commitments outstanding at a point in time, so that the financial implications of decisions to enter into incremental commitments can be appropriately considered by decision makers.
		4	**Measurement (Operations)**	Process performance measures do not provide a reliable portrayal of operating performance and do not accurately reflect reality. The measures do not provide relevant information for decision making because they are not informative, understandable, believable, actionable, or indicators of change.
		5	**Alignment Risk**	The objectives and performance measures of the company's business processes are not aligned with its overall business objectives and strategies. The objectives and measures do not focus people on the right things and lead to conflicting, uncoordinated activities.
		6	**Accounting Information Risk**	Financial accounting information used to manage business processes is not properly integrated with nonfinancial information focused on customer satisfaction, measuring quality, reducing cycle time and increasing efficiency. The result is a myopic, short-term fixation on manipulating the outputs of business processes to achieve financial targets, rather than fulfilling customer expectations by controlling and improving processes.