RISK MANAGEMENT FRAMEWORK

GENERIC CORPORATE RISK IDENTIFICATION AND MITIGATION PLAN

Version 2.0

MARCH 2012

PT PENJAMINAN INFRASTRUKTUR INDONESIA (PERSERO) | *INDONESIA INFRASTRUCTURE GUARANTEE FUND*

RISK MANAGEMENT FRAMEWORK

GENERIC CORPORATE RISK IDENTIFICATION AND MITIGATION PLAN

PT PENJAMINAN INFRASTRUKTUR INDONESIA

(*INDONESIA INFRASTRUCTURE GUARANTEE FUND*)

VERSION 2.0

MARCH 2012

Document Log and Revision Table

Version	*Description*	*Date*	*Note*
1	*Original Document*	*10 August 2011*	*This version has been endorsed by BoD Decree No. SK-002/DIR/RAP/08/2011*
2	*Update on overall benchmarking to the risk management international standard (i.e. COSO-ERM and ISO:31000)*	*1 March 2012*	*Improvement assisted by a specialist consultant (i.e. KPMG Indonesia)*

Table of Contents

A. INTRODUCTION

1 Background

Indonesia Infrastructure Guarantee Fund (IIGF) is a State Owned Enterprise which was designed and intended to function as, among others, the single window for appraising infrastructure PPP (Public-Private Partnership) projects requiring government guarantees. In that regards, IIGF become one of the critical elements on the development of PPP projects in Indonesia.

PPP is a scheme that allows government infrastructure initiatives to be developed and managed by the private investors. This scheme will include cooperation between the local government, line ministry or state-owned enterprise as Contracting Agencies (CA) and the private investor in infrastructure projects development. IIGF will guarantee the commitment of the CA under the PPP project agreement to attract private investors and/or creditors to invest their fund in the project.

Thus, the primary objectives for IIGF to be established include the following:.

- Providing guarantees for PPP projects in infrastructure.
- Improving creditworthiness, particularly bankability of PPP projects in the perspectives of investors/lenders.
- Improving governance and transparent process in the provision of guarantee.
- Minimizing the possibility of sudden shock to the National State Budget ("APBN") and ring-fencing the exposure of government's contingent liabilities

In achieving the above objectives, it is essential for IIGF to establish integrated management frameworks, including Enterprise Risk Management (ERM) framework. ERM framework is a structured and consistent approach to directing and controlling an organization with regard to risk and uncertainty affecting the organization and represents a holistic approach to manage risks that IIGF faces in the changing business environment. Effective ERM is a requirement therefore, across all business processes at IIGF to obtain reasonable assurance regarding the meeting of business objectives.

IIGF ERM framework requires the embedding of a Risk Management practice and culture across the whole organization. As the organization that provides risks coverage for infrastructure projects, IIGF needs to have a clear and comprehensive approach in managing risks taking into account the unique risks inherent in various activities and projects. This framework document provides high-level guidance on how IIGF can manage its risks in corporate wide aspect and in the related infrastructure project risk aspect to achieve defined business objectives.

2 References

The main references of this IIGF Risk Management Framework are:

- COSO Enterprise Risk Management Framework; and
- ISO 31000:2009.

3 Objective of IIGF Risk Management

ERM implementation aims to achieve the following objectives:

- To develop IIGF to be a risk resilient organization in achieving its corporate vision and missions by means of thorough assessment of the risks inherent in all IIGF's business activities;

- To support risk-based decision making by management in achieving healthy business growth with consideration on defined risk/ return profile
- To comply with Good Corporate Governance principles by creating prudent strategy and processes;
- To enhance IIGF reputation among its stakeholder.

4 Purpose of This Document

As the IIGF's ERM framework, this document provides a structured methodology in identifying, evaluating, mitigating, monitoring and reporting of risks for IIGF as a business organization.

This document defines IIGF's Risk Management framework, which includes:

- Establishment of common principles & standards for Risk Management practice to allow common understanding of Risk Management;
- Risk appetite and tolerance that is agreed by management to define measurement of risk level;
- Adopted Risk Management framework that defines high-level business requirement for Risk Management processes; and
- Accountability and responsibility for Risk Management implementations.

5 Compliance

This framework document shall be complied with at all times. Non compliance of this document may be deemed a breach of discipline. All personnel shall be aware and comply to this framework in addition to compliance monitoring by Internal Audit.

6 Communication

Communication of Risk Management policies and procedures along with Risk Management results shall be performed periodically and/ or consistently to all personnel to create risk-based culture and common understanding of Risk Management language.

7 Review and Modification of The Risk Management Policies

The BoD shall review this Risk Management framework and its policies annually or whenever there are significant changes to IIGF's business and/ or internal environment. The revised policy / the amendment document shall be placed before Audit and Risk Management Committee (RMC) of the Board of Commissioners (BOC) for approval.

8 Limitation

Implementation of this framework will only provide reasonable assurance in managing the risks to achieve IIGF's objectives, due to the following:

- Subjective assessment during decision making;
- Negligence (human failures);
- Collusion and covering up deliberate misconduct in manipulating the financial statements or information;
- Considerations of cost vs. benefit in responding to risks; and
- Overriding Management's policies and operating procedures.

B. RISK MANAGEMENT STRATEGY

A well-formulated and uniformly understood Risk Management strategy is vital for driving the success of IIGF's ERM implementation. In addition, very importantly, in defining IIGF's risk appetite/tolerance, i.e., the level of risk it is prepared to assume, IIGF's Risk Management strategy needs to be aligned to its business strategy.

In essence, the approach adopted in this framework document can be described as the strategy, principles and technique of managing risks within IIGF by taking a holistic approach towards risk identification, measurement, monitoring and control/mitigation. As IIGF's business strategy changes, the ERM framework will have to evolve to adapt to the changes and hence it is critical that the prevailing ERM framework as prescribed in this document needs to be periodically reviewed and aligned against the IIGF's business strategy and directions so that the business objectives and Risk Management strategy are complementary.

1 Risk Management Mission Statement

IIGF's Risk Management mission statement establishes the "tone at the top" that guides the Risk Management activities throughout the organisation. The mission statement serves to communicate the IIGF's vision, principles and mandates.

IIGF's mission statement for Risk Management is "to understand the key risks facing the organization and to facilitate the Risk Management process by providing the appropriate tools and methodologies to explicitly manage risks. This would achieve a consistent approach in managing risk within the organization".

2 Risk Management Philosophy

In support of its Risk Management mission statement, ERM shall create a risk-aware organization through:

- Establishment of Risk-based Management System, which manage all key risks through embedded and inherent Risk Management practice in all business activities and decision making.
- Manage risk at all levels throughout the organization
- Clear accountabilities and independencies in conducting compliance review and monitoring of all activities (all Business Process Owners).
- Adoption of widely accepted international standards

3 Risk Appetite and Tolerance

Risk appetite and tolerance defines IIGF's attitude toward risks. As calculated risk-taking is an integral part of the IIGF's business, an appropriate balance between the level of risk and the level of return desired shall be defined and established. An effective Risk Management framework that is commensurate with the size and complexity of IIGF's operations is put in place to ensure that the risks undertaken are well managed within the boundaries of IIGF's risk appetite / tolerance.

Risk appetite/tolerance is defined within IIGF as a notional measure of the financial and non-financial values that it is prepared to place at risk of loss, within a given level of confidence in the course of its business. Risk appetite and tolerance shall be defined based on linkage between IIGF strategy to expected value/ return and consideration to management appetite in pursuing business value/ return against its amount of risk.

In this respect, IIGF encourages the taking of controlled risks, the grasping of new opportunities and the use of innovative approaches to further achieve business objectives, provided that, the associated risks of proposed actions and decisions should be properly identified, evaluated and managed to ensure that exposures are acceptable.

Particular care is needed in the taking of any action which could:

- Impact reputation;
- Impact earnings
- Impact financial liquidity and reserve;
- Result in financial loss;
- Impact health, safety and environment; and
- Undermine the independent and objective review of activities.

Risk Appetite and Tolerance are translated into Risk Impact and Likelihood guidelines. Please refer to Appendix F.2 for defined risk impact and likelihood guidelines. Risk appetite and tolerance shall be reviewed and updated at least annually, or whenever IIGF has significant changes in both external and internal business environment.

4 Risk Management Principles

In line with leading practices, IIGF adopts the Risk Management principles as follows:

- Risk Management is an integral part of all organizational processes, which shall be embedded in all activities, processes and systems; and considered in all decision making.
- Risk Management is dynamic, iterative, responsive to change, and tailored in alignment of corporate objective achievement
- Risk Management is a human driven process that creates common responsibilities of all personnel
- Risk Management is a driver to create adapting and sustain organization

5 Embedding of ERM

IIGF management understands that embedding the Risk Management process and culture into day to day business activities is crucial to achieve the risk resilience organization. Here, 'embedding' means, "to incorporate or to contain as an essential part or characteristic".

Below are key areas that will be included:

5.1 Business Planning

Business planning at IIGF consists of a series of cyclical processes; at the highest level, the Strategic Planning Process determines organizational and strategic requirements and sets Corporate and high-level division goals.

In performing Business Planning, embedded ERM process can be performed through:

- Consideration of existing risks in determining business plan, that is business planning is determined to treat existing risks;
- Consideration of new risks as a result of defined business plan;
- Determination of performance objectives and KPIs to ensure that the risks are closely monitored and treated to achieve business objectives; and
- Communication of existing and new risks relation to defined business plan and KPIs.

5.2 Business Execution

Business execution is the implementation of strategies and plans and the control of associated activities. IIGF business exists within constantly changing and increasingly uncertain business environments; these changes and uncertainties have the potential to affect the ability of the organization to meet its KPI.

In successful organizations (where KPIs are consistently achieved) management understand the business environment, develop plans appropriate to the environment and, having the ability to recognize uncertainty and change, make timely adjustments – they have effective control over their business.

KPI might not be met wherever effective control is either not achievable or is not in place.

In business execution, embedded ERM process can be performed through:

- Risk awareness of business process owner, which is translated to self risk identification, evaluation, treatment, monitoring and reporting with coordination with Risk Management Function;
- Identification of risk that may hinder the division's objectives
- Determination and monitoring of KRI to the division's objective risks
- Consistency of control performance as defined in policies and procedures

5.3 Project Risk Evaluation and Monitoring

IIGF business nature is to provide risk treatment of infrastructure project risks by providing financial guarantee. The projects being guaranteed (individually or as a portfolio) may have their own risk profile, which is separated from IIGF risk profile. However, IIGF risk profile may have positive correlation with project risk since a failure in the project could result in financial loss(es) to IIGF. Therefore, the Risk Management in these projects (especially on the risks being covered by the guarantee) is crucial to IIGF performance.

In managing project risks, embedded ERM process can be performed through:

- Risk identification during determination of project pipeline/ target and screening stage, considering IIGF risk appetite;
- Risk assessment of the project in the guarantee appraisal, structuring and implementation phases;
- Determination of risk treatment of project risk with coordination with relevant project stakeholders to be included in the project Risk Mitigation Plan developed by the Contracting Agency (CA);
- Implementation of the defined risk treatment in the related project agreements (i.e. PPP Agreement, Guarantee Agreement, Recourse Agreement) to increase IIGF influence in project Risk Management;
- Implementation of the framework for IIGF to monitor project risks through the performance of the guaranteed project's Risk Mitigation Plan in all relevant project phases;
- Ensuring guaranteed project's Risk Management framework is aligned with IIGF Risk Management framework.

5.4 Guarantee Structuring

Each infrastructure project is unique in nature depending on type of project, location and other relevant parameters. Each project may need specific consideration and treatment in providing the optimum guarantee structure.

In determining guarantee structure, embedded ERM process can be performed through:

- Risk assessment on each possible structure involving potential co-guarantor(s) and/or reinsurer (s) to align with IIGF risk appetite and guarantee capacity;
- Consideration of consolidated existing guarantee structure (i.e. consideration of all guarantee structure as portfolio);
- Impact assessment of determined guarantee structure to corporate risk profile;
- Determination of limit framework for capital against the guarantee exposure;
- Consideration of guaranteed project diversification;

5.5 Financial Resource Management

As a financial service institution, financial resource management is crucial for IIGF. IIGF must ensure that there will be adequate fund to cover guarantee exposure, while at the same time, the fund needs to be utilized to cover operational expenses and grow the business by increasing exposure limit capability.

In managing fund, embedded ERM process can be performed through:

- Determination of limit structure as described in fund mobilization policy, investment policy (e.g. counterparty exposure limit, asset allocation policy), and also cashflow and liquidity management;
- Monitoring and assessment of limit framework compliance, maturity requirement, market risk sensitivity and counter-party risk;
- Valuation of IIGF's investment portfolio.

5.6 Tools of Embedding ERM Process

To embed ERM process in daily activities, several tools that can be utilized are:

5.6.1. Policies and Procedures (SOPs)

Policy and Procedures shall be embedded with Risk Management process by establishing clear rules and standards for all business activities that is aligned with defined risk appetite and tolerance; risk monitoring; and risk treatment.

5.6.2. Limit Framework

Limit Framework shall be defined in areas where IIGF can reliably measure and monitor risk exposure, across a range of risk variables. Limits may be set at a number of levels, such as single guarantee exposure, guarantee portfolio, investment/treasury transaction, procurement and concentration level (i.e business sectors, geography). At the top level, risk tolerance limits are set to align with Risk Appetite and the expressed or implied tolerance of key stakeholders. Limit framework also shall be defined in related policies.

5.6.3. Delegation of Authorities (DoA)

DoA shall be defined to ensure that key risk-taking decisions are taken only by certain individuals, or committees, with the skills, judgment and perspective to ensure that IIGF's control standards and risk/return objectives are met. DoA should be aligned defined risk appetite and tolerance.

5.6.4. Internal Audit

Assurance activitities as part of Internal Audit activities shall be prioritized to high risk area through Risk-based audit implementation.

5.6.5. KPI

KPI shall be defined to ensure that Risk Management is part of everyone responsibilities. KPI shall be embedded with Risk Management element by considering compliance to risk mananagement policies and procedures; and consistency in performing and managing risk monitoring and risk treatment.

5.6.6. Third Party Agreement (e.g. Guarantee Ageement, Recourse Agreement, Vendor contract)

Comprehensive agreement with third party shall be defined to manage identified risks resulted from the agreement subject. Defined agreement shall consider risks that may be arising in performing the agreement and include articles that treat the risks and/ or IIGF rights to monitor and treat the risks.

6 ERM Framework Evaluation

Implementation of this Risk Management framework shall be evaluated periodically by an independent assurance provider (Internal Audit). Evaluation criteria are as follows:

- Adequacy of ERM compared against referred international standard
- Compliance of Risk Management Framework by all division
- Adequacy of risk infrastructure to support effective and efficient Risk Management process
- Effectiveness of embedded ERM process

C. DEFINITION AND RISK CATEGORY

1 Risk Category

IIGF categorize risks into the following category:

- ***Strategic risk*** , include all risks related to strategy planning, execution and monitoring
- ***Financial Risk***, include all risks related to Market risk and Liquidity risk
- ***Operational Risk***, include all risks arising from execution of a company's business functions

Figure 1. Risks in IIGF

2 Risk Taxonomy and Risk Definition

The purpose of this section is to provide clear definitions of risk and covers under this ERM framework. The risk taxonomy (shows the breakdown of possible risk sources) and the risk definitions are as the follow:

A. Category of Strategic Risks

The risk resulting from inaccurate determination and execution of IIGF's business strategies, inaccurate business decisions, or the unresponsiveness to external changes.

A.1. Strategy and Planning risk class

The risk resulting from the weakness of strategic context and planning issues of the IIGF which may impact to the IIGF strategic values and performance as an organization.

B. Category of Financial Risks

This category classifies risks generally occurs due to the inability of IIGF to achieve its revenue target, losses from the placement of investment funds, and the inability of IIGF to obtain new funding, whether from creditors or from shareholders.

B.1. Market (e.g. interest rate, currency) risk class

This class put together the risk resulting from adverse movement of market factors which include interest rates and foreign exchanges and equity price.

B.2. Liquidity and Credit risk class

The financial risks in this class relate to the liquidity and creditworthiness issues related to the IIGF assets and revenues.

C. Category of Operational Risks

This category of risks generally arising from execution of IIGF's business functions. It focuses on the risks arising from the people, systems and processes through which a company operates (including from guarantee provision activities as the main business of IIGF).

C.1. General Operational risk class

General operational risk is generally related to the inability of IIGF to operate its business functions efficiently, which causes operational losses from non guarantee provision activities.

C.2. Guarantee Provision risk class

This risk group classifies the operational risks related to the role of IIGF as the Business Entity for Infrastructure Guarantee (Badan Usaha Penjaminan Infrastruktur or BUPI).

C.3. Legal and Compliance risk class

This risk group related to the non compliance of the IIGF as a corporate to the legal or regulatory standards which may impact to the IIGF strategic values and performance as an organization.

The definitions of each risk under each risk category and risk class are provided as Appendix 8 of this document.

D. RISK MANAGEMENT GOVERNANCE

1 Governance Model

The ERM governance model is premised on three lines of defence – Risk Taking Units (Business Unit); Risk Control Units (Risk Management Function) and the Internal Audit Function (Internal Audit).

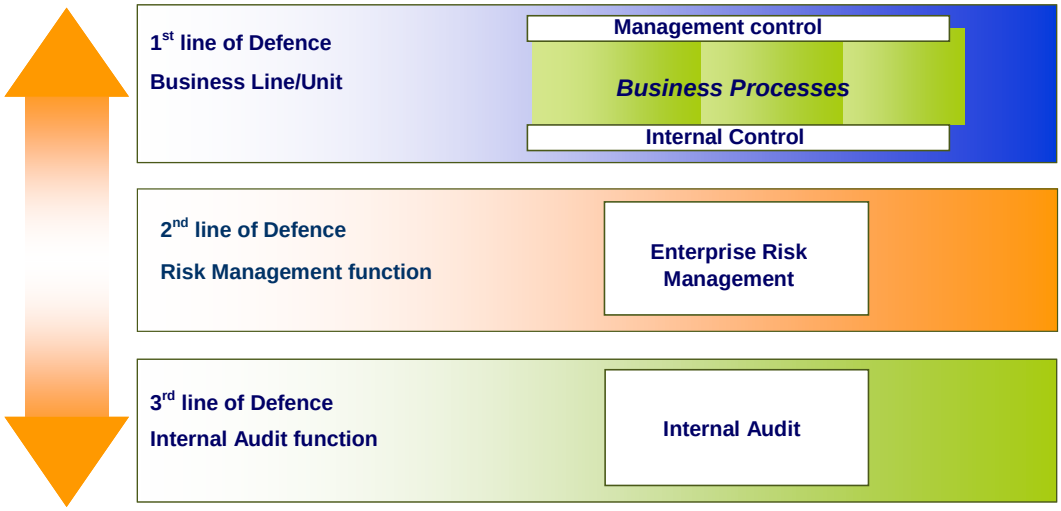


Figure 2. ERM Governance Model

The ERM governance model is designed in this manner so as to place accountability and ownership as close as possible to where the risks arise and to create centres of excellence that add real value across the business.

The key roles of each of the three (3) lines of defence are:

1.1 First Line of Defense

The key roles of the Business Line/Unit are:

- Daily responsibility for taking and managing risks arising from their business activities, as the primary risk owners;
- Implementation and execution of ERM framework, policies and procedures;
- Reporting on risk exposures by providing management information;
- Alignment of business plans and strategies to the overall ERM framework

1.2 2nd Line of Defence

The key roles of Risk Management function are:

- Development of the ERM framework, policies and procedures;
- Organization-wide coordination and facilitation of Risk Management activities;
- Development and providing support methodologies and tools;
- Organization-wide monitoring and reporting on risk;
- Providing Risk Management specialist support and advice to the business.

1.3 3rd Line of Defence

The key roles of the Internal Audit function performed by Internal Audit are:

- Independent responsibility to ensure appropriateness of the ERM framework and process;
- Ensure adequate functioning of the ERM framework and process as it has been designed.

2 Roles and Responsibilities

Within IIGF, the various roles and responsibilities with respect of Risk Management are set out in the following paragraphs. It also outlines the extent of involvement from Internal Audit.

The risk reporting structure is built from the existing organisation structure. Reporting lines for Risk Management is aligned to the ERM Governance Model. Further details on the reporting structure and reporting lines are as described under the section on Risk Monitoring and Reporting.

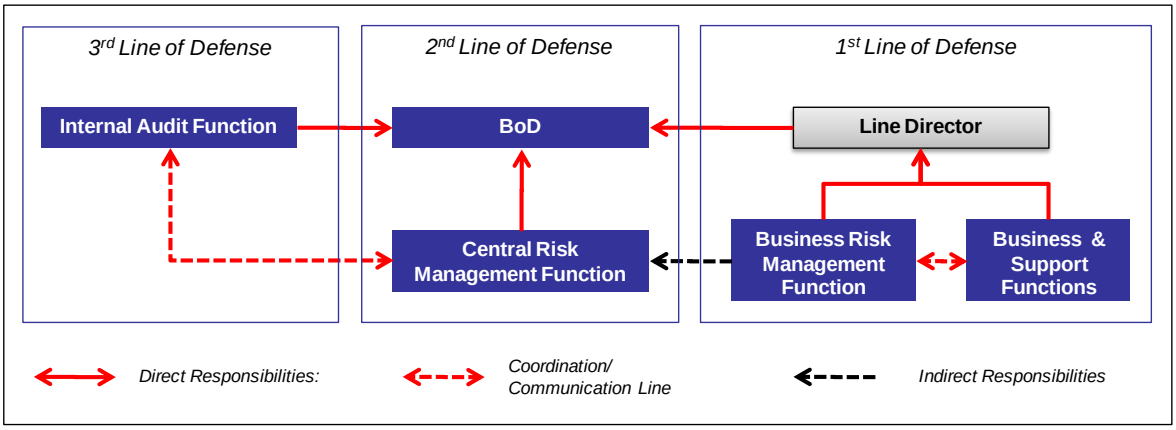


Figure 3. Risk Management Structure

The main roles and responsibilities are:

2.1 Boad of Directors (BoD)

BoD has ultimate responsibility in every aspect of Risk Management activities. Roles and responsibilities of BoD are:

1. Managing and controlling overall corporate risk
2. Determining Risk Management policy;
3. Monitoring and directing IIGF management in Risk Management implementation and also assuring the adequacy of tools, systems and resources to support Risk Management implementation;
4. Reviewing and approving the objective, strategy, framework, vision and mission, organizational structure, risk appetite, risk tolerance, risk culture, and resource allocation of Risk Management periodically;
5. Monitoring and evaluating Risk Management implementation;
6. Facilitating the risk mitigation process;
7. Evaluating the Risk Management policies;
8. Ensuring comprehensive independent review of Risk Management implementation.

2.2 Central Risk Management Function

Central Risk Management Function currently resides under Risk Management (RM) division. The specific roles are as follows:

1. Developing comprehensive Risk Management framework and strategy.
2. Reviewing and providing input to IIGF's BoD regarding Risk Management policy and strategy by considering change factors that significantly affect IIGF's business activity.;
3. Promoting awareness and understanding of Risk Management process to assure IIGF's business activities are aligned with Risk Management strategy through adequate training and communication session;
4. Ensuring that all relevant divisions are actively involved and supported Risk Management implementation that aligned with defined framework and policy by coordinating and facilitating the Risk Management process in all divisions;
5. Developing early warning detection and response system, and also mitigation program for critical corporate risk;
6. Facilitating and monitoring the Risk Management reporting process from all divisions/functions;
7. Establishing Risk Management culture in all levels within IIGF, including adequate communication regarding Risk Management framework.
8. Facilitate overall Risk Management processes
9. Strategic link for the enterprise in terms of risk by monitoring consolidated risk profiles as a corporate as a whole
10. Provide guidance and coordination among constituencies in performing risk management processes
11. Identify enterprise trends, synergies, and opportunities for change based on current risk profile
12. Liaison between third line of defense and first line of defense
13. Oversight over certain risk areas (e.g., credit, market, project) and in terms of certain enterprise objectives (e.g., compliance with regulation, reputation, earnings)
14. Support BoD / BoC in determining IIGF risk appetite
15. Prepare periodic capital monitoring review
16. Ensure Management develops adequate risk mitigation plans
17. Develop IGF into a risk resilient organisation through constant communication, reinforcement and training
18. Provide an independent view of management process to review and manage risks associated with project appraisals, project monitoring, claims, pricing, recourse and co-guarantee arrangements
19. Assess risks on individual projects/ support when needed

2.3 Business and Support Function

Risks, by its nature, are embedded in every activity across the organization. As the primary owner of the risks, business and support functions are responsible for the day-to-day management of these risks arising from their activities. Their specific responsibilities are:

1. Ensuring implementation and execution of the ERM framework within their respective functions;
2. Aligning business plans and strategies to the overall ERM framework.
3. Creating awareness of risk and control within their respective functions.
4. Ensuring the adequacy and cost effectiveness of controls.
5. Identifying, assessing and managing risks in day-to-day activities within their respective functions.
6. Submitting reports to Central Risk Management Function in the prescribed format on periodic basis.
7. Compliance to ERM framework, policies and procedures.
8. Coordinating with Central Risk Management Function to identify and monitor any changes on business, process or control environment that may have impact to the risk exposure.

2.4 Business Risk Management Function

Business Risk Management Functions are located within each Directorate and act as the key interface between the Central Risk Management Function and functions under each Directorate. This function assists Business Units in the management and supervision of risk inherent in their activities. They thus report functionally and administratively to line Director, whilst at the same time having an indirect reporting relationship to Central Risk Management Function to achieve an optimal risk management implementation within IIGF.

Their specific responsibilities are:

1. Assist the line Directors in managing risks inherent in their activities
2. Assist and facilitate functions under each Directorate in implementing risk management process according to the guidance provided by Central Risk Management Function
3. Prepare and facilitate risk management training specific for the functions under their responsibilities
4. Coordinate and communicate with Central Risk Management Function for the implementation of risk management process within their respective business

2.5 Internal Audit Function

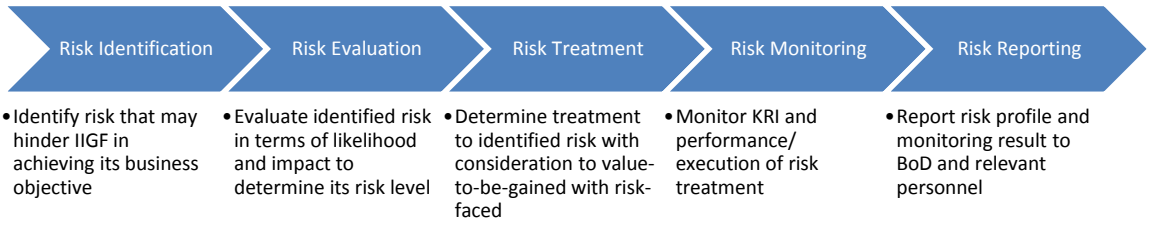
Internal Audit (IA) acts as independent assurance function. Roles and responsibilities of Internal Audit are:

1. Liaise with senior management and/ or board regarding performance and implementation of Risk Management
2. Rationalize and systematize risk assessment and governance reporting
3. Provide oversight on Risk Management content/ processes, followed by second line of defense (as practical)
4. Provide assurance that Risk Management processes are adequate, appropriate and comply with relevant regulation
5. Utilizing identified Risk Management processes result in performing corporate wide risk-based audit

E. RISK MANAGEMENT PROCESS

Risk Management is a continuous process. In general, Risk Management process shall comprise of:

1. Risk Identification
2. Risk Evaluation
3. Risk Treatment
4. Risk Monitoring
5. Risk Reporting



1 Risk Identification

Risk Management process starts with risk identification. The objective of risk identification process is to identify potential risks that may have impact to the achievement of corporate goals. Risk identification of corporate wide risk shall be performed at least annually or whenever there are significant changes to IIGF's business environment.

1.1 Risk Identification Principles

- Has clear description explaining the risk event unambigiously
- Be able to be mapped to relevant corporate/ division objective
- Based on best available external and internal information
- Identify causes of risk
- Has clear risk owner
- Has clear and measureable KRI
- Be able to be mapped to relevant risk category (as defined in page 12 of this document)

1.2 Context

Risk identification shall be based on context that is relevant to IIGF business environment.

1.2.1. External context

- Regulations that are related to infrastructures, funding, project guarantee, state-owned company, etc. in local and national scope
- Political environment within executive agency, parliamentary, relevant line ministries both in local and national scope.
- Business environment that is related to infrastructure, funding, project guarantee, etc. in local, national, regional and global scope.
- Socio economic environment that is related to income per capita, social demographic, etc. in local and national scope.
- Expectation of IIGF as catalyst in infrastructure development by government

1.2.2. Internal context

- Implementation of pre-appraisal work
- Increasing resources capability (e.g. people, financial, technology, processes,etc.) as IIGF is a newly formed organization
- Compliance to Good Corporate Governance Principles

1.3 Key Steps in Risk Identification Process

1.3.1. Corporate Risk

1. In the early stage of identification process, Central Risk Management Function together with the respective function will identify risks that may possibly emerge in all products and activities. The outcome of identification process will be populated in the risk register (please refer to appendix F.8 and used as a basis in conducting periodic risk assessment). This process also involves Internal Audit Division to ensure that potential risks have been identified.
2. Each function identifies potential and new risks that emerge as a result of changes taken place in that particular function, such as changes in internal/external policy, new regulations, or process / system. This identification process as necessary may inlvolves Central Risk Management Function. The outcome of this activity will be used to update the function's risk register.
3. Respected function's Director, review and validates the risk register.
4. Central Risk Management Function maintains the consolidated risk registers.

1.3.2. Project Risk

1. Business Risk Management Function facilitate Project Appraisal function in initiating risk identification process of the project based on defined risk register by project owner (e.g. contracting agency, private investor), discussion with project stakeholder and other appropriate method. In this step, Central Risk Management function may be involved to provide input and insight in identifying risks
2. Central Risk Management Function maintains the consolidated risk registers

2 Risk Evaluation

The next step is to evaluate the risks that have been identified to understand the level of risks in terms of consequences, likelihood, adequacy of controls and the causes.

2.1 Scope of Risk Evaluation

2.1.1. Corporate-wide Periodical Risk Evaluation

The risk evaluation shall be conducted periodically (e.g. semi-annually or quarterly). It will be facilitated by the Business Risk Management Function and as necessary Central Risk Management Function with the involvement of all divisions in IIGF to ensure that the outcomes of the exercise have addressed the specific concerns in all IIGF business processes.

2.1.2. Specific Risk Analysis

In addition to the periodical risk evaluation facilitated by Risk Management function, specific risk analysis exercise must be performed by particular organization functions on the business process involving decision above certain risk threshold. The business processes (within certain organization functions) assigned by the management to conduct this exercise are:

1) Significant procurement activities (i.e. for goods or services above Rp 1 billion);
2) Pre Appraisal Work activities
3) Project Appraisal activities
4) Other critical activities that has significant impact to IIGF

2.2 Risk Evaluation Parameter

Risk level is evaluated against two main parameter, namely likelihood of risk occurrence (likelihood) and possible impact on risk occurrence (impact).

- Likelihood of Risk Occurrence defines probability of risk event occurrence within one year. Likelihood may be defined based on percentage of probability with consideration on frequency of event that creates the risk within one year. Please refer to F.1for defined likelihood of occurrence.
- Impact on Risk Occurrence defines the highest impact of one risk event occurrence. Impact may be categorized as financial impact, reputation impact, compliance impact and other relevant category. Please refer to F.2 for defined impact criteria.
- Control criteria define the level of controls currently implemented to mitigate the risk. This evaluation will differentiate between gross and residual risk. Please refer to F.3 for control evaluation criteria.
- Risk grading matrix defines the level of risk in terms of impact and likelihood. Please refer to F.4 for risk level criteria.

2.3 Risk Evaluation Principles

- All identified risk shall be evaluated
- Consideration and justification to chosen likelihood and impact shall be documented based on credible, reliable, and sufficient amount of data
- Risk evaluation shall consider correlation between identified risks, conditional probability of risk events
- For market risks, risks are evaluated using a consistent and structured model which performs sensitivity analysis, cash flow simulation and other relevant approaches
- For counterparty risks, risks are are evaluated using a consistent and structured model which performs credit exposure evaluation and risk-based scenario testing and other relevant approaches
- For project exposure risk, risks are evaluated using a consistent and structured model which performs scenario analysis, incorporating recourse timing, recoveries and other liabilities and other relevant approaches.

2.4 Risk Aggregation

Identified risk with similar characteristic may be aggregated using the highest risk level within the characteristic group.

2.5 Key Steps in Risk Evaluation Process

2.5.1. Corporate Risk

1. Each function evaluates risks in terms of likelihood/frequency, impact, adequacy of controls in place and causes using the agreed assessment criteria and template on periodic basis. ***Note:*** *specific evaluation approach for market and counterparty risks is governed under separate policy and procedure.*
2. Function's Director reviews, validate and sign-off the risk evaluation result before submitted to Central Risk Management Function
3. Central Risk Management Function analyses the risk evaluation and provide feedback as necessary.
4. Risk Management Function prepares IIGF risk profile report to be submitted to CEO and RMC.

2.5.2. Project Risk

1. Business Risk Management Function and as necessary Central Risk Management Function facilitate Project Appraisal function in evaluating risk in terms of likelihood/frequency, impact, adequacy of

controls in place and causes using the agreed assessment criteria and template on periodic basis from individual project aspect.

2 Operation Director and Finance Director review, validate and sign-off the risk evaluation result.

3 Central Risk Management Function prepares project risk profile report to be submitted to CEO and RMC.

3 Risk Treatment

Objective of risk treatment is to determine appropriate action that gives the most optimized benefit for IIGF in encountering identified risk.

3.1 Risk Treatment Category

Risk treatment is categorized into four main categories:

- Accept: risk treatment is not defined
- Avoid: risk treatment is defined to avoid the risk
- Mitigate: risk treatment is defined to reduce risk level
- Transfer: risk treatment is defined by transferring to other party

3.2 Risk Treatment Principles

- Risk treatment is determined based on risk treatment guidelines in 0.
- Work plan, PIC, budget and timeline for all risk treatment implementation shall be defined
- Cost-benefit analysis of all risk treatment against expected benefit shall be defined

3.3 Key Steps in Risk Treatment Process

3.3.1. Corporate Risk

1 Each function determines risk treatment for every identified risk according to risk treatment guideline. As risk treatment responsibilities may be overlapping between functions, each relevant function should gain each other commitment in performing agreed risk treatment. Central Risk Management Function may involve to facilitate the process

2 Relevant Division head and directors review and validate defined risk treatment and report to Central Risk Management Function as part of regular risk reporting

3 Central Risk Management Function validates, maintains and monitors the progress of consolidated risk treatment plan

3.3.2. Project Risk

1 Project Appraisal function held discussion with project stakeholder to determine risk treatment for every identified risk according to project and risk treatment guideline. Agreed key risk treatment shall be defined as part of guarantee contract requirement as appropriate. As risk treatment responsibilities may be overlapping between functions, each relevant function should gain each other commitment in performing agreed risk treatment. Central Risk Management Function may facilitate the process

2 Relevant Division head and directors review and validate defined risk treatment.

3 Project Monitoring function monitors the execution of risk treatment on day-to-day basis

4 Central Risk Management Function validates, maintains and monitors the progress of consolidated risk treatment plan

4 Risk Monitoring

Objective of risk monitoring is to monitor the most recent risk level of identified risk and progress on defined risk treatment implementation. Risk monitoring shall be performed at least quarterly.

4.1 Risk Monitoring Principles

- Self monitoring is performed by each risk owner with confirmation and consolidation by Central Risk Management Function
- Risk monitoring performance is embedded in all relevant personnel job description and KPI
- Risk monitoring is embedded into operational performance monitoring
- Key Risk Indicator (KRI) is used as one of the approach to monitor risks. Please refer to appendix F.6 for the methodology.
- Any unexpected risk level movement shall be followed with appropriate risk treatment plan
- For monitoring of risk treatment implementation progress, any deviation from expected progress should be followed up with remediation action plan
- Monitoring is performed based on best information available with relevant external and internal context
- Risk Management technology shall be utilized to allow efficient and effective risk monitoring and/ or Risk Management process in general
- Result of Internal audit works as independent assurance provider may be utilized as part of risk monitoring process and/ or to assess adequacy of Risk Management process

4.2 Key Steps in Risk Monitoring Process

4.2.1. Corporate Risk

1. Each function monitors risk profile based on key risk indicator and performance of defined risk treatment. Any deviation of risk treatment performance shall be escalated to relevant personnel.
2. Central Risk Management Function validates and consolidates risk monitoring result

4.2.2. Project Risk

1. Project Monitoring function monitors risk profile based on key risk indicator and performance of defined risk treatment in project agreement (e.g. Guarantee Agreement, Recourse Agreement, etc.) and subsequent document. Any deviation of risk treatment performance shall be escalated to relevant personnel.
2. Project Monitoring function submit Risk Monitoring result to Central Risk Management Function
3. Central Risk Management Function monitors risk profile and performance of defined risk treatment from project portfolio aspect. Any deviation of risk treatment performance shall be escalated to relevant personnel.
4. Central Risk Management Function validates and consolidates project risk monitoring result with corporate risk.

5 Risk Reporting

Objective of risk reporting is to report result of Risk Management activities.

5.1 Risk Reports

Risk reports consist of:

- High level consolidated risk profile dashboard
- Analysis of key risks, including risk description, KRI, historical and current risk level, risk evaluation consideration, risk treatment plan, effectiveness of related control
- Risk register with description of risk, risk owner, risk level and risk treatment plan
- Detail of each risk, as part of Risk Management working paper

5.2 Risk Report Frequency and Distribution

5.2.1. Corporate-wide risk assessment

Corporate wide risk assessment reports shall be produced quarterly and distributed to:

- BoC through RMC
- BoD
- Internal Audit as sources for Risk-based audit
- Division head for relevant risks report

5.2.2. Specific risk assessment

Specific risk assessment reports shall be produced as necessary and distributed to:

- BoD
- Internal Audit as sources for Risk-based audit
- Relevant Division head
- BoC, based on case-by-case necessity

5.3 Risk Reporting Principles

- Risk reports shall be produced based on the most recent information
- Risk reports shall include key analysis on key risks to allow reader understand overall risks that are affect IIGF
- Risk Management technology shall be utilized to allow efficient and effective risk reporting and/ or Risk Management process in general

5.4 Key Steps in Risk Reporting Process

5.4.1. Corporate Risk

1 Central Risk Management Function consolidates risk identification, risk evaluation, risk treatment and risk monitoring.
2 Central Risk Management Function generates risk profile report with key analysis and distributes to relevant personnel.

5.4.2. Project Risk

1 Central Risk Management Function consolidates risk identification, risk evaluation, risk treatment and risk monitoring.
2 Central Risk Management Function generates risk profile report with key analysis and distributes to relevant personnel.

F. APPENDICES

1 Criteria of Likelihood of Risk Occurrence

Likelihood of risk occurrence is one of the parameter that affects risk level. In each event/ activity, risk is created with some probability of occurrence. Risk occurrence probability has positive correlation with risk level since increases in likelihood of risk occurrence also increases the risk level. Therefore, likelihood also plays role in translating risk appetite to risk level. Below are criteria of likelihood of risk occurrence that shall be used during risk evaluation.

Likelihood of risk occurence	Description
Very Low	0% - 10% probability of risk could occur within 1 year or on each event/ activity that creates the risk
Low	10% - 30% probability of risk could occur within 1 year or on each event/ activity that creates the risk
Medium	30% - 50% probability of risk could occur within 1 year or on each event/ activity that creates the risk
High	50% - 70% probability of risk could occur within 1 year or on each event/ activity that creates the risk
Very High	70% - 100% probability of risk could occur within 1 year or on each event/ activity that creates the risk

2 Criteria of Risk Impact

Risk impact is another parameter that affects risk level in the event of risk occurence. In each occurrence of risk, there could be a loss that has positive correlation with risk level since increases in loss also increases risk level. Below are criteria of risk impact in the case of occurrence in one risk event.

Impact Category	Insignificant	Minor	Moderate	Major	Catastrophic
Financial Loss - Operations & TGA *	< IDR 2,5 million	IDR 2 million- 50 milliion	IDR 50 million- 100 milliion	IDR 100 million - 10 billion	> IDR 10 billion
Financial Loss - Investment, Guarantee Claim **	< IDR 2 billion**	IDR 2 billion- 9 billiion	IDR 9 billion- 14 billiion	IDR 14 billion- 20 billiion	> IDR 20 billion
Ratio of Capital to Guarantee Exposure	> 1.5	1.0 - 1.5	0.8 - 1.0	0.5 - 0.8	0.5
Liquidity	> 1.5 year operational cost	1 - 1.5 year operational cost	6 months - 1 year operational cost	6 - 3 months operational cost	< 3 months operational cost
Reputation	Negative perception in internal environment and not related to integrity	Negative exposure in region coverage and not related to integrity	Negative exposure in national coverage and not related to integrity	Negative exposure in national coverage and related to integrity	Negative exposure in national coverage and related to integrity followed by legal action
Compliance	Regulation violation that can be corrected instantly	Regulation violation that is subject to warning letter	Regulation violation that is subject to fine or penalty	Regulation violation that may result in ke personnel imprisonment	Revocation of business license
Health, Safety and Environment	Cause minor injuries that require first aid	Cause injuries that require intensive medical care	Cause bodily injury and/or permanent disability	Cause death	Cause death to more than 1 people

*Financial Loss - Operation & TGA:refers to Delegation of Authorities limit for Financial aspect; Example: Insignificant --> IDR 2,5 million (limit by EVP Treasury) & default of consultancy contract (e.g. survey work);

**Financial Loss - Investment: adjusted and refers to earlier KPMG interview result with BoD, focusing on deposit placement in a bank; estimated probability of default=2%; Example: Insignificant --> IDR 100 bio x 2% = IDR 2 bio;

**Financial Loss - Claim: estimated from potential of recourse mechanism failure;

3 Control Assessment Criteria

3.1 Type of Control

There are several types of control that may be utilized in defining Risk Treatment. Types of control are as follow:

- Preventive

  Preventative controls are designed to stop undesirable transactions, items, events, errors or incidents occurring. Examples are: authorization and approval controls, staff training, automated system calculation and validation, password and access controls.

- Detective

  Detective controls are designed to promptly reveal undesirable transactions, items, events, errors or incidents so that appropriate corrective action can be taken. Examples are: reconciliations, review of exception reports, day 2 checking.

- Recovery

  Recovery techniques are designed to reduce the consequences or damage arising from crystallization of an individually significant incident or a significant number of undesirable transactions, items, events, errors or incidents. Examples are: tested business continuity plans, succession plans, back-up sites and files, crisis management.

3.2 Evaluating Control

Control evaluation levels that may be utilized in risk evaluation are:

1 Controls are satisfactory considering the current operating environment.
2 Controls in place are satisfactory considering the current operating environment, however are not operating across all processes in which it should occur.
3 Controls in place could be compromised or fail. Improvement required aligning with good practice standards, although they provide comprehensive coverage.
4 Controls in place require improvements or have not yet been implemented. Immediate action is required to correct the control deficiency.

4 Risk Level

Risk level is determined by two main parameter, namely likelihood of risk occurrence and risk impact, which translate risk appetite as defined by BoD. High level of risk defines risks that are not acceptable, while low level of risk defines risks that are acceptable. Moderate level of risk defines risk that might be acceptable with some additional consideration regarding benefit to be obtained. Below is risk level matrix that shall be used in risk evaluation.

Likelihood of risk	Risk impact in case of risk materialization				
	Insignificant	Minor	Moderate	Major	Catastrophic
Very Low	Low	Low	Low	Low	Moderate
Low	Low	Low	Moderate	Moderate	Moderate
Medium	Low	Moderate	Moderate	High	High
High	Moderate	Moderate	High	High	High
Very High	Moderate	High	High	High	High

5 Risk Treatment Guideline

Risk treatment is a critical activities in risk management that defines subsequent activities in facing the risks. Determination of risk treatment shall be aligned with defined risk appetite that is translated in the risk level matrix. Below are risk treatment guidelines for each risk level that shall be use in determining response to identified risks.

Risk Level	Risk Treatment
Low	• Accept the risk with constant monitoring • At minimum, detective control is defined for the risk • At minimum, risk treatment approval is by Division Head and relevant Director • Risk treatment shall be implemented within 6 month
Moderate	• Reduce risk level, when ever possible • Preventive control must be defined for the risk • At minimum, risk treatment approval is by Division Head and relevant Director and CEO • If cost of risk treatment outweight benefit, accept the risk, with approval of Division Head and BoD • Risk treatment shall be fully implemented within 3 month
High	• Reduce risk level, when ever possible • If cost of risk treatment outweight benefit, accept the risk • Preventive control must be defined for the risk • Risk treatment approval is by Division Head and BoD • Risk treatment shall be fully implemented immediately • Require monthly risk monitoring

6 Key Risk Indicator (KRI) Approach

6.1 Definition of KRI

Risk indicators are statistics and/or metrics that indicate likelihood of risk occurance and impact of risk which can provide insight into a IIGF's risk position. KRI shall be defined after risk identification and supports the information in risk evaluation by providing critical information to business stakeholders about major risks in IIGF. The number of KRI is at the discretion of the business that owns the risk however at a minimum there should be at least one KRI per risk. Each KRI should have a tolerance allocated and data should be monitored periodically. These indicators shall be reviewed on a periodic basis (such as monthly or quarterly) to alert IIGF to changes that may be indicative of risk concerns and as early warning system in risk monitoring.

6.2 Identification of KRI

KRI should be identified that reflect the risk environment or the effectiveness of the controls in place. A first step might include looking at existing Key Risk Indicators or KRI and other regular business reporting measures to evaluate whether any of those measures would be helpful in monitoring the risks and controls in the business. The business should also review any other risk related data available to determine if the data would be useful as a KRI.

Once potential KRI are identified, the business must ascertain that the data for the KRI is appropriate. This includes ensuring that the data is regularly available (at least quarterly), confirming data integrity, and

confirming appropriateness for monitoring purposes. There could be a distinct difference between data sources and definitions, as well as methods for presenting KRI data (e.g. percentages versus absolute numbers). The business should carefully look at the KRI data they plan to track and also determine who will be responsible for collation of data for monitoring and reporting purposes.

6.3 Integration with the risk and control assessment

The KRI identification process needs to be closely integrated with the risk assessment process. After management identifies their risks and controls in place to mitigate those risks, the next step should be the identification of KRI to support the judgment around the effectiveness of the controls in place. KRI trends can be compared with trends in risk and control issues to evaluate the correlation between the KRI and the risk it is linked to.

A poor performing KRI should act as a flag to encourage management review of the risk and control environment. Action plans may need to be put in place to address the issue. Improvement in a KRI result may reflect that the action taken by management has addressed the risk or control issue.

6.4 KRI defined tolerances

Initially, it may be difficult to have a solid grasp on what the defined tolerances should be for each 'green', 'yellow' and 'red' KRI assessment. In order to define tolerances, the business may need to set initial tolerance levels using their best judgement and refine the levels after a study of KRI trends over an extended period is completed. After tolerance levels are defined for KRI, they will need to be reviewed on an annual basis.

6.5 Validation

At least annually, the business must reassess the projecting power of indicators and analyze correlation of KRI to the risk and control environment. The business should look at the trend of the KRI data and discuss whether the KRI was effective in monitoring the risk and control environment. KRI data sources may need to be re-confirmed or new KRI identified to better assist management in monitoring the risk and control environment. During the annual review process, the business should also review tolerance levels and determine if any revisions are necessary. Significant business changes, risk events or losses may also trigger reassessments during the year.

6.6 KRI Action Plan

Action Plan is a plan detailing the tasks, persons responsible, timeline and key milestones. IIGF need to develop KRI rating table to define variance from predetermine threshold that is still acceptable. An Action is triggered if the actual value of KRI falls above the acceptable level.

Several considerations to construct KRI rating table are:

1. Pass experience which cause the risk to happen
2. Input from management or internal audit
3. Risk appetite

6.7 KRI Reporting

At minimum the KRI report will include:

1. KRI for high rated risks grouped by risk category and identified as predictive or lagging

2. current period data and movement from the previous period
3. Scoring or rating that measures the performance of the KRI against tolerance or target levels.

7 Risk Management Committee (RMC) Term of Reference

7.1 Term of Reference

The RMC term of reference is governed under IIGF Corporate Governance document.

7.2 Composition

RMC is established to have a focus group for Risk Management and Internal Audit activities. The composition of RMC is as follows:

Roles	Function
Chairman	CFO
Deputy Chairman	COO
Secretary 1	Risk Management unit Head
Secretary 2	IA Head
Member	Head of BUD
	Head of PAU
	Head of Treasury
	Head of PMO

7.3 Delegates

Delegates for members are permitted however they will be required to make decisions binding on the member they represent. Delegates are not permitted on an ongoing or permanent basis

7.4 Meeting Timing

The Committee will meet on agreed schedule. The Chairman is responsible for determining the frequency of meeting.

7.5 Minutes

The Committee must assure that minutes of each meeting are recorded and retained. Minutes are to be presented by the Chairman of the Committee at the next following meeting.

7.6 Attendance

Any two third of members will constitute a quorum and will be deemed sufficient for Committee decision making process.

The Committee will invite specialize divisions (e.g. legal, human resource, etc) or subject matter experts to present specific topics or issues as required.

7.7 Management and Storage of Committee Minutes and Paper

Committee secretary must produce and circulate draft minutes within one week from the date of the meeting. The secretary will maintain and retain a physical copy and a soft copy of all meeting minutes, papers, etc on IIGF network to force accessibility by committee members and other stakeholders as appropriate.

7.8 Minimum Standard Meeting Agenda

The minimum meeting agenda with respect to Risk Management topics are as follows:

Item #	Agenda Item	Purpose / activity	Frequency
1	Review the outcomes from previous meeting	Oversight and complete requisite actions arising in previous meetings	Each meeting
2	Review the effectiveness of ERM implementation across the organization	▪ Review the effectiveness and application of ERM within the business and support function ▪ Identify potential improvement required for ERM framework and policy ▪ Review the resolution of internal and external audit issues	Each meeting
3	Review the resource structure and ERM training	▪ Review the resource of risk structure and the adequacy of training ▪ Identify and perform action on additional resource or training required including coordinating with related division (e.g. human resource, strategic planning and training)	Each meeting
4	Review and perform action on Quarterly Reporting Pack	▪ Review Risk Maps and Risk Profiles to identify changes, systemic issues or significant issues that need to be resolve in RMC ▪ Review KRIs to assess the future impact of risk profile and identify appropriate strategies as required. ▪ Review Action Plan for completion and understanding underlying reasons ▪ Review emerging issues and calendar of events to identify future strategies and potential impacts on the Business Unit.	Quarterly

8 Risk Register Template

Risk register is required to document all identified risk, result of risk evaluation and determination of risk treatment. It shall be always updated in every step of risk management process. Below is template for risk register and guideline to populate the template.

Guideline:

1. Risk Category: fill this field with risk category that related to identified risk as decribed in 'Risk Description'
2. Risk Description: fill this field with decription of identified risk which explains nature of the risk
3. Risk Owner: fill this field with risk owner who is responsible in managing the activities that direcly related to the risk
4. Cause(s): fill this field with the description of set of factors that may affects or lead to the occurrence of risk event
5. Impact: fill this field with the description of potential direct or indirect loss or cost to IIGF that could have been suffered from a risk event
6. Current Control: fill this field with the description of any action (e.g.policies, procedures, or activities) taken by relevant personnel (Control Owner), designed to ensure that risks are contained within the risk appetite/tolerance
7. Control Owner: fill this field with the assigned person who is responsible for the business unit, which owns the controls associated with the risk event
8. Control Evaluation: fill this field with the effectiveness level of existing control (refers to control assessment criteria)
9. Impact Level: fill this field with grading as describe in "Impact Category" (e.g. insignificant, minor, moderate, major, and catastrophic) after consideration to existing control effectiveness
10. Likelihood: fill this field withthe grading criteria as described in "Likelihood of Risk Occurrence" table (e.g. very low, low, medium, high, and very high) after consideration to existing control effectiveness
11. Risk Level: fill this field with the grading criteria as described in "Risk Level" matrix (e.g. insignificant, minor, moderate, major, and catastrophic) based on defined value in 'Likelihood' and 'Impact Level'
12. Treatment Category: fill this field with treatment category as described in "Risk Treatment Guideline" based on its risk level
13. Action Plan: fill this field with description of risk treatment action to be done in addressing the risk
14. PIC: fill this field with the assigned person who is responsible for defined risk treatment activities in 'Action Plan'
15. Due Date: fill this field with the target completion date of risk treatment plan.

Risk Register Template

			Risk Evaluation							Risk Treatment			
Risk Category	Risk Description	Risk Owner	Cause(s)	Impact	Current Control	Control Owner	Control Evaluation	Impact Level	Likelihood	Risk Level	Treatment Category	Action Plan	PIC	Due Date
Strategic Risk	Budget and planning risk													
	Business environment risk													
	Business model risk													
	Measurement (strategy) risk													
	Measurement (operations) risk													
	Alignment risk													
	Planning risk													
	Organizational structure risk													
	Human resource risk													
	Leadership and management risk													
	Corporate governance risk													
	Information for decision-making risk													
	Accounting information risk													
	Perceived benefit risk													
	Shareholder risk													
	Stakeholder risk													
	Regulatory risk													
	Legal risk													
	Emerging risk													
Reputation Risk	Reputational risk													
	Code of Conducts risk													
Financial Risk	Accounting exposure or translation risk													
	Financial reporting risk													
	Interest rate risk													
	Currency risk													
	Equity risk													
	Financial distress risk													
	Commodity risk													
	Insurance premium risk													
	Capital adequacy risk													
	Capital provisioning risk													
	Concentration risk													
	Correlation risk													
	Pricing risk													
	Liquidity risk													
	Investment's Credit Risk													
Operational Risk	Key personnel risk													
	Internal fraud risk													
	External fraud risk													
	Employment practices risk													
	Damage to physical assets risk													
	Business disruptions risk													
	Management of execution, delivery and process risk													
	Workplace safety risk													
	Catastrophe risk													
	Guarantee claim risk													
	Cost or time overruns Risk													
	Project pipeline risk													
	Pre-appraisal risk													
	Failed guarantee appraisal risk													
	False claim payment risk													
	Recourse mechanism risk													
	Contracting agencies risk													
Counterparty Credit Risk	Guarantee claim risk													
	Cost or time overruns Risk													
	False claim payment risk													
	Recourse mechanism risk													
	Contracting agencies risk													

9 Risk Taxonomy

Such risk breakdown was resulted from the implementation of risk identification and risk assessment of IIGF done in Q1 2012. This structure will benefit the update and refinement of such periodic exercise.

A	**Strategic Risks**	
	the risk resulting from inaccurate determination and execution of IIGF's business strategies, inaccurate business decisions, or the unresponsiveness to external changes.	
A.1.	***Strategy and Planning risk class***	
	The risk resulting from the weakness of strategic context and planning issues of the IIGF which may impact to the IIGF strategic values and performance as an organization.	
A.1.1	Strategic planning risk	An unimaginative and cumbersome strategic planning process may result in irrelevant information that threatens IIGF's capacity to formulate viable business plan or result in inappropriate goals and objectives.
A.1.2	Budget risk	Non-existent, unrealistic, irrelevant or unreliable budget and planning information may cause inappropriate financial conclusions and decisions by the IIGF management.
A.1.3	Business environment risk	Failure to monitor the external environment or formulation of unrealistic or erroneous assumptions about business environmental risks may cause inappropriate strategic decisions by IIGF management.
A.1.4	Business model risk	The risk resulting from having an obsolete business model and IIGF does not recognize it and/or lacks the information needed to make an up-to-date assessment and build a compelling business case for modifying that model on a timely basis.
A.1.5	Measurement risk	Non-existent, irrelevant or unreliable both performance and financial measures that may threaten the IIGF's ability to execute its strategies and its operation and may result in conflicting, uncoordinated activities throughout IIGF.
A.1.6	Organizational structure risk	Risk resulting from ineffectiveness of the IIGF's organizational structure, which threatens its capacity to change or achieve its long-term objectives.
A.1.7	Human resource risk	Insufficient or failed internal human resource performance planning/management may prevent IIGF in achieving its strategic vision and mission.
A.1.8	Leadership and management risk	Insufficient leadership and management skills of IIGF senior management may prevent IIGF in performing its strategic vision and mission.
A.1.9	Corporate governance risk	This risk comes about through potential improper governance structures (including delegation of authority) between directors, senior management, and staff, leading to improper decision making.
A.1.10	Information for decision-making risk	Irrelevant or unreliable or low quality of information used to support the execution of the IIGF business model, the internal and external reporting on performance and the continuous evaluation of the effectiveness of the IIGF business.
A.1.11	Accounting information risk	Overemphasis on financial accounting information to manage the business may result in the manipulation of outcomes to achieve financial targets at the expense of not meeting the client satisfaction, quality and efficiency objectives.
A.1.12	Perceived benefit risk	Benefit of work outcomes from IIGF can be perceived differently by the client due to inefficient and inflexible business process that may lead to business demand incontinuity.
A.1.13	Shareholder risk	Unrealistic or misunderstood expectations from shareholder may put additional burden on the achievement of the corporate vision and mission by the IIGF management. The risk can also be triggered by not effectively communicating the governance structure, strategic plan, operational activities, and performance of the corporation to the shareholders.
A.1.14	Stakeholder risk	Incompetent or incapable or poor-informed stakeholders may prevent IIGF in performing its strategic role as expected. This may also due to challenges faced by the IIGF from dealing with red tape environment and can also be triggered by not effectively communicating the relevant information to the relevant stakeholders.
A.1.15	Reputational risk	The risk resulting from negative publication related to IIGF's business activities or negative perception toward IIGF. This risk related to the trustworthiness of business and may be triggered by either internal or external factors. Damage to a IIGF's reputation can result in lost revenue or destruction of shareholder value, even if the IIGF is not found guilty of a crime or a bad situation.

B.	**Financial Risks**	
	This category classifies risks generally occurs due to the inability of IIGF to achieve its revenue target, losses from the placement of investment funds, and the inability of IIGF to obtain new funding, whether from creditors or from shareholders.	
B.1.	***Market (e.g. interest rate, currency) risk class***	
	This class put together the risk resulting from adverse movement of market factors which include interest rates and foreign exchanges and equity price.	
B.1.1	Interest rate risk	The risk that variability in value borne by an interest-bearing asset (e.g. loan or bond) impacting IIGF's financial performances (e.g. lower value of bond investment, increase of liabilities), due to interest rates variability.
B.1.2.	Currency risk	The risk of foreign exchange rates and/or the implied volatility will change, which affects, for example, the value of IIGF's assets held in that currency.
B.1.3.	Equity risk	The risk that IIGF's investments will depreciate due to stock market dynamics causing one to lose money.
B.1.4.	Financial distress risk	The risk of collapse of an entire financial system or entire market (i.e. systemic risk) which may has catastrophic impact to IIGF.
B.1.5.	Commodity risk	The risk of reduction in the value of the IIGF's income or assets due to the volatility of commodity costs and volume (e.g. coal).
B.1.6.	Insurance premium risk	Risk that any IIGF risks that are insurable as at the signing date pursuant to the agreed insurances later become uninsurable or facing substantial increases in the rates at that insurance premiums are calculated.
B.2.	***Liquidity and Credit risk class***	
	The financial risks in this class relate to the liquidity and creditworthiness issues related to the IIGF assets and revenues.	
B.2.1.	Capital adequacy risk	Risk of IIGF may not have sufficient capital reserves to operate its business or to absorb unexpected losses arising from guarantee claim, investment and operational risks.
B.2.2.	Capital provisioning risk	The risk is triggerred by inappropriate setting of capital reserve (i.e. under-reserve or over-reserve) which may impact inefficiencies in IIGF financial and operational performances.
B.2.3.	Concentration risk	Uneven distribution of exposures of the IIGF's guarantee and/or investment portfolio may increase the potential losses or probability of default of the portfolio.
B.2.4.	Pricing risk	The risk stemming from both under-pricing and over–pricing the guarantee due to inaccurate and inappropriate pricing framework or exercise, which may impact the IIGF's revenue performance.
B.2.5	Liquidity risk	The risk that may arise whereby the IIGF cannot meet its obligation due to inability of IIGF to meet the liquidity needs within a certain period of time (i.e. cashflow liquidity risk), or inability of IIGF to liquidate financial instruments as needed without realizing abnormal financial loss on the transactions (i.e. market liquidity risk).
B.2.6	Investment's Credit Risk	The risk of IIGF's investment loss due to bond issuer's failure to pay its obligations (i.e. interest coupon and/or principal) or bank's failure to meet its obligation on the deposit (i.e. interest and principal) due to default, liquidity problem or bankruptcy.

C.	**Operational Risks**	
	This category of risks generally arising from execution of IIGF's business functions. As it is a very broad concept which focuses on the risks arising from the people, systems and processes through which a company operates (including from guarantee provision activities as the main business of IIGF).	
C.1.	***General Operational risk class***	
	General operational risk is generally related to the inability of IIGF to operate its business functions efficiently, which causes operational losses from non guarantee provision activities.	
C.1.1.	Key personnel risk	The risk emanates from the failure of the key management to perform their official duties as a result of various reasons, such as high attrition, prolonged sickness, etc.
C.1.2.	Internal fraud risk	This risk can originate from misappropriation of assets, tax evasion, intentional mismarking of positions, bribery, etc.
C.1.3	External fraud risk	This risk may emanate from theft of information, hacking damage, third-party theft, forgery, etc.

C.1.4	Employment practices risk	The risk emanates from IIGF failure as an equal opportunity employer avoiding any discrimination against gender, race, colour, etc.
C.1.5	Damage to physical assets risk	The risk relates to the damage to the physical assets due to natural disasters, terrorism, vandalism, etc.
C.1.6	Business disruptions risk	The risk related to disruption of business activities as a result of utility disruptions, software failures, hardware failures.
C.1.7	Delivery and process risk	The risk resulting from the failures or breakdowns in internal procedures, people, and systems which may related to negligent errors issues (e.g. data entry errors, accounting errors, failed mandatory reporting, negligent loss of assets, etc) causes operating failure or losses to IIGF as company.
C.1.8.	Workplace safety risk	The risk related to failure of IIGF in providing a safe and conducive working environment which may causes operating failure or losses to IIGF as company.
C.1.9	Procurement of 3rd party risk	The risk related to failure to maintain credibility and competitiveness of the procurement process of 3rd party vendor/consultant due to lack of understanding on the service requirement, the market condition and its relevant procurement method/documentation.
C.2.	***Guarantee Provision risk class***	
	This risk group classifies the operational risks related to the role of IIGF as the Business Entity for Infrastructure Guarantee (Badan Usaha Penjaminan Infrastruktur or BUPI).	
C.2.1.	Guarantee claim risk (beyond CA control)	Occurrence of (un)foreseen guarantee claim triggered by the scope and level of inherent risk of each guaranteed project may impact significant shock to IIGF's capital position and operational performance.
C.2.2	Cost or time overruns risk	The risk of the project takes longer to complete or implement, or costs more than was anticipated resulting in reputation damage to the IIGF (or government).
C.2.3	Project pipeline risk	The risk that the IIGF operational performance is not achieved due to the high externalities/uncertainty of the project pipeline influenced by both CA and other Government institutions (in)actions.
C.2.4	Pre-appraisal risk (including TGA)	The risk that the IIGF resources allocated to prepare the project being proposed to be guaranteed by IIGF is not delivering the expected results (i.e. GAP can't be ready to be submitted), due to both CA and other Government institutions (in)actions.
C.2.5	Guarantee appraisal risk	The risk that the result of guarantee appraisal shows that the project fail to achieve appraisal criteria, while the allocation IIGF resources has been made.
C.2.6	False claim payment risk	Claim payment based on the claim documentations that turn out to be false or based on unreliable claim assessment process may impact the recourse mechanism failure and the significant loss of IIGF's capital.
C.2.7	Recourse mechanism risk	Failure or unreliable of recourse mechanism of the guarantee provided by IIGF as the recovery route of the claim payment made to the guarantee beneficiary.
C.2.8	Credit counterparty	The risk that the counterparty will not live up to its contractual obligations. Counterparty should be considered when evaluating a contract
C.2.9	Failed project transaction	The risk of the project failed to reach Financial Close/going thru for implementation due to lack/no interest from (financiers) market appetite to the project.
C.3.	***Legal and Compliance risk class***	
	This risk group related to the non compliance of IIGF as an organization to legal or regulatory standards which may impact to the IIGF strategic values and performance as an organization.	
C.3.1	Compliance risk	The risk resulting from IIGF's violation or incompliance to internal and external regulations including the regulatory standards (e.g. accounting standard) which may impact to the IIGF strategic values and performance as an organization.
C.3.2	Regulatory risk	The exposures of IIGF, as a state-owned entity, to changes in legality status and regulations applied as the basis of operational activities of the Company.
C.3.3	Legal risk	The risk resulting from weak juridical aspects that may caused by legal claims, absence of supporting legislative regulations, or deficient covenant, such as, incomplete contract requirements. The risk also occurs when counterparty are not legally able to enter into a contract due to legal actions or uncertainty in the applicability or interpretation of contracts, laws or regulations.
C.3.4	Code of Conducts risk	The risk triggered by illegal or inappropriate business practices or activities by the IIGF or its employees.

10 ISO 31000:2009 and COSO-ERM Linkage to IIGF ERM Framework

ISO 31000:2009 ERM Framework	COSO – ERM Framework	IIGF ERM Framework
Scope, Terms, and Definition	Internal Environment	**A. Introduction** **F. Appendixes**
Principles		B. 4. Risk Management Principles
Framework		
Mandate & commitment	Internal Environment	B. 1. Risk Management Mission Statement
Design		**D. Risk Management Governance** D. 1. Governance Model D. 2. Roles and Responsibilities
Implementation	Control Activities	B. 5. Embedding of ERM
Monitoring & Review		B. 6. ERM Framework Evaluation
Continual Improvement		A. 7. Review and Modification of The Risk Management Policies
Process		
Communication & Consultation	Information & Communication	A. 6. Communication B. 2. Risk Management Philosophy
Establishing the Context	Objective Setting	A. 3. Objective of IIGF Risk Management
	Internal Environment	B. 3. Risk Appetite and Tolerance **C. Definition and Risk Category**
Risk Assessment - Identification - Analysis - Evaluation	Event Identification Risk Assessment	**E. Risk Management Process** E. 1. Risk Identification E. 2. Risk Evaluation
Risk Treatment	Risk Response	E. 3. Risk Treatment
Monitoring & Review	Monitoring	E. 4. Risk Monitoring
Recording		E. 5. Risk Reporting

11 Glossary of Terms

TERM(s)	DESCRIPTION
IIGF	Indonesia Infrastructure Guarantee Fund
PPP	Public Private Partnership
CA	Contracting Agency
ERM	Enterprise Risk Management
BoD	Board of Director
BoC	Board of Commissioner
CEO	Chief Executive Officer
COO	Chief Operating Officer
CFO	Chief Financial Officer
RMC	Audit and Risk Management Committee
KRI	Key Risk Indicator
IA	Internal Audit function
BUD	Business Development division
PAU	Project Appraisal and Underwriting division
PMO	Project Monitoring division
SOP	Standard Operating Procedure

IIGF | PT Penjaminan Infrastruktur Indonesia (Persero)
Indonesia Infrastructure Guarantee Fund

Sampoerna Strategic Square, North Tower 14th Floor
Jl. Jenderal Sudirman Kav. 45-46
Jakarta 12930 - Indonesia

+62 21 5795 0550 +62 21 5795 0040 info@iigf.co.id
www.iigf.co.id