RISK BASED
ANALYSIS ON ENFORCEMENT & INSPECTION HANDBOOK

For Government Ministries & Agencies

"Driving Productivity of the Nation"

www.mpc.gov.my

MALAYSIA PRODUCTIVITY CORPORATION
Lorong Produktiviti, Off Jalan Sultan
46200 Petaling Jaya, Selangor Darul Ehsan, Malaysia.
Tel : 603 - 7955 7266 / 7955 7050 / 7955 7085
Faks : 603 - 7957 8068 / 7955 1824 / 7954 0795
Emel : marketing@mpc.gov.my
Laman Web: http://www.mpc.gov.my

ISBN NO.: 978-983-2786-42-9

PRODUCTIVITY AND REGULATION

Productivity is the only driver of income growth that is unlimited, as opposed to resource exploitation or increase in population and labour force participation, each of which faces natural limits. The potential for productivity growth to generate higher income for Malaysians makes it a natural and important consideration for decision makers. As such the continuing need to stimulate productivity rightly remains at the forefront of government policies.

Regulation is the lifeblood of a modern, well-functioning economy. Almost all regulations have the potential to impact on productivity, either through the incentives which they provide to businesses to change operating and investment decisions, or more directly through their impacts on compliance costs. It is inconceivable to think of a modern economy functioning without regulation. However, poor regulation can cause frustration and unintended consequences, or simply add red tape that adds nothing useful to the economy, society or the environment.

FOREWORD FROM DIRECTOR GENERAL

DATO' MOHD RAZALI HUSSAIN
MALAYSIA PRODUCTIVITY CORPORATION (MPC)

It gives me great pleasure to share with you this publication entitled "Risk-based Analysis on Enforcement and Inspection for Government Ministries and Agencies". It presents a comprehensive guide to facilitate regulators to develop coherent risk management framework for the application of risk management in regulatory inspection and enforcement.

The chapters are developed based on MS ISO 31000:2010 (Risk Management Principles and Guidelines) concepts, covering a series of topics including risk management regulatory design, general risk criteria in regulatory review and key components of risk management; modelling risk identification, analysis and evaluation; design of innovative approaches to respond and treat risks; the monitoring and communication of risks; as well as benefits and challenges of risk management in regulatory cycle.

The challenge for government is to develop and apply enforcement strategies that can balance between the best possible outcomes and compliance while keeping the costs and burden as low as possible. Effective regulations achieved through a more robust process of risk-based analysis and consultation with stakeholders enhances efficiency and accountability and at the same time promotes greater participation, inclusiveness, better buy-in and transparency.

This publication also draws heavily on case studies presenting the different risk-based inspection systems of Australia, Netherlands, England and Wales, UK and Ireland, indicating the nature of risks varies from one sector to another, and for this reason, many methods and tools have been developed to help them address risks systematically.

We hope that this publication will serve as useful reference for regulators to strive for continual improvement and enhancement of the inspection and enforcement process.

DATO' ABDUL LATIF HJ ABU SEMAN

DEPUTY DIRECTOR GENERAL
MALAYSIA PRODUCTIVITY CORPORATION (MPC)

The challenge in risk analysis is to gauge the consequence on non-compliance and the failure to comply, that is to determine whether the regulation is "leastly likely to comply" or "carries the biggest spill-over impact" in targeting inspection.

As such, developing risk measurement may help to consider and enable the creation of data source, development of analytics and providing basis for determining decision criteria. These criteria can then be used to identify high-risk subjects or for determining sampling plans. Such risk identification and detection mechanisms are crucial for a good risk management process.

RISK BASED ANALYSIS PROJECT TEAM

This publication aims to assist regulators to develop coherent frameworks for the application of risk management in regulatory inspection and enforcement. The chapters are developed based on MS ISO 31000:2010 (Risk Management Principles and Guidelines) concepts, covering a series of topics including: risk management; modelling risk identification, analysis and evaluation; design of innovative approaches to respond and treat risks; the monitoring and communication of risks; and the salient features of NPDIR that apply risk management.

Greater emphasis on risk-based approaches to the design of regulation and compliance strategies can reduce costs for business and reduce the opportunity costs of government action.

CONTENT

CHAPTER 1

INTRODUCTION

1.0 PRELIMINARY

Regulation is a key tool for achieving social, economic and environmental policy objectives of government and usually "regulation" is treated as synonymous with "law". Regulation is designed and enforced by regulators to ensure companies can efficiently conduct their businesses while providing safety, security, environmental protection and fairness to them. Regulation is fundamentally enforced by regulatory agencies formed or mandated by governments to carry out the purpose or provision of the legislation.

Malaysia is one of the most competitive economies in Asia and is globally recognised as having a business-friendly environment. The Government has encouraged private sector-driven and people-centred growth through a variety of initiatives and policies that have been very successful. To maintain the momentum of these initiatives for the Government has embraced good regulatory practice (GRP) in its administration. In 2013 the Government has engaged Organisation for Economic Co-operation and Development (OECD) to review its regulatory management system and provide support for piloting and implementing its regulatory policy. As a result, the National Policy on the Development and Implementation of Regulations (NPDIR) was launched by the Government in July 2013 and enforced in 2014 (figure 1.1 illustrates the regulation cycle in GRP).

MPC has been appointed as the key co-ordinating agency for the NPDIR and is also the secretariat for the Special Task Force to Facilitate Business (PEMUDAH) which is the bridge for the NPDIR implementation with external stakeholders. MPC reports this initiative to the National Development Planning Committee (NPDC) and the Chief Secretary to the Government.

MPC has subsequently published a number of documents to support the Policy's implementation. These include the Best Practice Regulation Handbook, Quick Reference Best Practice Regulation Handbook, Guideline on Public Consultation Procedures and Guide to Reducing Unnecessary Regulatory Burdens.

Over the last decade decision-making in public administration has increasingly been characterised as an exercise in "handling risk". A consequence of this is that public decision makers are now thinking in terms of risk, and utilising techniques of risk management and risk assessment. Numerous regulatory reform programmes are promoting an even greater emphasis on these and associated "risk concepts".

The speed at which risk and associated concepts have become central features of administrative decision making is unprecedented. Likewise, these concepts are now being embraced in public administration across many different jurisdictions.

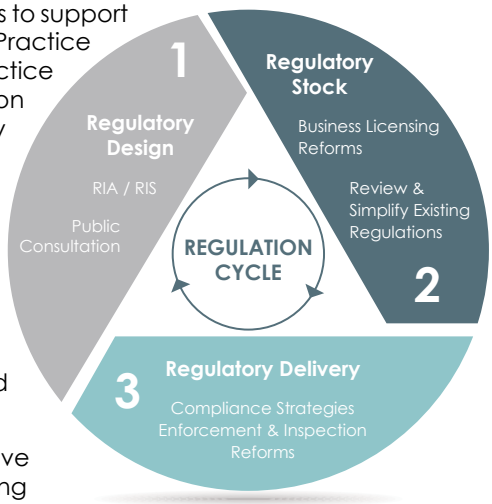


Figure 1.1: Regulation Cycle

1.1 NATIONAL POLICY ON THE DEVELOPMENT AND IMPLEMENTATION OF REGULATIONS (NPDIR).

The Government, under the Tenth Malaysia Plan, in response to increasing global competition, intensified its regulatory reform efforts by entrusting MPC with the responsibilities to undertake improvements to the regulatory environment by, among others, reviewing existing regulations with a view to removing unnecessary rules and compliance costs and undertaking cost-benefit analysis of new policies and regulations to assess the impact on the economy.

MPC has since undertaken several initiatives under its Modernising Business Regulations programme to bring changes to the regulatory environment in government.

Prior to NPDIR, rule-making processes are based largely on practices that have evolved over time and have not been consolidated into law or officially issued guideline. There was increasing recognition that over-regulation, poorly designed regulations and in some cases under-regulation leading to regulatory failures that undermine the intentions of good policies. Global competition, social, economic and technological changes requires government to consider the inter-related impacts of regulatory regimes, to ensure that regulatory structures and processes continue to be relevant, robust, transparent, accountable and forward-looking.

The absence of an official guideline has on occasion created gaps in the rule-making process resulting in ineffective regulations and unnecessary regulatory burdens on businesses. Thus, the introduction of NPDIR which adopted the best practices in OECD countries.

The goal of good regulatory policy is to achieve coherence, effectiveness, efficiency and accountability in the rule-making and implementation process. This is an essential part for realizing several of the policy objectives of the New Economic Model (NEM) that include:

a) Removal of barriers and reduce cost of doing business;

b) Improvement in decision-making for policy implementation; and

c) Improvement in economic efficiency through enabling fair competition.

1.1.1 Key Principles and Mechanisms of the NPDIR

NPDIR guides the development of good regulations, which is essential in achieving the NEM policy objectives. It sets out core principles that authorities should adhere to and mandated the steps to be taken to put the principles into practice. It will also seek to eliminate or reduce cumbersome and inappropriate bureaucratic procedures that affect the cost of doing business.

The NPDIR sets out the policy and principles for the management of the regulation cycle through the Quality Regulatory Management System (QRMS) as illustrated in Figure 1.2. The QRMS introduces the role of the National Development Planning Committee (NDPC) as the oversight body for assessment of compliance to GRP as outlined in NPDIR. NDPC is a high-level planning coordination committee chaired by the Chief Secretary to the Government.

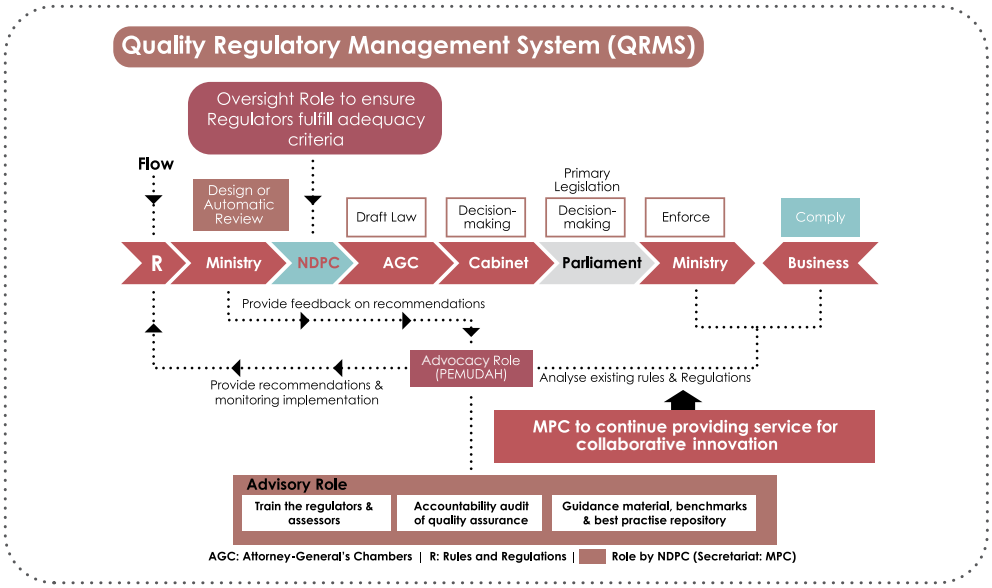


Figure 1.2: Quality Regulatory Management System (QRMS)

The NPDIR also requires that regulators review all regulations once every 5 years. The review plan should take into account the nature of the regulation and its performance. Five-yearly reviews will be published on MPC's online RIS repository.

MPC will publish regulatory annual report on regulatory activities undertaken by Federal Government regulators. It will provide an assessment of the progress made in the implementation of NPDIR. MPC will request each agency to the list of all regulations made during the previous year and the office will review these regulations to determine progress in the adoption of NPDIR. Regulators need to communicate their regulation review schedule and strategies for the year to MPC in January each year.

MPC shall initiate a review of the NPDIR after 5 years or earlier if the need arises. The review will take into account successes achieved, constraints encountered in implementation over the 5-year period, the changes in national priorities in international business environment and the impact of other national policies that have direct relationship with this policy.

1.1.2 Key Requirements in the NPDIR

NPDIR requirements apply to all federal government regulators and are confined to regulations that relate to or impact on business, investment and trade. Every regulator should appoint a Regulatory Coordinator and notify MPC to ensure development of regulations meet the Regulatory Process Management Requirements in the NPDIR.

A critical requirement of NPDIR is to undertake Regulatory Impact Analysis (RIA) and the preparation of regulatory impact statement (RIS) in regulatory development. Regulators are required to submit the RIS to policy makers for their decision-making. Before submission to the decision makers, the RIS has to be submitted for adequacy assessment by NDPC. MPC serves as the technical secretariat that assesses the adequacy of the RIS prior to its submission to NDPC.

1.2 REDUCING UNNCECESSARY REGULATORY BURDENS (RURB)

As part of the government's regulatory reform to promote enterprise growth, wealth and employment, two key initiatives are undertaken:

i) impact analysis for new regulations under National Policy Development Council (NPDC) and

ii) review of existing regulations under Special Task Force to Facilitate Business (PEMUDAH)

MPC functions as the secretariat for both NPDC and PEMUDAH and reports on the outcomes of both RIA and RURB activities.

RURB has been initiated as a comprehensive set of reviews of the current business regulations, focusing on the 12 National Key Economic Areas (NKEAs). The intended outcome is reduce regulatory costs of doing business, help improve the business climate that support economic growth. In working towards these outcomes, regulations that efficiently contribute to national objectives will be maintained, while redundant, unnecessarily burdensome and outdated regulations and rules will be removed or modified.

One of the six core principles for assessing regulation and its administration under the RURB is having a proportionate and targeted response to the risk being addressed. Written regulation, which reflects a rational approach to risk, focuses on the sources of risk, provides instruments which will address them effectively without putting heavy requirements on business unless the size and severity of the impact is large enough to justify this. A well-designed regulation from risk perspectives will facilitate smooth implementation, enforcement and monitoring of regulations. Risk based enforcement tools can be developed more cohesively.

A key element of accountability by a regulator is in the quality of administration and enforcement of regulation. Using risk analysis to identify areas of intrinsically potential high adverse impacts and/or possible low compliance is an indicator of good quality implementation of regulation. Regulators should apply systematic framework that prioritizes the deployment of its scarce resources based on evidence derived from risk assessment.

In particular, a risk based approach in RURB would identify unnecessary regulatory burdens arising from:

- excessive coverage by a regulation that affects economic activities beyond its intended objectives
- subject-specific regulations that duplicate generic ones
- prescriptive regulation that limits flexibility and innovation
- overly complex regulation
- unwieldly license application and approval processes
- requests to provide more information that necessary or repetitive ones
- overlap or conflict in the activities of different regulators
- Inconsistent application or interpretation of regulation.

However, from a practical viewpoint, it is challenging to apply risk analysis to gauge likelihood and consequences to determine if a regulation is 'excessive', 'unwieldly' or even 'prescriptive' before classifying it as a regulatory burden that needs to be addressed.
As such, developing risk measurement criteria should be carefully considered to make possible sensory of data source, develop analytics and basis to derive a certain criterion. These criteria can be used as range limits to trigger a red flag or for mere sample selection.

1.3 ENFORCEMENT AND INSPECTION

Ensuring effective compliance with rules and regulations is an important for a well-functioning society and trust in government. It is a major element in safeguarding health and safety, protecting the environment, securing stable state revenue and delivering other essential public goals. This is critically important from a social perspective and as a foundation of economic growth. The challenge for governments is to develop and apply enforcement strategies for the best possible outcomes by achieving the highest possible levels of compliance, while keeping the costs and burden as low as possible.

Inspection is an important tool used by enforcement authorities to implement regulation and can be a key source for evaluation and information on whether a particular regulation is actually effective (ex-post evaluation). "Enforcement" is a broader term than inspections as it includes all types of controls conducted by regulatory agencies and their potential follow up measures (sanctions, prosecution etc.) as well as activities of law-enforcement bodies that are not primarily "business regulators" (e.g. the police, prosecutors etc.). Enforcement actions are applied as necessary by the regulators in the event of deviations or non-compliance with regulation.

The UK adopts a statutory Regulator's Compliance Code based on Hampton principles that prescribed that inspections should only be performed following a risk assessment, so that resources are focused on those least likely to comply and that has the biggest impact.
Successfully improving the inspections and enforcement system requires regulators to address a number of issues, such as:

a) Institutional overlaps and structures, clarifying which agency should deal with which type of risk, and reducing duplication and overheads;

b) Roles and responsibilities of national and local jurisdictions, combining flexibility and responsiveness with coherence and consistency;

c) Risk-focus in resource allocation, planning and implementation of inspection visits – relying on a comprehensive and up-to-date information system;

d) Transparency of requirements and clear guidance, allowing businesses to know what is expected of them, and what they can expect from inspectors.

The main challenge for regulators moving to risk-based approach is changing the culture and skills of inspectors. Four key issues emerged with respect to inspections:

- the training and re-skilling of inspectors; how to avoid false positives;
- how to balance a focus on outcomes with a focus on compliance; and
- how to manage risk-based inspection systems in a federal inspection structure.

1.3.1 Training and re-skilling of inspectors

Risk-based frameworks have significant implications for inspectors and the inspection function. The shift to a risk-based approach often requires a fundamental change in culture, a different analytical approach, a different understanding of the role of inspectors and supervisory staff, and a new skill set.

By its very nature, risk-based frameworks help regulators to prioritize and minimize scope for inspectors' discretion in determining how to plan inspections, who to inspect, and what to inspect for.

Regulators who have operated a risk-based framework for some years, need to avoid a "tick box" mind-set. Adequate training is required for inspectors particularly in the whole philosophy of risk-based inspection and enforcement.

1.3.2 How to balance focus between outcomes and focus on compliance

Regulators are often charged with implementing an existing set of legal requirements which are not outcome focused, and which they are unable to change. It may well be that breach of a particular requirement does not affect the risk or outcome. The fact that there is a conundrum suggests the

rule should be re-written if not removed, but often it is not within the regulator's power to make these changes. Leaving a number of breaches unsanctioned can reduce the credibility of the regulatory regime as a whole.

1.3.3 Federal inspection systems

The extent to which the federal regulator, in non-federal systems, influence what happens at a state level varies with the constitutional and political context. Co-ordination problems are clearly exacerbated where the federal regulator exerts little control. However, even in systems where the federal regulator does have powers over the inspection processes of state authorities, there are problems with the co-ordination of inspections and consistency in risk assessments. The result is that inspections and the regulatory priorities are not integrated. Similar problems arise across regulators with a large number of regionally dispersed inspectors.

The vital role that inspections play for improving policy development in regulatory governance cycle is illustrated in Figure 1.3

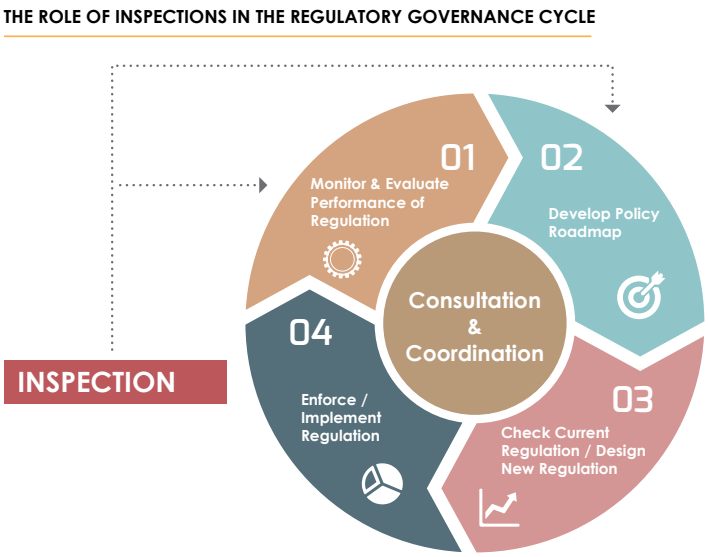


Figure 1.3:
The Role of Inspection in the Regulatory Governance Cycle

The challenge in risk analysis is to gauge the consequence on non-compliance and the failure to comply, that is to determine whether the regulation is "leastly likely to comply" or "carries the biggest spill-over impact" in targeting inspection.

As such, developing risk measurement should be carefully considered to enable the creation of data source, development of analytics and providing basis for determining decision criteria. These criteria can then be used to identify high-risk subjects or for determining sampling plans. Such risk identification and detection mechanisms are crucial for a good risk management process.

CHAPTER 2

OVERVIEW OF RISK MANAGEMENT IN GOVERNMENT REGULATORY CYCLE

2.0 PRELIMINARY

This publication aims to assist regulators to develop coherent frameworks for the application of risk management in regulatory inspection and enforcement. The chapters are developed based on MS ISO 31000:2010 (Risk Management Principles and Guidelines) concepts, covering a series of topics including: risk management; modelling risk identification, analysis and evaluation; design of innovative approaches to respond and treat risks; the monitoring and communication of risks; and the salient features of NPDIR that apply risk management.

Greater emphasis on risk-based approaches to the design of regulation and compliance strategies can reduce costs for business and reduce the opportunity costs of government action.Accordingly, regulators will require compatible methodologies for sectoral risk assessments to compare risks and prioritise enforcements on the basis of their relative efficiency.

It is important to account for relevant information in the application of risk-based regulatory enforcement, by favouring flexible approaches, creating linkages with information collection and innovation agendas, and planning revisions based on updated assessments.

MPC will take stock of national practices in the handling of informational gaps in risk- based regulatory inspections, with attention to institutional design (framework) and to pro-active interactions between regulators and business communities.

2.1 GENERAL RISK CRITERIA IN REGULATORY DELIVERY

All enforcement activities should adopt risk-based analysis and approaches. Criteria for inspection and enforcement should be based on these considerations:

- Impact factor of a regulation on a sector/sub-sector from the RIA
- Size (or other profiling metrics) of the inspection prospect, prioritised into different sample plans, e.g. larger sample size for larger outcomes.
- Likelihood of non-compliance according to sector/company
- a random sampling for those not selected above.

Adequate information for statistical analysis is required to carry out risk management activities. Adequate resources should be allocated for risk management activities.

2.2 KEY COMPONENTS OF RISK MANAGEMENT

Risk refers to the uncertainty that surrounds future events and outcomes. It is the expression of the likelihood and impact of an event with the potential to influence the achievement of an organization's objectives.

Risk management contains three key components:

- Risk Management Principles – overall objectives and commitment at the top management of the regulatory body;
- Risk Management Framework – the decision and communication structure organized to effectively detect, respond and monitor risks
- Risk Management Process - techniques that inspection and enforcement planners, managers and field officers should be adept with.

The relationship between these three elements is depicted in the Figure 2.1 below:

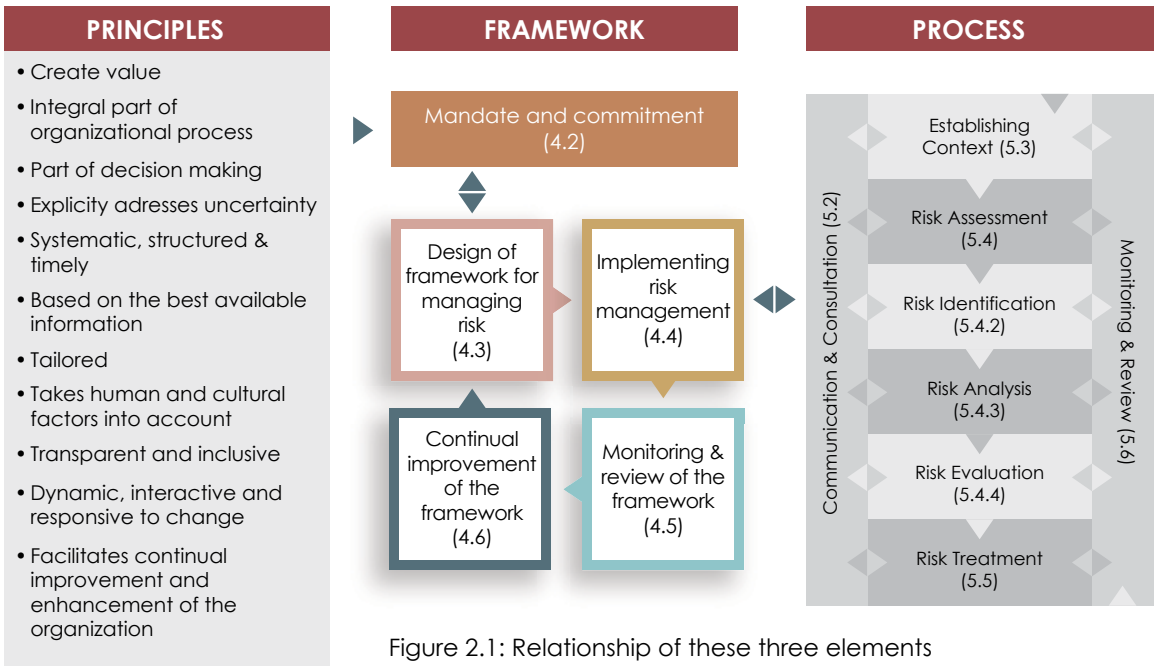


Figure 2.1: Relationship of these three elements

With proper design and implementation, risk management enables the inspection and enforcement function to more focused, targeted and increased likelihood of meeting policy objectives.

2.3 APPLICATION OF RISK MANAGEMENT IN NPDIR

The NPDIR has a set of requirements articulated in the Best Practice Regulation Handbook that carry risk management features. Examples of risk management processes that can be applied in the execution of NPDIR to control/reduce implementation risks are as follows (Table 2.1):

ISO 31000	Best Practice Regulation Handbook	Areas Relevant for Risk Management Application
Communication and consultation	4.5 Consultation 4.7 Strategy for Implementation	• Engagement of the public and consultation with government and internal peers for better information, public relations and buy-in • The communication plan to involve all affected parties
Establishing the context	4.1 Problem / Issue Statement	• Present magnitude of the problem from external and internal context perspectives • Identify stakeholders community
Risk assessment • Risk identification • Risk analysis • Risk evaluation	4.1 Problem / Issue Statement 4.3.1 Risk Assessment 4.4 Impact Analysis	• Summary of risk assessment and justify why government intervention is needed • Explain and quantify risks • Assessment on the expected impact (cost and benefits) of each feasible option
Risk treatment	Problem / Issue Statement 4.3 Instrument Options 4.3.2 Identifying Feasible Options 4.6 Conclusion and Recommendation 4.7 Strategy for Implementation	• Demonstrate why government intervention is needed • Describe each regulatory / non- regulatory option and the key differences between the options in achieving the desired results • Test the effectiveness and appropriateness of alternative regulatory instruments • A clear statement identifying the preferred option based on the impact analysis supported by the preceding analysis and a comparison with other options • The mechanism adopted to ensure compliance • The methods to detect non-compliance • The penalty for non-compliance

Monitor and review	4.4.8 Enforcement and Compliance	• Assessment of the likely impact of different enforcement methods • Aministrative methods of preventive control, e.g.: licensing, registration and enforcement • Approaches including warning notices, suspension notices and prohibition notices
	4.7.1 Review	• Outline about how the regulation will be reviewed
	6.1 Publication of Regulatory Annual Report	• Regulatory annual report on regulatory activities undertaken by federal Government regulators will be published • All regulations made in the previous year will be reviewed and progress in the adoption of NPDIR will be determind

For more effective implementation of risk-based analysis on enforcement and inspection function, regulators first need to risk assessments on the regulatory development process. For example, stakeholders' lists of the proposed regulated community should be profiled according to the magnitude of impact on for example, revenue, production volume or number of employees, to enable segmentation and stratification for targeting inspection.

CHAPTER 3

BENEFITS AND CHALLENGES OF RISK MANAGEMENT IN REGULATORY CYCLE

3.0 PRELIMINARY

At the level of regulatory agencies the potential benefits of a risk-based approach to regulation come from a more efficient resource use through resources being applied to highest risk issues and the equal treatment of like risks. Whether or not they are made transparent, decisions about risk are always being made by regulators. Even in the case of the most subjective of risk judgements, a transparent risk assessment process will reveal opportunities for measuring and refining the implicit assumptions that are held by regulators and inherent in the regulation of risks

This is particularly relevant to stakeholder management by multi-sector regulators. Multi-sector regulators have to make judgements about which issues to give greatest attention and priority to in circumstances where not all policy problems within the regulator's domain will necessarily require equal or like treatment. (OECD 2010, Chap.1 p 25)

Risk assessment provides a basis for regulatory agencies to communicate and consult with the public and within government as to how they are going to allocate their limited resources to ensure maximum public benefit. In this way it can contribute to building trust in government institutions and regulatory authorities through the transparent substantiation of the legitimacy of agencies and their role in regulation. (OECD 2010, Chap.1 p 25)

A risk-based approach can also assist in measuring performance and building accountability within agencies. Risk analysis relies on a transparent process for analysing alternative decisions in the face of risk and uncertainty. Rather than simply rewarding (or punishing) the performance of government agencies for outcomes which may be unrelated to their actions, a risk-based approach can reveal the sources of success and failure in the processes of regulatory decision making. This in turn can feed back into improvements to the rigour of future decision making processes through ex post evaluation of the regulatory responses. (OECD 2010, Chap.1 p 25)

The careful allocation of responsibility for risk management has the potential to produce greater economic benefits by allowing risks to be managed at the level of society where it will be most effective. This can include reducing unnecessary reliance on government involvement in individual's lives, thereby building a more resilient society and allowing opportunities for adaptive behaviour. Regulation has to be examined for its potential to displace entrepreneurial activity which can potentially address risks and minimise negative externalities more effectively through the development of private or market based solutions. (OECD 2010, Chap.1 p 25)

One of the most essential tasks of government is to manage risk on behalf of the public, where risk is simply the chance of an adverse outcome. The "adverse outcome" may concern financial wellbeing, human health, safety, environmental quality or even national security. Of particular concern are new, emerging risks that are unfamiliar to government.

The common challenge is to manage risk wisely in settings where risks are often poorly identified and quantified, where enlightened value judgments about optimal risk taking are disputed, and where well-intentioned policies aimed at curbing one risk may inadvertently create other risks (McDaniels

and Small, 2004). Since knowledge about risks changes over time, often slowly and sometimes rapidly, a common challenge is to make wise decisions in a dynamic context where flexibility is needed to account for new information.

3.1 RISK-BASED ANALYSIS ON ENFORCEMENT AND INSPECTION

Risk-based Analysis on Enforcement and Inspection ("RBAEI") relates to the interface of risk management with regulatory management system. It is concerned with how the regulator organises itself to deal with risk issues when considering regulatory enforcement and inspection. This helps to better align enforcement targets with policy objectives, improve the development of regulatory capacity, build and maintain public trust, and to improve the efficiency of government operations.

A key aspect relevant to the promotion of risk-based approach is the decision-making feature of that regulators. Regulatory Coordinators and oversight bodies can use to promote a consistent approach across the regulatory process management. It can improve the design and enforcement of regulations.

The role of regulators is important because of the autonomy that regulators exercise in the design, administration and enforcement of regulation. The process that regulators engage in influences both the shape of regulation, and the substantive compliance costs and administrative costs imposed on business and citizens.

Figure 3.1:

Scenario likelihood & Impact Incidents

Regulators are also responsible for the overall effectiveness of the implementation of regulatory initiatives. The implementation of risk-based approach is concerned with understanding how regulatory authorities put into operation methods and processes to achieve their regulatory goals and monitor how successful these initiatives are in practice. This latter aspect is important because the experiences of one regulator can be learning for another regulator. This may also apply to other regulators operating within another sector in the same jurisdiction, or in the same sector in a different jurisdiction.

A significant objective of incorporating a better treatment of risk in regulatory enforcement and inspection is to improve regulatory design and administration, to reduce the fiscal costs of administering regulation and minimise the burden on business and the community.

A focus on risk then has the potential to improve the design and operation of government activities. In the public-sector risk, defined as the potential failure to achieve objectives or deliver public services, is analogous in some ways to the risk to profitability of the private sector risk management. This focus on risk is emerging as the basis upon which public organisations, which are not otherwise subject to

the disciplines of competition, profitability and share values, can self-challenge and improve their own management practices.

3.2 CHALLENGES OF RBAEI

Risk based Analysis on Enforcement and Inspection has two related dimensions which may be in conflict:

- managing the regulators' risks associated with delivering overall regulatory objectives, as well as;
- managing targeted and proportionate compliance and enforcement responses commensurate to the regulated community.

As many regulatory initiatives depend upon the co-ordination of the roles of a number of regulatory bodies, blame avoidance behaviour by a single or dominant regulator can have wider systemic effects across government.

The identification of these issues underscores the need for guidance on the enforcement and inspection strategies to anticipate the potential pitfalls using risk-based approach. The above analysis points to some of the potential problems of a risk-based approach and to their solutions. The counterfactual to be considered is the extent to which agencies would be better at achieving their policy goals in the absence of a push for greater transparency and accountability in risk-based approaches.

One area where this is already being addressed by a few OECD countries is the development of risk assessment tools and the documentation of risk assessment in the preparation of regulatory impact analysis (RIA). A few countries including Malaysia require risk assessment to be included in RIA, but there is scope for improving the guidance that is available to regulators to do this.

The issues which to be addressed for improvement include:

- Guidance on methodologies for undertaking Risk Assessment including analytical techniques and sources of information.
- Guidance on the identification of acceptable risk thresholds (for example common approaches to the statistical valuation of human life across different regulatory sectors).
- Guidance on the identification and assessment of subjective versus objective risks.
- Guidance on the use of the precautionary principle in Regulatory Impact Analysis.
- Practices for promoting the use of independent rigorous scientific advice and peer review.
- Strategies for consultation and communication with the public on risk issues.

The potential for risk-based approach to impose a paperwork burden on the regulated sector should be noted. As risk-based decision making relies on an assessment of the probabilities of harm and the likelihood of non-compliance the regulator has to have access to a substantive knowledge on the regulated sector.

Risk-based regulators may move from broad directive regulation action to a more tailored arrangements which rely more heavily upon the internal risk management systems of the regulated firm. For this the regulator engages in information gathering from regulated entities until a solid body of evidence is collected. This creates a tension between the need to obtain information from regulated entities and the use of directive regulation to reduce the administrative burden of compliance costs.

Given these challenges in administering transparent risk-based approaches, there is the need for guidance on the incorporation of risk management in the design of regulatory enforcement strategies and risk communication to maintain the effectiveness of regulators. The benefits from this guidance to achieve more effective and responsive regulation and regulatory institutions.

In summary, the regulatory management challenge for the government seeking to improve the governance of risk is to promote evidence-base regulatory regimes. To provide an adequate prescription for regulators, the following elements will be crucial in designing better approaches to assessing and managing risk.

- Put systems in place with sound scientific analysis for the estimation of risks – This requires processes to obtain scientific information and to use this information to evaluate the extent of regulatory problems. Ensuring the accuracy of scientific evidence depends upon having open and transparent processes for the formulation and collection of scientific evidence with independent criticism and peer review of scientific claims.

- Set regulatory priorities taking account of risks – An overall risk programme should be developed based on an examination of significant risks. An agenda should be set for regulatory enforcement, identifying the policy priorities and how it is proposed to respond to these based on the weight of evidence. Associated with this would be the establishment of processes for identifying and evaluating possible responses to a crisis.

- Where possible the scoping of regulatory enforcement should be risk-based – Risk-based regulatory strategies are designed to be targeted based on an assessment of the risk that they are intended to address. To achieve this, risk assessment should inform all aspects of the regulatory cycle, through data collection, the selection of regulatory instruments, the scheduling of inspection and the allocation of resources for prosecution. The use of cost benefit assessment can identify opportunities for increasing net welfare by introducing better regulation as well as reveal cases of over regulation. Creative and flexible regulatory approaches to achieve regulatory objectives may deliver better outcomes than traditional approaches.

- Examine policy enforcement programs for their potential risk-risk trade-offs – Efforts to bring about a reduction of risks in one policy area can inadvertently give rise to an increase of risk in another policy area. The instrumentalist and compartmentalised nature of governments can result in too narrow a consideration of the consequences of policy. A failure to consider the interconnected

nature of government activities and public value objectives can result in the unexpected transference of risk across government. This results in the full costs of regulation not being properly considered and overlooks the potentially creative opportunities for "joined up" policy solutions.

- The design of enforcement and inspection structure can encourage innovation – Policy settings should be cognisant that risk taking is a source of creative innovation in society; risk can have negative consequences but it can also produce rewards. Government is recognising that it is not always best placed to manage risks and to be cautious about regulating to remove opportunities for informed risk-taking by citizens, and which may also depress opportunities for innovation. A considered approach to risk is also a key source of innovation within the public sector.

- Incorporate communication in all aspects of the policy cycle – An increased focus on risk-based regulation increases the challenges for regulators to establish and maintain effective communication with stakeholders. Risk communication is an integral part of the risk assessment and management framework, both for collecting evidence and building support for the basis of inspection selection.

CHAPTER 4

RISK MANAGEMENT PRINCIPLES

4.0 PRELIMINARY

Risk management principles set the direction, the tone at the top in the inspection and enforcement hierarchy. It improves governance, increases the likelihood of achieving objectives, establish reliable basis, organizational learning and effective allocation of resources.

4.1 RISK MANAGEMENT PRINCIPLES IN INSPECTION AND ENFORCEMENT

The following are principles of risk management in the regulatory inspection and enforcement function:

	PRINCIPLES
a.	Create value
b.	Integral part of organizational processes
c.	Part of decision making
d.	Explicitly addresses uncertainty
e.	Systematic, structured & timely
f.	Based on the best available information
g.	Tailored
h.	Takes human and cultural factors into account
i.	Transparent and inclusive
j.	Dynamic, interactive and responsive to change
k.	Facilitates continual improvement and enhancement of the organization

- Create Value (a): Inspectors/ enforcers should recognise that their activity exist to allow, or even encourage, economic progress and that the regulation in question was created when there was a clear case for protection. Inspection and enforcement should be an integral of overall value creation in the regulatory process.

- Integral part of organisation (b): the inspection and enforcement system as a whole, should apply risk assessment methods to concentrate resources in the areas that need them most. It should be systematic, structured and timely to explicitly address uncertainty.

- Decision-making (c): Regulators should provide authoritative, accessible advice easily and cheaply to the prospects, taking into account human and cultural factors.

- Address uncertainty (d): No inspection should take place without reason. It should be based on best available information and if needed, tailored to the prospect.

- Systematic, structured and timely (e): Businesses should not give unnecessary information or give the same piece of information twice. Regulators should strive for continuous improvement and enhancement in the inspection and enforcement process.

- Proportionate and responsive : Regulators should be decisive; few businesses that persistently break regulations should be identified quickly and face proportionate and meaningful sanctions.

- Tansparent & inclusive: Regulators should be accountable for the efficiency and effectiveness of their activities, while remaining independent, transparent and inclusive in the decisions they take.

Enforcement officers and their management need to recognize and establish mechanisms to assess risk and direct resources accordingly. A number of common challenges faced by regulators include development of assessment and evaluation criteria to deal with a wide range of risks. The role of Regulatory Coordinators and MPC comes into play where considerable value can be derived from knowledge sharing across ministries and agencies.

CHAPTER 5

RISK MANAGEMENT FRAMEWORK

5.0 PRELIMINARY

When managing risks of interest involves more than one department or jurisdiction of the Federal Government, it is essential for the government to devise mechanisms for participation and collaboration by the multiple departments, including procedures for co-ordination and dispute resolution.

Emerging risk issues are often of interest to more than one department in the Federal Government. Climate change may be of concern to energy departments as well as environmental ministries. A food safety scare may draw the attention of agriculture departments as well as regulatory agencies responsible for food safety. Many national governments have multiple departments engaged in the regulation of different financial sectors of the economy.

In order to ensure informed and co-ordinated management of risk, the leadership of national government needs to put into place procedures to ensure that information and views are elicited from all involved departments. When there is conflict in policy objectives a central unit in national government needs to take responsibility on dispute resolution and co-ordination of all resulting policies. Although the need for cross-department co-ordination is evident in many policy areas, the challenge is more complex on risk issues because of the wide range of scientific disciplines and departmental constituencies that may be involved.

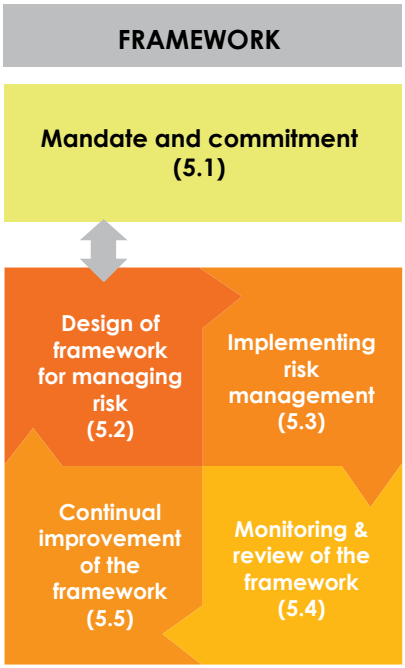


Figure 5.1:

The Management Framework (MS/ISO31000)

The success of risk management therefore will significantly depend on the framework that provides the structural foundations and arrangements that will be embedded at all levels. The framework serves as the communication channel for sensory/indicator functions, systematic dissemination of information from bottom upward and decision making from top downward. An integrated 'organizational structure' of risk management will be needed for which the MS/ISO 31000 will be useful guidance.

It is important that risk principles and objectives are communicated at all levels of decision making in regulatory enforcement function – from strategic prioritization of resources to premise-based targeting and proportionate sanctioning regimes. Governments should ensure that a consistent definition of risk is used throughout all inspectorates, and that it forms the basis for allocation of resources and for enforcement approaches. Such risk-analysis should be used at all steps of the regulatory process – when designing regulation, enforcing it, and evaluating it.

It is particularly important at the enforcement stage, because it is physically impossible for government to inspect every business as it would result in massive and unnecessary administrative burden that does not commensurate with achieving objectives. Thus, prioritisation in inspection and enforcement actions is imperative and as such regulators should ensure that risk criteria, indicators, limits, methodologies and technical processes are properly implemented.

The framework ensures that information about risk derived from the risk management process is adequately reported and used as a basis for decision making and accountability at all relevant organizational levels.

Figure 4 above describes the necessary components of the framework for managing risk and the way in which they interrelate in an iterative manner.

5.1 MANDATE AND COMMITMENT

The introduction of risk management and ensuring its ongoing effectiveness require strong and sustained commitment by management of regulators, as well as strategic and rigorous planning to achieve commitment at all levels. Management should:

a) establish a RBAEI policy;

b) ensure that the regulator's culture and RBAEI policy are aligned;

c) determine risk management performance indicators that align with performance indicators of the organization;

d) align risk management objectives with the objectives and strategies of the organization;

e) promote compliance

f) assign accountabilities and responsibilities at appropriate levels within the organization;

g) ensure that the necessary resources are allocated to risk management;

h) communicate the benefits of RBAEI to all stakeholders; and

i) ensure that the framework for managing risk is maintained.

5.2 DESIGN OF FRAMEWORK FOR MANAGING RISK

In design of framework for managing risk, there are six components; including understanding of the organization and its context, establishing risk management policy, accountability, integration into organizational processes, resources, establishing internal communication and reporting mechanisms including for external communication and reporting. Further description is as bellow.

5.2.1 Understanding of the Organization and its Context

In the design of the framework for RBAEI , it is important to evaluate and understand both the external and internal context of the organisation, since these can significantly influence the implementation of the framework. Evaluating the organisation's external context may include, but is not limited to:

a) the social and cultural, political, legal, financial, technological, economic, natural and competitive environment, international, national, regional and local environment;

b) key drivers and trends impacting on the objectives of the regulator and regulated community;

c) relationships with and perceptions and values of external stakeholders.

5.2.2 Establishing Risk Management Policy

The risk management policy should clearly state the regulators objectives for, and commitment to, risk management and typically addresses the following:

a) the rationale for RBAEI;

b) links between the regulator's policies and the RBAEI;

c) accountabilities and responsibilities for managing risk;

d) dealing with conflicting interests;

e) commitment of resources to those accountable and responsible for managing risk;

f) meassuring and reporting risk management performance;

g) review and improvement of the risk management policy and framework continually in response to environmental changes.

5.2.3 Accountability

Regulators should ensure that there is accountability, authority and appropriate competence for managing risk, including implementing and maintaining the RBAEI process and ensuring the adequacy, effectiveness and efficiency of any controls. This can be facilitated by:

5.2.4 Integration into Organizational Process

Risk management should be embedded in all the organization's practices and processes in a way that it is relevant, effective and efficient. The risk management process should become part of, and not separate from, those organizational processes. In particular, risk management should be embedded into the policy development, business and strategic planning and review, and change management processes.

There should be an organization-wide risk management plan to ensure that the risk management policy is implemented and that risk management is embedded in all of the organization's practices and processes. The risk management plan can be integrated into other organizational plans, such as a strategic plan.

5.2.5 Resources

The organization should allocate appropriate resources for risk management. Consideration should be given to the following:

a) people, skills, experience and competence;

b) resources needed for each step of the risk management process;

c) the organization's processes, methods and tools to be used for managing risk;

d) documented processes and procedures;

e) information and knowledge management systems; and

f) training programs

5.2.6 Establishing Internal Communication and Reporting Mechanisms

The regulator should establish internal communication and reporting mechanisms in order to support and encourage accountability and ownership of risk management processes. These mechanisms should ensure that:

a) key components of the RBAEI framework, and any subsequent changes, are communicated appropriately;

b) there is adequate internal reporting on the framework, its effectiveness and the outcomes;

c) relevant information derived from the application of risk management is available at appropriate levels and times; and

d) there are processes for consultation with internal stakeholders.

These mechanisms should, where appropriate, include processes to consolidate risk information from a variety of sources, and may need to consider the sensitivity of the information.

5.3 IMPLEMENTING RISK MANAGEMENT

5.3.1 In implementing the risk management framework for managing enforcement and inspection, the regulator should:

- define the strategy for implementing the framework;
- apply the RBAEI policy and process into the management system;
- comply with regulatory requirements;
- ensure that decision making, including the development and setting of objectives, is aligned with the outcomes of risk management processes;
- maintain information and training sessions; and
- communicate and consult with stakeholders to ensure that its risk management framework remains appropriate.

RBAEI should be implemented by ensuring that the risk management process outlined later in Chapter 6 is applied through a risk management plan at all relevant levels and functions of the organization as part of its practices and processes.

5.4 MONITORING AND REVIEW OF THE FRAMEWORK

In order to ensure that RBAEI is effective and continues to support regulatory performance, the regulator should:

- measure RBAEI performance against indicators, that are periodically reviewed performance level;
- monitor RBAEI progress against the risk management plan;
- periodically review whether the framework, policy and plan are still appropriate, given the organizations' external and internal context;
- report on risk how well the RBAEI policy is being followed; and review the effectiveness of the RBAEI framework.

5.5 CONTINUAL IMPROVEMENT OF THE FRAMEWORK

Based on results of monitoring and reviews, decisions should be made on how the RBAEI framework, policy and plan can be improved. These decisions should lead to improvements in the regulator's management of risk and its risk management culture.

CHAPTER 6

RISK MANAGEMENT PROCESS

6.0 PRELIMINARY

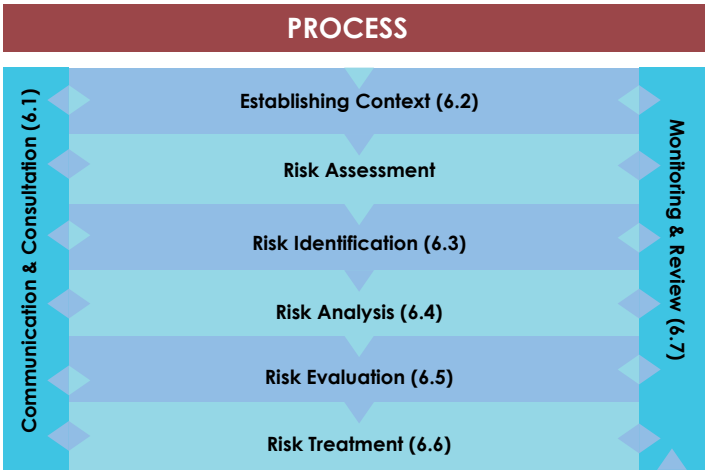


Figure 6.1: Risk Management Process

In the previous process, Risk Analsysis determines two sub-attributes; likelihood and consequences. Independently they may not represent the overall risk attribute because there may be high likelihood risks that carry low impact but when aggregated could exceed low likelihood risks that has high impact. Thus, the need for Risk Evaluation process to gauge the overall severity attribute of the risk.

Risk evaluation combines likelihood and impact/consequences to derive the severity level of the risk. Like in statistics, expected outcome is the product of a value (eg. Ringgit) and the probability of occurrence. Severity levels are stratified to represent the overall scale of the risk. Higher severity will require greater intervention or more immediate treatment. It also sets priority to directly influence allocation of resources to treat them.

The Risk Management Process involves eight key tasks as illustrated in Figure 6.1 above. The tasks are:

- Communication and Consultation (6.1). This should take place with the internal and external stakeholders during all stages of the risk management process. The concept of 'risk communication' is generally defined as an interactive process of exchange management. This applies inside regulatory bodies, departments or units or outside to external stakeholders and the regulated community. Inappropriate communication about risk can lead to a breakdown in trust and/or poor risk management.

- Establishing the Context (6.2) is crucial to understand the applicable scope of the risk management. Establishing the context defines the basic parameters within which risks must be managed and sets the scope for the rest of the risk management process. The context includes the regulator's external and internal environment and the purpose of the risk management activity. Context is the backbone of risk management.

- Risk assessment is the overall process of risk identification (6.3), risk analysis (6.4) and risk evaluation (6.5);

  - Risk identification (6.3) is to develop a comprehensive list of sources of risks and events that might have an impact on the achievement of each of the objectives (or key elements) identified in the context. The list should be comprehensive as unidentified risks can pose a major threat to the regulator or result in significant opportunities being missed.

  - Risk analysis (6.4) is about developing an understanding of the risk. It provides an input to decisions on whether risks need to be treated and the most appropriate and cost-effective risk treatment strategies. Risk analysis involves consideration of the sources of risk, their positive and negative consequences and the likelihood that those consequences may occur. Factors that affect consequences and likelihood may be identified. Risk is analyzed by combining consequences and their likelihood. In most circumstances, existing controls are considered. A preliminary analysis can be carried out so that similar risks are combined or low-impact risks are excluded from detailed study. Excluded risks should, where possible, be listed to demonstrate the completeness of the risk analysis.

  - Risk evaluation (6.5) is a process to gauge the overall severity attribute of the risk. Risk evaluation combines likelihood and impact/consequences to derive the severity level of the risk. Like in statistics, expected outcome is the product of a value (eg. Ringgit) and the probability of occurrence. Severity levels are stratified to represent the overall scale of the risk. Higher severity will require greater intervention or more immediate treatment. It also sets priority to directly influence allocation of resources to treat them.

- Risk treatment (6.6) involves selecting one or more options for modifying risks, and implementing those options. It involves identifying the range of options for treating risks, assessing these options and the preparation and implementation of action plans. It will usually not be cost-effective or even desirable to implement all possible risk treatments. It is, however, necessary to choose, priorities and implement the most appropriate combination of risk treatments. Treatment of individual risks will seldom occur in isolation and should be part of an overall treatment strategy. Having a clear understanding of a complete treatment strategy is important to ensure that critical dependencies and linkages are not compromised.

- Monitoring and review (6.7) should be a planned part of the risk management process and involve regular checking or surveillance. It can be periodic or ad hoc. Factors that may affect the likelihood and consequences of an outcome may change, as many the factors that affect the suitability or cost of the treatment options. It is therefore necessary to repeat the risk management cycle regularly. Actual progress against risk treatment plans provide an important performance measure and should be incorporated into the regulator's performance management, measurement and reporting system

6.1 COMMUNICATION AND CONSULTATION

Communication and consultation with external and internal stakeholders should take place during all stages of the risk management process. Plans for communication and consultation should be developed at an early stage. [example: In the initial planning stage of the RIA initiative, stakeholders analysis is carried out to identify and prioritise important and influential stakeholders for consultations during the regulation development process….]

Effective external and internal communication and consultation should take place to ensure that those accountable for implementing the risk management process and stakeholders understand the basis on which decisions are made, and the reasons why particular actions are required.

A consultative team approach may:

- help establish the context appropriately;
- ensure that the interests of stakeholders are understood and considered;
- help ensure that risks are adequately identified;
- bring different areas of expertise together for analyzing risks;
- ensure that different views are appropriately considered when defining risk criteria and in evaluating risks;
- secure endorsement and support for a treatment plan;
- enhance appropriate change management during the risk management process; and
- develop an appropriate external and internal communication and consultation plan.

Communication and consultation with stakeholders is important as perceptions can vary due to differences in values, needs, assumptions, concepts and concerns of stakeholders. As their views can have a significant impact on the decisions made, the stakeholders' perceptions should be identified, recorded, and taken into account in the decision-making process.

6.2 ESTABLISH THE CONTEXT

Understanding the external context is important to ensure that the objectives and concerns of external stakeholders are considered when developing risk criteria. The external context can include social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local; key drivers and trends having impact on the objectives of the regulation should also be taken into consideration.

The internal context is the internal environment in which the regulator seeks to achieve its objectives. This can include governance, organizational structure, culture; policies, objectives, and the strategies that are in place to achieve them; capabilities in terms of resources and knowledge and information systems, information flows and decision-making processes.
The following are factors that may trigger a regulator to initiate a regulatory risk review (Table 6.1):

Influencing Factors for Regulatory Risk Review	
External Context	**Internal Context**
Political • Leadership changes • Political Strife • Regional spillovers • Terrorism • Public perception shift • Media • External pressures	Infrastructure/Resources • Fiscal budget policy • Physical facilities • Political empowerment • Boundary of authority • Access to government leadership • Government peer relationships • Public-private partnership structure • Media Access
Economic • Capital movement • Credit ratings • Sectorial concentration • Money and market liquidity • Inflation • Unemployment • Regional competition • Price sensitivities	Talent • Knowledge capacity • Productivity • Learning capabilities • Organizational culture • Accountability and responsibility • Decision making
Social • Demographics • Cultural shifts • Public sentiments • Social media • Privacy • Health and diseases • Human rights • Religion	Process • Design (relevance and quality) • Adequacy • Complexity • Dependencies • Traceability • Level of automation
Technological • Internet penetration • Disruptions • Electronic commerce • Electronic government • Big data analytics • Emerging technology • Utilities access	Technology • Information availability • Data integrity • System availability • Social technology changes • Public data • System implementations • Maintenance
Natural Environment • Natural disaster • Sustainable development • Energy • Emissions and waste	•Underutilization/Redundancy
Legal Framework • Regulatory changes • International agreements • Political shifts • Economic reforms	

The context in risk management will involve- establishing the goals, objectives, scope, activities, projects and services of the risk management process. It includes establishing the risk assessment methodologies, the way risk performance is measured, specific decision to be made and any specific or tailored approach required for certain conditions.

Regulators should define criteria to be used to evaluate the significance of risk. When defining risk criteria, factors to be considered should include the following:

- the nature and types of causes and consequences that can occur and how they will be measured;
- the likelihood of occurrence;
- the timeframe(s) of the likelihood and/or consequence(s);
- the level of risk;
- the views of stakeholders;
- the level of acceptance and tolerance range; and
- accounting for combinations of multiple risks and how and which combinations should be considered.

6.3 RISK ASSESSMENT: IDENTIFICATION PROCESS

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation.

Regulators should identify sources of risk, areas of impacts, events and their causes and their potential consequences to generate a comprehensive list of risks based on those events (scenario development) that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives. It is also important to identify the risks associated with not pursuing an opportunity (opportunity costs).

Comprehensive identification is critical, because a risk that is not identified at this stage will not be included in further analysis. Identification should include risks whether or not their source is under the control of the regulatory body, even though the risk source or cause may not be evident. Risk identification should include examination of the knock-on effects of particular consequences, including cascade and cumulative effects. It should also consider a wide range of consequences even if the risk source or cause may not be evident. It is necessary to consider possible causes and scenarios that show what consequences can occur. All significant causes and consequences should be considered.

The regulator should apply risk identification tools and techniques that are suited to its objectives and capabilities, and to the risks faced. Relevant and up-to-date information is important in identifying risks. This should include appropriate background information where possible. People with appropriate knowledge should be involved in identifying risks.

6.4 RISK ASSESSMENT: ANALYSIS PROCESS

Risk analysis involves developing an understanding of the risk, providing an input to risk evaluation and to decisions on whether risks need to be treated, and on the most appropriate risk treatment strategies and methods. Risk analysis can also provide an input into making decisions where choices must be made and the options involve different types and levels of risk.

Risk analysis involves consideration of the causes and sources of risk, their positive and negative consequences, and the likelihood that those consequences can occur. Factors that affect consequences and likelihood should be identified. Risk is analyzed by determining consequences and their likelihood, and other attributes of the risk. An event can have multiple consequences and can affect multiple objectives. Existing controls and their effectiveness and efficiency should also be taken into account.

The way in which consequences and likelihood are expressed and the way in which they are combined to determine a level of risk should reflect the type of risk, the information available and the purpose for which the risk assessment output is to be used. These should all be consistent with the risk criteria. It is also important to consider the interdependence of different risks and their sources.

Risk analysis can be undertaken with varying degrees of detail, depending on the risk, the purpose of the analysis, and the information, data and resources available. Analysis can be qualitative, semi-quantitative or quantitative, or a combination of these, depending on the circumstances.

Consequences and their likelihood can be determined by modelling the outcomes of an event or set of events, or by extrapolation from studies or available data. Consequences can be expressed in terms of tangible and intangible impacts. In some cases, more than one numerical value or descriptor is required to specify consequences and their likelihood for different times, places, groups or situations.

6.4.1 Basis of Analysis

At a strategic level, broad categories of risk are identified and analysed to provide an organizational risk profile that shows important issues for which management systems and risk treatments need to be established. At a project or team level, managers identify and prioritize the specific risks that threaten the objectives they are tasked to achieve.

The organization examines key risks in detail, for the following reasons, which may be quantitative or qualitative

(i) to obtain more information about consequences or likelihood so decisions about priorities are based on information and data rather than guesswork;

(ii) to better understand the risk and its causes so that treatment plans can be directed at true rather than superficial causes of problems;

(iii) where decision criteria require more in-depth analysis (often this is where decision criteria are expressed quantitatively);

(iv) to help people choose between options where each has different costs and benefits and potential opportunities and threats;

(v) to provide an understanding of residual risk after treatment strategies have been applied

6.4.2 Qualitative Analysis

The information is brought together and summarized as single word descriptions of consequence and likelihood to use in a risk ranking table. The underlying information on which the ranking is based is recorded to assist decision makers and support the conclusions drawn.

Qualitative analysis may be used :

a) where quantitative precision is not needed;

b) to perform an initial screening of risks prior to further, more detailed analysis;

c) where the level of risk does not justify the time and resources needed to do a numerical analysis; or

d) where the numerical data are not available or inadequate for a more quantitative analysis.

Even when qualitative analysis is used, best possible use should be made of available information, including quantitative inputs.

6.4.3 Semi-quantitative and quantitative analysis

The level of risk can be calculated using a quantitative method in situations where the consequences and likelihood of occurrence can be quantified. For example, fraud risk assessments may be quantitative where the likelihood can be expressed numerically and the potential impacts are measured in terms of monetary loss.

In many instances, relatively straightforward methods are used effectively, although more refined techniques are sometimes necessary.

(However, even sophisticated quantitative techniques may have their weaknesses and these need to be kept in mind. In particular, the assumptions that underlie the quantitative techniques should be clearly stated and understood).

6.4.4 Measurement and scales

Whatever type of analysis is used, some form of measurement of consequence and likelihood is necessary. The choice of the type of scale used to carry out this measurement is largely dependent upon the nature and range of the consequence and the level of knowledge and variability of the likelihood.

Measurement scales can be characterized as:

a) Nominal - Assigns data into categories.

E.g. Lists or classifications of wildlife, cultural patterns, land use, etc.
Limitation/Freedom:
No mathematical operation can be performed

b) Ordinal - Comparative scales. Can be judged as "more" or "less than…"

E.g. Rankings such as High, Medium, Low or 1, 2, 3, 4, 5 where numerical value does not relate to value or quantity.

Limitation/Freedom:
Not measures of absolute magnitude, only relative. Summation is arbitrary in absence of zero points.

c) Interval - Quantitative intervals between units of measurement are constant such as10 exceeds 9 is similar to 2 exceeds 1)

E.g. A scale such as 1, 2, 3 . . .9, 10 where numerical value has some meaning but zero point is arbitrary.

Limitation/Freedom:
Can integrate, add/subtract or divide/multiply by a constant only. Amalgamation is possible only if defined equal points on all scales (e.g. A deficit of 2 is not twice 1 since redefining the zero point could transform value 2 to 5 and value 1 to 4)

d) Ratio - Quantitative. Similar to Interval Scale but with set or non-arbitrary set point.

E.g. A measure of effect where zero point is set as no effect (e.g. a scale such as 'no loss', RM1 loss', RM2 mil loss', etc.

Limitation/Freedom:
Measures magnitude not significance. Can be mathematically combined provided units are same or suitable conversion applied

6.4.5 Analysis Principles

The organization uses analysis tools that enable risk to be expressed from the combination of its two components, namely, consequence and likelihood.

(The relationship between these two will depend on many factors that in turn reflect the true nature of the risk and the way it is perceived. This is a function of the context. Particularly, where human values apply, the relationship between the components may well be non-linear and even discontinuous. The more complex the problem, the less certain or definable may be this relationship. For example, a series of minor environmental mishaps may reach a threshold where consequences become of public concern).

From the definition, risk is a function of both likelihood and a measure of consequence. In its simplest form risk can be shown as:

Risk = A function of (Consequence and Likelihood)

Whether using qualitative or quantitative analysis, the nature of the function and underlying logic needs to be understood. Any mathematical operation subsequently applied must conform to that logic, and in particular any use of units must be valid. Indeed, inspection of the units offers a useful check of the underlying logic.

If it is taken that the level of risk is proportional to each of its two components (consequence or likelihood) the risk function is essentially a product function. This can be shown mathematically as:

Risk = Consequence × Likelihood (R = C × L)

This simple relationship does not take account of the complicating factors such as non-linear relationships between utility and the value of consequences. As a result, for quantitative analysis, a fuller relationship is likely to need to include a weighting factor for one of the two components (to achieve a required relative scale between them) and may also require an exponential operator ('raise to power' operators, x and y) for one or both components. For example:

Risk = (C × weighting factor)x × (L)y

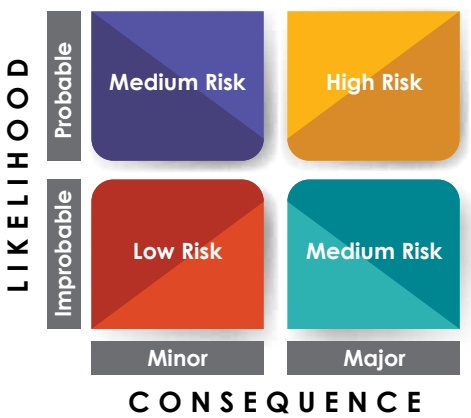
Each of the above descriptions of risk are quite likely to only hold true within a given range. For example, where the frequency is high or an event almost certain, then the risk becomes equal to the consequence alone. Likewise, high consequence outcomes may be so unacceptable that the frequency of occurrence is not a relevant factor.

6.4.6 Graphical Representation

The organization uses graphical representation of risk. In its simplest qualitative form, the relationship between risk and its components can be considered and illustrated by means of a simple 2 x 2 matrix (figure 6.2). For example, it is important to note that the relationship that defines the level of risk may be dominated by either consequence or likelihood or the two components may carry similar or equal weight.

The number of steps or divisions along each axis will be determined by the level of detail, the nature of the measures as well as the context, scope, resources and use to which the output will be used.

A particular strength of the qualitative approach is that no attempt need be made to understand the true



Cell values= Risk units for ranking only

consequence/probability/risk relationship. However, any matrix is invalid unless each possible combination is explored to ensure the tool accurately reflects the organizational perception of risk.

A similar approach can be used to illustrate a semi-quantitative analysis tool. As with the qualitative analysis the scales for each component need not be linear (figure 6.3).

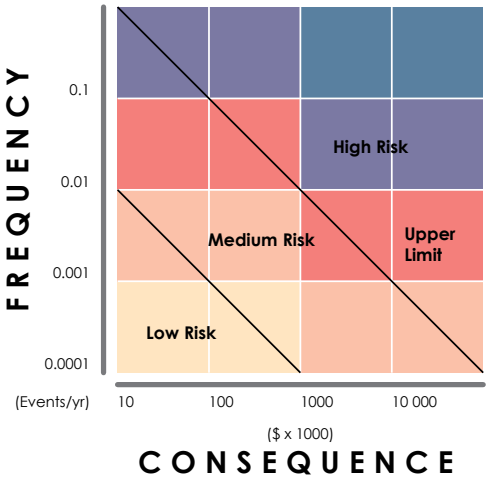
In the case of semi-quantitative analysis some form of mathematical manipulation may be used. It is therefore important that the limitations of the chosen scale types be considered to ensure the manipulation is valid. It should be noted however, that although ordinal scales are commonly used, the manipulation that can be carried out are very limited. The use of ratio scales on the other hand allow most mathematical operations to be performed provided suitable units or conversions are applied (see the following figure 6.4).

(Note that if the risk relationship is taken to be the product of the two components (consequence and likelihood), a constant risk line will not appear straight on the plot unless logarithmic scales are used. Where a simple mathematic expression is used to represent them, a diagram is not needed).

The simplest form of quantitative analysis is similar in concept to semi-quantitative but with usually more rigorous use and manipulation of the values that represent the two components of risk. The use of any scale other than a form of 'ratio' is usually not valid.

However, even where the values are relatively easy to define, there may still need to be some allowance (usually in the form of a weighting or other factor or mathematical function) to account for the human value or utility of a given consequence or perception of likelihood.

Cell values= Risk units for ranking only



Cell values= Risk units for ranking only

When carrying out a quantitative analysis, the measurement units should always be stated.

6.4.7 Consequence and likelihood tables

The organization uses tables to provide definitions for rating scales so there is a common understanding of their meaning. Tables are consistent with the specific objectives and context of the risk management activity.

a) Consequences

The table shows a simple qualitative consequence table that might be used by an organization with criteria related to health and safety, the environment and financial success. It also considers the political and financial impacts of risks, such as might be encountered in a public-sector program analysis. Table 6.2 shows a very simple descriptive table.

Severity Level	Consequences Type		
	Profit Reduction	Health & Safety	Legal
v	RM 10M-100M	Multiple fatalities/ disability >50	Significant persecution and litigation
iv	RM 1M - 10M	Single Fatality/ disability	Major breach of regulation and litigation
iii	RM 100K - 1M	Moderate impairment (<30%) to single person	Major breach with moderate fines
ii	RM 10K - 100K	Reversible disability requiring hospitalization	Minor legal issues, non-compliance and breaches
i	< RM 10K	No medical treatment required	

Where differing types of consequence are shown together in a table or where the same descriptor is used for the level, then an equivalence between each consequence will be inferred. If this is not true then separate tables and descriptors need to be used (Table 6.3). Where equivalence is intended, then great care needs to be taken to ensure this is defendable and, where appropriate, agreed with stakeholders.

Table 6.3: Simple Consequence Scale – Example 2

Description	Definition
Severe	Most objective cannot be achieved
Major	Some important objective cannot be achieved
Moderate	Some objective affected
Minor	Minor effects that are easily remedied
Negligible	Negligible impact upon objective

b) Likelihood

The organization constructed scales need to meet the circumstances of the study in hand. Tables 6.4 and 6.5 below are examples of likelihood scales. The first uses order of magnitude scales to span a range of likelihoods from approximately yearly to one in 10 000 years. The second example (Table 6.6) shows a scale that is more suited to a defined period of time where the absolute likelihood of an event may be related to given activities – a project for example where the chance of achieving a certain outcome may need to be considered. Again, the scale must match the need.

Table 6.4: Example of Likelihood Scale – Example 1

Level	Descriptor	Description	Indicative frequency
A	Almost Certain	Events occur on annual basis	Once a year of more
B	Likely	Events occur several times or more in your career	Once every 3 years
C	Possible	Events might occur once in your career	Once every 10 years
D	Unlikely	Events occur somewhere from time to time	Once every 30 years
E	Rare	Heard of some accurrence somewhere	Once every 100 years
F	Very Rare	Never heard of this happening	Once every 1,000 years
G	Almost Incredible	Theoretically possible but not expected to occur	Once every 10,000 years

Table 6.5: Example of Likelihood Scale (probability) – Example 2

Descriptor	Description	Alternative Descriptor
Probable	Can be expected to occur during project	Good odds
Possible	Not expected to occur during project	Low to even odds
Improbable	Concelvable but highly unlikely to occur during project	Poor odds

The number of occurrences in a time period will depend on the population, area or number of assets etc. being considered. Interpretation of indicative frequency scales such as in Table 6.4 (Example 1) must reflect the scope defined in the context and be consistent across a study.

The likelihood of gain or loss can be considered to be a function of both the exposure to the source of risk and the probability that the outcome will occur. These two factors can be assessed separately. For example, in Occupational Health and Safety, one might consider the exposure to a chemical hazard and the probability that harm will occur following exposure.

Systems engineering techniques such as fault tree analysis can be used to analyses probabilities in more detail.

6.4.8 Level of Risk

A qualitative approach can only describe risk in qualitative ways – and this is usually done with descriptive terms. An example of this is given in Table 6.6 below. Quantitative analysis may on the other hand produce a single figure, datum or value or a mass of detailed data. Where this is the case, great care needs to be taken to ensure the units of risk are expressed and understood. Particular care must be taken with quantitative analysis when examining consequences that are intangible or difficult to quantify such as environmental or safety effects or reputation.

Table 6.6

Likelihood Label	Consequences Label				
	i	ii	iii	iv	v
A	Medium	High	High	V. High	V. High
B	Medium	Medium	High	High	V. High
C	Low	Medium	High	High	High
D	Low	Low	Medium	Medium	High
E	Low	Low	Medium	Medium	High

Assumptions and their impact as well as the level of certainty also need to be given.

Table 6.6 above also illustrates the process and descriptors that may be used to combine a level of consequences with a level of likelihood to determine a level of risk. The number of categories of risk defined in a table like this should reflect the needs of the study.

The categories may be linked to the level of management attention that is recommended or the time scale of the response required. For example:

a) Very high or high risk: senior executive management attention needed, action plans and management responsibility specified.

b) Medium risk: manage by specific monitoring or response procedures, with management responsibility specified.

c) Low risk: manage by routine procedures, unlikely to need specific application of resources.

Another simple example is shown in Table 6.7 below.

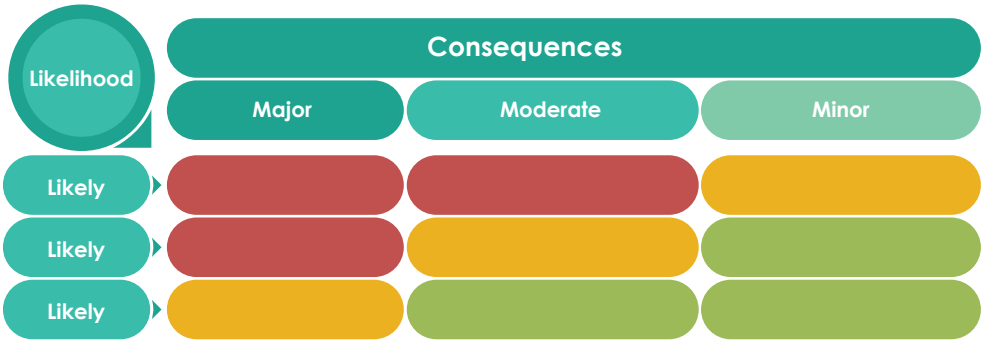


Table 6.7: Example – Simple Risk Level Matrix

Table 6.8: Risk Treatment Key

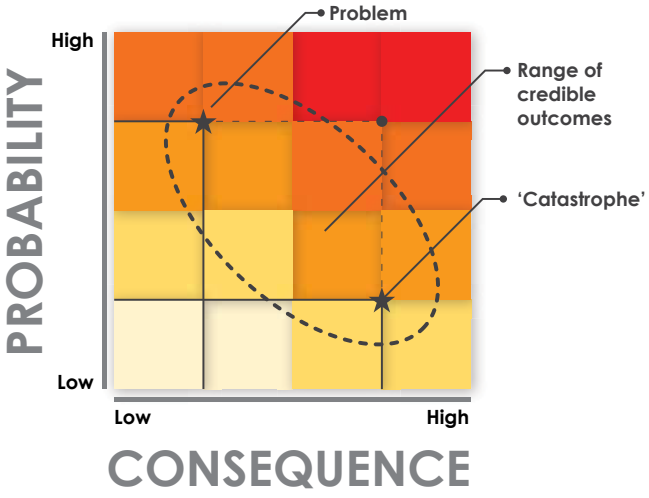


Figure 6.5: Risks with range of outcomes

Many risk events may arise in a variety of ways, with a range of outcomes and associated likelihoods. For example, if a processing error were to occur in a business, it might be a minor problem, or it might cause a very large loss. Usually, the minor problems are much more frequent than the catastrophes, and the potential risks fall in a pattern such as that shown in Figure 6.5. When selecting a risk for assessment, there are now several choices: select a typical problem, with low consequence but high probability; or a representative catastrophe, with a high consequence but a low probability, or some intermediate outcome.

In many cases it is appropriate to focus on events with potentially catastrophic outcomes, as these are the ones that pose the largest threats and are often of greatest concern to regulators.

In some cases, it may be important to identify and analyses both 'problems' and 'catastrophes' as separate risks. For example, a frequent but low-impact (or chronic) problem may have large cumulative or long-term effects that are at least as important as those of a rare but high-consequence (or acute) event. In addition, the treatment actions for dealing with these two distinct kinds of risks are often quite different, so it is sensible to distinguish between them and to record them both.

It is important to be consistent when analyzing risks that might occur in different ways like this. For example, selecting a consequence rating corresponding to a rare catastrophe and a probability rating corresponding to a frequent problem would identify a risk outside the feasible range in Figure 6.5 above, not a valid outcome for further analysis. For example, if a consequence rating corresponding to a rare catastrophe is selected the likelihood rating must correspond to the likelihood of that catastrophic outcome. If a likelihood more appropriate to a frequent problem is selected, the selected risk would lie outside the feasible range as shown by the question mark in figure above, not a valid outcome.

6.5 RISK ASSESSMENT: EVALUATION PROCESS

The purpose of risk evaluation is to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment and the priority for treatment implementation.

Risk evaluation involves comparing the level of risk found during the analysis process with risk criteria established when the context was considered. Based on this comparison, the need for treatment can be considered.

Decisions should take account of the wider context of the risk and include consideration of the tolerance of the risks borne by parties other than the organizations that may benefits from the risk. In some circumstances, the risk evaluation can lead to a decision to undertake further analysis. The risk evaluation can also lead to a decision not to treat the risk in any way other than maintaining existing controls.

This decision will be influenced by the organization's risk attitude and the risk criteria that have been established.

6.5.1 Risk Tolerance

The simplest risk criterion divides risks that need treatment/action from those which do not. This gives attractively simple results but does not reflect uncertainties either in estimating risks or in defining the boundary between those that require treatment and those that do not.

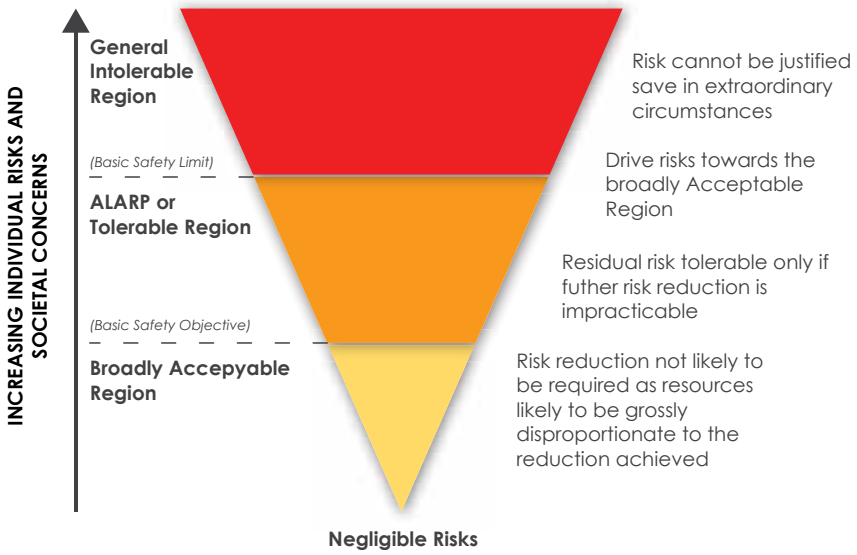
A common approach is to divide risks into three bands:

a) An upper band where adverse risks are intolerable whatever benefits the activity may bring, and risk reduction measures are essential whatever their cost.

b) A middle band (or 'grey' area) where costs and benefits, are taken into account and opportunities balanced against potential adverse consequences.

c) A lower band where positive or negative risks are negligible, or so small that no risk treatment measures are needed.

For risks with significant potential health, safety or environmental consequences, this is expressed as the 'As Low As Reasonably Practicable' or ALARP concept illustrated in Figure 6.6 below but the concept is also applicable for other risks.



The width of the cone indicates the size of risk and the cone is divided into bands as discussed above.

When risk is close to the intolerable level the expectation is that risk will be reduced unless the cost of reducing the risk is grossly disproportionate to the benefits gained. Where risks are close to the negligible level then action may only be taken to reduce risk where benefits exceed the costs of reduction.

The concept in ALARP is based on the percept of practicality (Can something be done?) as well as the costs and benefits of action or inaction (Is it worth doing something in the circumstances?). These two aspects need to be balanced carefully if the risks the organization is treating are related to an expressed or implied duty of care.

6.6 RISK TREATMENT

Risk treatment involves selecting one or more options for modifying risks, and implementing those options. Once implemented, treatments provide or modify the controls.

Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. The options can include the following:

a) avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
b) taking or increasing the risk in order to pursue an opportunity;
c) removing the risk source;
d) changing the likelihood;
e) changing the consequences;

f) sharing the risk with another party or parties (including contracts and risk financing); and
g) retaining the risk by informed decision

Selecting the most appropriate risk treatment option involves balancing the costs and efforts of implementation against the benefits derived. Decisions should also take into account risks which can warrant risk treatment that is not justifiable on economic grounds, e.g. severe (added burden to the regulated community, high negative consequence) but rare (low likelihood) risks.

When selecting risk treatment options, regulators should consider the values and perceptions of stakeholders and the most appropriate ways to communicate with them. Where risk treatment options can impact on risk elsewhere on stakeholders, these should be involved in the decision.

Though equally effective, some risk treatments can be more acceptable to some stakeholders than to others. The treatment plan should clearly identify the priority order in which individual risk treatments should be implemented.

Risk treatment can also introduce secondary risks that need to be assessed, treated, monitored and reviewed. These secondary risks should be incorporated into the same treatment plan as the original risk and not treated as a new risk. The link between the two risks should be identified and maintained

6.7 MONITORING AND REVIEW

Both monitoring and review should be a planned part of the risk management process and involve regular checking or surveillance. It can be periodic or ad hoc. Responsibilities for monitoring and review should be clearly defined. The regulator's monitoring and review processes should encompass all aspects of the risk management process for the purposes of:

- ensuring that controls are effective and efficient in both design and operation;
- obtaining further information to improve risk assessment;
- analysing and learning lessons from events (including near-misses), changes, trends, successes and failures;
- detecting changes in the external and internal context, including changes to risk criteria and the risk itself which can require revision of risk treatments and priorities; and
- identifying emerging risks.

Progress in implementing risk treatment plans provides a performance measure. The results can be incorporated into the regulator's overall performance management, measurement and external (e.g. MPC's Annual Report) and internal reporting activities.

The results of monitoring and review should be recorded and externally and internally reported as appropriate, and should also be used as an input to the review of the risk management framework.

CHAPTER 7

RISK MANAGEMENT IN STAKEHOLDERS AND PUBLIC CONSULTATION

7.0 PRELIMINARY

MPC has developed the Best Practice Regulation Handbook ("BPRH") to support the implementation of the NPDIR. A core component to implement the NPDIR is the public consultation process. Public consultation ensures informed decision-making, transparency and accountability of government in the development of regulations. Undertaking public consultation process enhances stakeholders' confidence in regulatory development and contributes towards greater success in its implementation.

7.1 DEFINING PUBLIC CONSULTATION

Consultation is a two-way process through which the government seek and receives the views of stakeholders on proposed changes in policy or regulations that affect them directly or in which they might have a significant interest. Public consultation generates inputs to supplements the procedures and analysis of the authorities especially at the identification and conceptualising stage of regulation development.

Government sponsored consultations may, among others, take the form of public meetings, community workshops, focus groups and surveys as well as interactive websites. Good consultation is characterised by systematic and active participation as well as effective gathering of relevant inputs of stakeholders such as business community, employees, interest groups, non-governmental organisations ("NGOs"), community-based organisations, professional organisations and individual citizens in the design and/or review of regulation.

With so many different stakeholders with diverse interests Stakeholder Analysis is therefore a critical component of the consultation process as it provides the basis for identifying those persons, groups and organisations that have significant and legitimate interests in a specific issue or policy area. This enables the development of better strategies for more effective stakeholders involvementin order to policy objectives.

In general, any proposed new regulation or change to existing regulation, should involve consultation with relevant stakeholders. Consultation must be an integral part of the process whenever a RIA is conducted to prepare a Regulatory Impact Statement (RIS). Consultation should begin as early as possible in the RIA process.

7.2 GUIDING PRINCIPLES FOR PUBLIC CONSULTATION

Six guiding principles of public consultation represent the essential elements of good practice in the development and implementation of NPDIR.

7.2.1 Principle No. 1 - Transparency with Accessibility

Authorities should ensure that stakeholders and the public understand the scope of the regulation development process and procedures, and that any constraints are made known. Consultation exercises should be designed to reach the intended stakeholders or regulated community.

7.2.2 Principle No. 2: Accountability

Government has an obligation to account for the use of stakeholders' resources and inputs received through the public consultation. To demonstrate this accountability, government need to ensure an open and transparent policy-making process.

7.2.3 Principle No. 3: Commitment

Leadership and strong commitment to information, consultation and active participation in regulation development are needed at all levels, from ministries, secretary generals, Director Generals, and senior officers. Appropriate time and resources must be provided to ensure their involvement in meaningful ways.

7.2.4 Principle No. 4: Inclusiveness and Equitability

The authorities should make every reasonable effort to include all the stakeholder groups and the interested individuals affected by the proposed regulations. Access to consultation processes and ability to participate is to be ensured despite race, ethnicity, religion, political affiliation, gender, disability status or any other possible basis for discrimination.

7.2.5 Principle No. 5: Timely and Informative

Engagement with stakeholders shall be within reasonable time frames to collect stakeholders' feedback and disseminate the information in time to inform on the regulation development. Information is needed at all stages of the regulation development and enforcement. Increased interest and motivation to participate occur by diffusing simple and understandable information to the affected and interested public.

7.2.6 Principle No. 6: Integrity with Mutual Respect

The authorities shall engage stakeholders and the affected public in an honest and forthright way. The process of engagement shall be open, transparent and accountable. There will be recognition of diversity among and between all stakeholders with the willingness to discuss and deliberate towards common understanding. This will mean giving regard for difference of perspective, objectives, values and needs among groups and individuals.

7.3 REQUIREMENTS FOR PUBLIC CONSULTATION

7.3.1 Consultation Paper (Issue Paper)

Consultation documents should be clear about the consultation process, what is being proposed, the scope to influence and the expected costs and benefits of the proposals. For instance, what has taken place in the development of the proposed regulation prior to the consultation exercise, how the consultation exercise will be run and, as far as is possible, what can be expected after the consultation exercise has formally closed.

7.3.2 Planning the Consultation Exercise

Consultation should normally last for at least 12 weeks with consideration given to longer time frame where required and feasible. When timing is tight, for example when dealing with emergency measures, or international, legally-binding deadlines, or when the consultation needs to fit into fixed time table such as the budget cycle, consideration should be given to whether a formal, written, public consultation is the best way of seeking views.

7.3.3 Accessibility of Consultation Exercises

Consultation exercises should be designed to be accessible to, and clearly targeted at those people the exercise is intended to reach. It is essential that interested parties are identified early in the process so that consultation exercises can be designed and targeted accordingly. When consultation exercises need to reach a diverse audience, several approaches may be required. In the consultation document, it should be stated what avenues are available for people to participate, how exactly to get involved, and why any supplementary channels have been chosen.

7.3.4 Stakeholder Analysis

Stakeholder Analysis is a process of systematically gathering and analysing qualitative information to determine whose interests should be taken into account when developing and/or implementing a regulation. BPRH suggests a common method of stakeholder analysis is the 2 X 2 Stakeholder Matrix. This is where stakeholders are plotted against two variables. These variables might be plotting the level of 'stake' in the outcomes of the project against 'resources' of the stakeholder. Another variable is the 'importance' of the stakeholder against the 'influence' of the stakeholder. However, stakeholders need to be profiled before the can be simplistically placed into the matrix quadrant using sticky notes.

7.4 STAKEHOLDERS PROFILING AND LISTING PRIOR TO STAKEHOLDERS MATRIX

In order to rank the stakeholders reasonably without compromising information and interests that may count for public empathy, the characteristics of stakeholders should be studied in detail.

Ministries and agencies should establish and maintain stakeholders list and profile them (Sample form Figure 7.1: Stakeholder's Base Profile). This is performed to identify all relevant stakeholders and analyse their relationship, how they have influence or are affected by the proposed regulation. Stakeholder's profile should be reviewed and updated prior to any consultation process.

Stakeholders list should be divided into different categories such as government agencies, companies, NGOs, community based organizations, employees and individuals (professions) to allow a more systematic identification process. Completeness of stakeholder list is imperative to avoid interested parties being left out.

Stakeholder's Base Profile form extends the information from the stakeholders list. Each stakeholder will be analysed for their roles and responsibilities towards a certain regulation via the following:

- desktop research on roles and functions
- interviewing or inquiring with the relevant parties
- brainstorming with various parties

Details of their function and relationship are then evaluated to derive expectations. The expectations are divided into:

(i) stakeholders' expectation on the regulation, how they would influence the development of the regulation and

(ii) 'Regulation's expectation' on them, how they would be affected by the regulation.

The stakeholder analysis allows ministries and agencies to understand stakeholders' needs and concerns in depth and incorporate these essentials into the regulation and later enforcement. This will increase stakeholders' awareness and buy- in, consequently ease the implementation of the proposed regulation.

Control No:

STAKEHOLDER'S BASE PROFILE

Stakeholder _____ **Stakeholder's Index** **SE 0 0 1**

Definition: Stakeholder is defined by any people, groups or organisations that can have an effect or effected by the proposed regulation.

"Relationship" with the Proposed Regulation:

- Fed. Gov. Ministry
- Fed. Gov. Agency
- State Government
- Local Company
- Foreign Company
- Service Provider
- Utility Company
- Emergency Response
- Public
- NGOs / CBOs
- Individuals (Professions)
- Employees
- INGOs
- International Bodies
- Financial Markets
- Commodity Markets
- Political Climate
- Financiers
- Public Insfrastructure
- Public Facilities

Details OF "Relationship" with the Proposed Regulation (Functions & Expectations).

Function:

-
-

Expectations on the proposed regulation:

-
-

Expectations on stakeholder:

-
-

Review Frequency: _____ Owner: _____

Prepared by: _____ Reviewed by: _____

( ) ( )

Date Registered: _____ _____

Figure 7.1: Stakeholder's Base Profile

CHAPTER 8

RISK ORGANIZATION STRUCTURE AND SAMPLE PROCEDURES TEMPLATE

8.0 PRELIMINARY

The key feature of a Risk Management Framework is the responsiveness of the risk management organization against the dynamics of the external and internal factors.

The following organisation structure (Figure 8.1) is an example of a cross-functional risk organization to ensure that risk management involves management and staff to ensure risk-based approaches are embedded into regulatory enforcement procedures across different units.

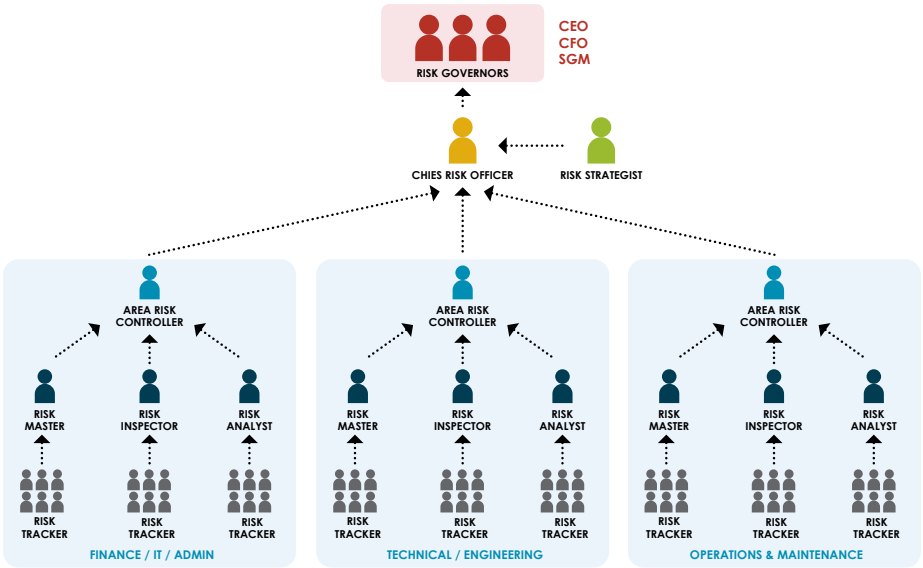


Figure 8.1: Risk Management Organisation

8.1 RISK MANAGEMENT ROLES AND RESPONSIBILITIES

The following outline defines the general roles and responsibilities of risk management teams (cross functional, multitasks) within the regulators existing organization structure.

8.1.1 Risk Governors (RG)

Risk Governors (RG) are made up of the Senior Management members of a regulator. Regulatory Coordinators would be suitable candidates. RG's key responsibilities are to review change recommendations, approve them for implementation and formal adoption into the regulatory process cycle.

8.1.2 Chief Risk Officer (CRO)

CRO is a function that directs and controls the unit with regard to risk. CRO facilitates cross-functional, multitask resources and plans for information gathering, decide which event and element are relevant to the regulator. CRO decides on approach and methods to assess the risk. CRO prioritizes risks and assigns responsibilities to address risks-based approaches in all regulatory processes. CRO reports to the Risk Governors and works closely with the Regulatory Coordinator.

8.1.3 Risk Strategist (RS)

RS' key responsibility is to be aware of the external environment and advise CRO on emerging risks that may need to be registered or trigger a registered risk ahead of time to ensure that the regulator has adequate time to react. RS is also responsible to review and highlight any chain effect of certain risk response or treatment.

8.1.4 Risk Controller (RC)

RC acts as a divisional/project 'CRO' and is directly responsible for recognizing, filtering registering risk triggers/alerts. RC activates risk control procedures, communicates with CRO and mobilizes resources on CRO's behalf. RC presides over divisional Risk Masters, Risk Analysts and Risk Inspectors. RC presides over the functional unit in evaluating and treating risks after communicating with the CRO.

8.1.5 Risk Inspector (RI)

RI vouches for Risk Tracker's trigger process and acts as a safeguard to ensure that all risk manifestations and incidences are being triggered and recorded. RI is the main risk detector of the regulator. RI also ensures that after risk treatment decisions are implemented risk indicators are being recorded and reported to measure its effectiveness.

8.1.6 Risk Analyst (RA)

RA's key responsibilities are to establish the relationship between risk elements and measure their likelihood and impact. Risk Analyst is the 'statistician' and 'economist' within the risk management function. RA breaks down the risks, articulating them logically to ensure that risk executives understand them. RA amplify scenario trees to ensure risk treatment decisions are accurate.

8.1.7 Risk Master (RM) - Problem Solver

RM is the creative problem-solver within the risk management function. RM uses formal problem solving and innovation methods to overcome or reduce risks. RM collaborates with CRO, RS, RM, RA to understand the problem in detail and to design effective solutions that suit the regulator. RM works with RI to gauge the effectiveness of actions for overcoming risks.

8.1.8 Risk Tracker (RT)

RT is the 'sensor' within the risk management function. It is a 'field personnel' to ensure that risk manifestations will not go unnoticed. They activate risk trigger/alert documentation and confides with risk executives in registering risk manifestations. They also act as a lookout after risk treatment procedures. RTs are given a set of parameters to monitor and they are usually assigned on daily operational processes that they are already responsible for. RG, CRO, RS, RC, RM, RI, RA are also expected to double as RTs as they should trigger risks when these come across.

8.2 RISK MANAGEMENT PROCEDURES

The following are sample procedures to assist risk managers and executives in carrying out their responsibilities. These procedures are presented in the following templates with reference to the roles and responsibilities as described in Section 8.1. The forms to be used along the procedural templates below.

RISK MANAGEMENT PROCEDURES

Revision no: 1 **Statement no:** 1 **of** 8 **Effective Date:** _____

ROLE : RISK TRACKER		
INPUT	**ACTIVITY**	**OUTPUT**
RAF (RA 3.8)	1. Risk Trigger & Registration 1.1. Understand risk indicators. 1.2. Continuosly measure indicators. 1.3. If indicator is triggered, alert Risk inspector. 1.4. Fill in **Risk Trigger / Alert Form** and submit to risk inspector. 2. Resource Mobilization Not Applicable. 3. Risk Analysis 3.2. Analyse the frequency with Risk Analyst. 4. Risk Evaluation Not Applicable. 5. Risk Treatment Not Applicable. 6. Change Implementation 6.1. Monitor if treatment procedures and changes made are effective by indicating if risk parameters are still breached. 7. SOP Update Not Applicable.	RTA RAF (RA 3.8)

RISK MANAGEMENT PROCEDURES

Revision no: 1 **Statement no:** 2 **of** 8 **Effective Date:** _____

ROLE : RISK TRACKER		
INPUT	**ACTIVITY**	**OUTPUT**
RAF (RA 1.4)	1. Risk Trigger & Registration 1.1. Upon receiving alert from Risk Tracker (RT), acknowledge Risk Alert/Trigger from. 1.2. Review RTA and if alert is valid, activate the trigger by signing off the RTA. 1.3. Asses if other possible scenario exists with RT. 1.4. Complete RTA (incident and scenario) and escalate to RC.	RTA (RC 1.1)
	2. Resource Mobilization Not Applicable.	
	3. Risk Analysis Not Applicable.	
	4. Risk Evaluation Not Applicable.	
	5. Risk Treatment Not Applicable.	
CIN	6. Change Implementation 6.1. Ensure that all risk treatment and procedural changes made are implemented on the ground 6.2. Obtain update from RT if risk still triggers.	
	7. SOP Update 7.1. Ensure SOP is being updated by Document Controller of the company and communicated to personnel responsible to perform the new procedures.	CIN

RISK MANAGEMENT PROCEDURES

Revision no: 1 **Statement no:** 3 **of** 8 **Effective Date:** _____

ROLE : RISK TRACKER		
INPUT	**ACTIVITY**	**OUTPUT**
RCD (RC 2.1)	1. Risk Trigger & Registration 1.1. Trigger and register risk when necessary.	
	2. Resource Mobilization Not Applicable.	
	3. Risk Analysis 3.1. Upon being prompted by Risk Controller (RC), prepare the Risk Analysis Form (RAF). 3.2. Determine if this an incident or a scenario. For incident, update the occurrence count. 3.3. Review the cause-event-consequences (C-E-Q) impact chain to ensure they are complete. 3.4. Identify existence of process to control against internal causes of risk. 3.5. Identify existence of mitigation/recovery procedures to reduce severity and reduce disruption time for consequences. 3.6. Assess the likelihood of event, causes and consequences with Risk Controller (RC) and Risk Tracker (RT). 3.7. Assess the dollar impact of consequences with RC and RT.	RAF
REF (CRO 4.1)	4. Risk Evaluation 4.1. Evaluate Risk with Risk Controller (RC), Risk Strategist (RS), Risk Master (RM) and Chief Risk Officer (CRO).	RAF (RC 3.1)
	5. Risk Treatment 5.1. Ensure solution under SPIN and RDR can reduce the risk.	REF
	6. Change Implementation 6.1. File REF to track changes.	
CIN (CRO 6.1)	7. SOP Update Not Applicable.	

RISK MANAGEMENT PROCEDURES

Revision no: 1 **Statement no:** 4 **of** 8 **Effective Date:** _____

ROLE : RISK TRACKER		
INPUT	**ACTIVITY**	**OUTPUT**
	1. Risk Trigger & Registration 1.1. Trigger and register risk when necessary.	
	2. Resource Mobilization Not Applicable.	
	3. Risk Analysis Not Applicable.	
REF (CRO 4.1)	4. Risk Evaluation 4.1. Evaluate Risk with Risk Controller (RC), Risk Strategist (RS), Risk Master (RM) and Chief Risk Officer (CRO).	
REF RAF (CRO 4.5)	5. Risk Treatment 5.1. Receiving the REF and RAF from the CRO, prepare the SPIN report to understand the problem. 5.2. Identify the overall solving approach and technique. 5.3. Organize an innovation squad and send to RC (to be approved by CRO) to solve /overcome problem on advice by Risk Strategist (RS). 5.4. Design prototypes and alternatives. Submit to RC. 5.5. Prepare the Solution Development Report (SDR) together with the names of the Innovation Squad and submit to Risk Controller (RC).	REF SPIN (RC 5.1) SDR (RC 5.2)
CIN (CRO 6.1)	6. Change Implementation 6.1. Upon approval of CIN form Risk Governors, file the CIN with the approved SDR for record.	
	7. SOP Update Not Applicable.	

RISK MANAGEMENT PROCEDURES

Revision no: 1 **Statement no:** 5 **of** 8 **Effective Date:** _____

ROLE : RISK TRACKER		
INPUT	**ACTIVITY**	**OUTPUT**
RTA (RI 1.4) RCD (CRO 2.1) RAF (RA 2.1) REF (CRO 4.1) SPIN (RM 5.1) SDR (RM 5.5) CIN (CRO 6.1)	1. Risk Trigger & Registration 1.1. Review RTA from Risk Inspector and assess preliminary chain effect. 1.2. Issue Risk Control Document (RCD) to formally register risk. 1.3. Submit RCD to Chief Risk Officer (7) for approval and resource mobilization. 2. Resource Mobilization 2.1. Upon approval from CRO, communicate with Risk Analysist (RA) to analyse risk in detail. 3. Risk Analysis 3.1. Review the Risk Analysis Form and submit to CRO. 4. Risk Evaluation 4.1. Evaluate Risk with Risk Controller (RC), Risk Strategist (RS), Risk Master (RM) and CRO. 5. Risk Treatment 5.1. Organise with RM via SPIN for Problem Solving Team to be approved by CRO. 5.2. Review the SDR with Risk Master (RM),Risk Analysist (RA), Risk Inspector (RI) and Risk Tracker (RT) 5.3. Submit and discuss SDR with CRO. 6. Change Implementation 6.1. Effect changes by calling a meeting with area manager, Risk Tracker (RT) and Risk Inspector (RI). 7. SOP Update 7.1. Draft the changes for SOP update.	RCD (CRO 1.1) RCD (RA 3.1) RAF REF SPIN (CRO 5.1) SDR (CRO 5.1)

RISK MANAGEMENT PROCEDURES

Revision no: 1 **Statement no:** 6 **of** 8 **Effective Date:** _____

ROLE : RISK TRACKER		
INPUT	**ACTIVITY**	**OUTPUT**
SPIN SDR	1. Risk Trigger & Registration 1.1. Trigger and register risk when necessary. 2. Resource Mobilization Not Applicable. 3. Risk Analysis Not Applicable. 4. Risk Evaluation 4.1. Evaluation risk with RA, RM, RC and CRO. 5. Risk Treatment 5.1. Preside over Risk Master to review SPIN and SDR to ensure strategic risk are being considered. 6. Change Implementation Not Applicable. 7. SOP Update Not Applicable.	SPIN SDR

RISK MANAGEMENT PROCEDURES

Revision no: 1 **Statement no:** 7 **of** 8 **Effective Date:** _____

ROLE : RISK TRACKER		
INPUT	**ACTIVITY**	**OUTPUT**
RCD (RC 1.3)	1. Risk Trigger & Registration 1.1. Review RCD from Risk Controller (RC) on validity of risk and chain effect. 1.2. Approve RCD for mobilization of risk resources.	
	2. Resource Mobilization 2.1. Issue approved RCD to relevant Risk Controller (RC).	RCD (RC 2.1)
RAF (RC 3.1)	3. Risk Analysis 3.1. Upon receiving RAF from the Risk Controller (RC), review completeness of information. 3.2. Approve RAF for risk evaluation.	RAF
	4. Risk Evaluation 4.1. Prepare the Risk Evaluation Report (REF) to summarise the group of risks under consideration. 4.2. Ensure that comparative analysis is carried and to compare with other risks to ensure balanced priority. 4.3. Evaluate Risk with the Risk Controller (RC), Risk Analysts (RA) and Risk Master (RM) and Risk Strategist (RS). 4.4. Decide on general options for risk treatment. 4.5. Issue REF and RAF to Risk Master (RM).	REF (RS 4.1, RC 4.1, RM, 4.1, RA 4,1) REF RAF (RM 5.1)
SPIN SDR	5. Risk Treatment 5.1. Upon receiving SPIN and SDR from Risk Controller (RC), discuss and approve the SDR. 5.2. Prepare Change Implementation Notice (CIN), RAF, REF, SPIN and SDR to Risk Governors (RG). 6. Change Implementation 6.1. Issue the CIN to Risk Controller (RC), Risk Master (RM) and Risk Analysts (RA). 7. SOP Update 7.1. Ensure than implementation text drafted RC is being updated in the SOP.	CIN SDR SPIN RAF REF (RG5.0) CIN (RC 6.1) (RM 6.1) (RA 6.1)

RISK MANAGEMENT PROCEDURES

Revision no: 1 **Statement no:** 8 **of** 8 **Effective Date:** _____

ROLE : RISK TRACKER		
INPUT	**ACTIVITY**	**OUTPUT**
CIN SDR SPIN RAF REF (CRO 5.2)	1. Risk Trigger & Registration 1.1. Trigger and register risk when necessary. 2. Resource Mobilization Not Applicable. 3. Risk Analysis Not Applicable. 4. Risk Evaluation Not Applicable. 5. Risk Treatment 5.1. Upon receiving the Change Implementation Notice (which includes RER, SPIN & SDR) review and approve for solution implementation on the CIN. 6. Change Implementation 6.1. Ensure Internal Audit function monitors implementation. 7. SOP Update 7.1. Ensure Quality Director effects changes on the SOP.	CIN

8.3 RISK MANAGEMENT SAMPLE FORMS

The following sample forms accompany the risk management procedures in section 8.2 above.

DOCUMENT SEQUENCE: 1

RTA NO

RISK TRIGGER/ALERT FORM

Division:	☐ Finance/ IT/ Admin	☐ Technical/ Engineering	☐ Operations & Maintenance
Reported by:		**Risk Position:**	
	Trigger Event		
Describe the event:			
	Risk Indicator		
Describe the risk parameter:			
Risk Indicator Reference No:			

Acknowledgement & Inspection
(To be filled in by Risk Inspector)

Acknowledged & Inspection:	
☐ Yes	Other Possible Spillovers:
Activate Risk?	Other Comments:
☐ No	

Signed by Inspector:

To be filled in by Risk Controller

Reviewed by: _____
(**)**

RCD NO:	
Risk Registration No:	

DOCUMENT SEQUENCE: 2

RCD NO

RISK CONTROL DOCUMENT

RTA NO:

Triggered by: **Triggered Date:**

Inspected by: **Inspected Date:**

Preliminary Chain Effect		
Causes (C)	**Event (E)**	**Consequences (Q)**

Other Risk Details

Risk Indicator: **Trigger Event:**

SOP Doc. Ref.: **Process/ System Involved:**

Division: ☐ Finance/ IT/ Admin ☐ Technical/ Engineering ☐ Operating & Maintenance

REGISTRATION OF RISK

Prepared by:

Name:

Risk Controller

Approved by:

Name:

Chief Risk Officer

RISK REGISTRATION NO
RRN:

Registration Date: _____

DOCUMENT SEQUENCE: 3

RAF NO

RISK ANALYSIS FORM

Name of Analyst: _____ **Date:** _____

Reported Risk _____ ☐ **Incident** ☐ **Scenario**

Division: ☐ **Finance/ IT/ Admin** ☐ **Technical/ Engineering** ☐ **Operations & Maintenance**

*Fill in ④ if the reported risk is an incident.

④ **Frequency**	
No of Transaction:	mth/ yr
Estimated risk incident:	mth/ yr
Doc that determines the statistic:	

⑤ **Estimate the loss value (RM)**	
No of Transaction:	day/ mth/ yr
Avg. Loss (RM):	per incident
Estimated loss (RM):	per annum

② **Causes (C)**	① **Event (E)**	③ **Consequences (Q)**

⑥ **Internal Process that Control this Cause**	⑦ **Mitigation/ Recovery Procedures**
Control Exist? ☐ Yes ☐ No	Procedures Exist? ☐ Yes ☐ No
Describe Control:	Describe Procedures:
SOP Referral Doc:	Referral Doc:

⑧ **Likelihood of Causes**	
Certainly	☐ 5
Probably	☐ 4
Possibly	☐ 3
Unlikely	☐ 2
Impossible	☐ 1

⑨ **Likelihood of Event**	
Very Common	☐ 5
Frequent	☐ 4
Sometimes	☐ 3
Hardly	☐ 2
Remote	☐ 1

⑩ **Likelihood of Consequences**	
Certainly	☐ 5
Probably	☐ 4
Possibly	☐ 3
Unlikely	☐ 2
Impossible	☐ 1

Prepared by:	**Reviewed by:**	**Approved by:**
Name:	Name:	Name:
Risk Analyst	Risk Controller	Chief Risk Officer

DOCUMENT SEQUENCE: 4

REF NO

RISK EVALUATION FORM

Date: _____

Current Risk

RRN	Risk	Approved Date	Likelihood	Impact	Severity	General Treatment

Brought Forward Risk

RRN	Risk	Last Reviewed Date	Status			Action Status (%)
			Likelihood	Impact	Severity	
						0 25 50 75 100
						0 25 50 75 100
						0 25 50 75 100
						0 25 50 75 100
						0 25 50 75 100
						0 25 50 75 100
						0 25 50 75 100
						0 25 50 75 100
						0 25 50 75 100
						0 25 50 75 100
						0 25 50 75 100
						0 25 50 75 100
						0 25 50 75 100
						0 25 50 75 100
						0 25 50 75 100
						0 25 50 75 100
						0 25 50 75 100

Assessed by: RA Name: _____

RM Name: _____

RC Name: _____

RS Name: _____

Assessed & Prepared by:

_____

Name:

Chief Risk Officer

DOCUMENT SEQUENCE: 5

SPIN NO

SPIN REPORT

RRN: _____ **Date:** _____

RAF NO: _____ **REF NO:** _____

S - Situation =	Context	→	P - Problem =	Difficulty/ Risk
N - Need Payoff =	Solution	←	I - Implication =	Consequences

Situation *(Provide high level perspective)*

Problem *(Describe the problem in perspective)*

Implication *(Summarise monetary and non - monetary impacts)*

Need- Payoff *(Identify general solution commensurate with size of problem)*

Proposed Problem Solving Team	
Name	**Dept.**

Prepared by : _____ **RM**

Reviewed by : _____ **RC**

Reviewed by : _____ **RS**

Approval by : _____ **CRO**

DOCUMENT SEQUENCE: 6

SDR NO

SOLUTION DEVELOPMENT REPORT

Name of the Innovation Team

Organised by	Venue	Date
Attendees		

i. Propose of the Event (RRN:)

ii. Overall Solving Approach and Technique

iii. Final Result: The Most Suitable Solution for the Risk

iv. Justification of the Final Result

iv. Estimated Duration for the Solution to Take Place:

Estimated Completion Date:

vi. Owner of the Process:

vii. Required Internal Resources:

viii. Estimated Cost:

Prepared by:

Name:

Risk Master

Reviewed by:

Name:

Risk Controller

Approved by:

Name:

Chief Risk Officer

DOCUMENT SEQUENCE: 7

CIN NO

CHANGE IMPLEMENTATION NOTICE

Notice Ref No:		**Date of No:**	
Risk Registration No:		**Risk Registration Date:**	

A. Subject:

i. To: _____
Risk Controller ⋮ Risk Master ⋮ Risk Analyst

ii. From: _____
Chief Risk Officer

iii. Area: _____ **iv. Process/ System Involved:** _____

v. Prority: ☐ High ☐ Medium ☐ Low

vi. Reason for Change: _____

vii. Objective of Change: _____

B. Change Details

Description of Proposed Change	SOP Ref.

Change Items

No	Item	Deyails of Change/ Instruction	Output	Duration	Completion Date
1					
2					
3					
4					

C. Risk Governor - Decision

Decision: ☐ Approved ☐ Approved w/ Conditions ☐ Rejected ☐ More Info

Change validated by:

Approved by:

Name:

CRO

Approval Date: _____

CHAPTER 9

OUTLINE OF DIFFERENT RISK-BASED INSPECTION SYSTEMS

9.0 PRELIMINARY

In 2010, OECD published a research that explored some of the risk-based frameworks used by regulators in the environmental, food and financial services sectors in a number of countries. The research was conducted by Professor Julia Black, Director of Research, Department of Law and Research Associate, ESRC Centre for Analysis of Risk and Regulation (CARR), London School of Economics and Political Science. This was published under OECD's Review of Regulatory Reform – Risk and Regulatory Policy: Improving the Governance of Risk.

9.1 AUSTRALIAN PRUDENTIAL REGULATION AUTHORITY (AUSTRALIA)

APRA was formed in 1998. It is responsible for the prudential regulation of deposit taking institutions, general and life insurers, and much of the superannuation (pension) industry, and is responsible for their financial soundness (prudential regulation). Its counterpart, the Australian Securities and Investments Commission, regulates securities business, superannuation funds and insurance, and is responsible largely for regulating the manner in which those firms conduct their business. APRA introduced a risk-based approach to supervision in 1999. A new framework was introduced in 2003-04, the Probability and Impact Rating System (PAIRS) and the Supervisory and Oversight Response System (SOARS). PAIRS has been subsequently refined, the latest refinements being introduced in 2008.

All entities are subject to an individual risk analysis, though larger firms and schemes are assessed more intensively. There is a two-stage process:

- an impact assessment based on size, and
- a probability assessment based on scoring of 0-4 of key risk categories.

The framework comprises an assessment of inherent risk and the quality of management and control to derive a net risk score. Net risk is then considered against overall capital support to derive the Overall Risk of Failure. This overall risk score is translated into a probability index rating.

Unusually, all the scoring is based on fourth power averaging. Scores are assigned from 0-4, and there is then a non-linear relationship between the score and the probability indices. The probability of failure increases exponentially through the risk scores, and the probability index runs from 1 to 256. A rating of two, for example, carries sixteen times the risk of a one rating. Once a probability figure is obtained, the figures are assigned to one of five categories of risk; low, low medium, high medium, high and extreme.

SOARS has two components: the supervisory attention index and the supervisory stance. The geometric average of the probability rating and the impact index rating determine the supervisory attention index rating, which is intended to set the level of resources to be applied on the financial institution. The descriptive probability and impact assessments frame the supervisory stance that is the actions the supervisor should take with respect to that institution in terms of the relative intrusiveness,

intensity and directiveness: how "insistent" or "negotiative" they should be in their attitudes towards it.

9.2 DE NEDERLANDSCHE BANK (DNB) (NETHERLANDS)

DNB is the Dutch Central Bank, and is also responsible for the prudential supervision of deposit institutions, insurance companies and pension funds. It introduced its Financial Institutions Risk Management framework (FIRM) in 2006-07. FIRM was developed drawing on experiences in particular of the Financial Services Authority in the UK and APRA. It draws most closely on APRA's model. FIRM is complemented by an assessment of the risks faced by firms from the external market environment.

Under the framework, all institutions are assessed. Supervisors assess the inherent risk of the business. The categories of inherent risk are:

- Financial risks.
- Liquidity risks.
- Insurance risks.
- Operational risks.
- Integrity risks.
- Strategic risks.

The inherent risk score is set against the assessment of the quality of the firm's management and controls to derive a net risk score. The net risk score is then set against an assessment of available capital to arrive at an overall risk of failure score. Scoring is expressed in a traffic light system: red for high risk; green for low risk.

Similar to the APRA framework, Specialist Supervisory Menus are linked to each risk score.

9.3 ENVIRONMENT AGENCY (ENGLAND AND WALES)

The Environment Agency for England and Wales is responsible for monitoring emissions to air and water and waste management. Its policy with regard to inspections is comprised of a number of elements:

- Compliance assessment methodology, for inspectors.

- Compliance classification scheme – this categorizes non-compliance events on the basis of their potential or actual severity.

- Operational Risk Appraisal system (Opra) – this was introduced in 2002 for application to emissions to air; it has recently been revised and extended to waste management (April 2008), consequent on the merging of waste management licences and pollution permit and control permits into Environmental Permits. The Environment Agency is planning to extend Opra to emissions to water in 2008-09.

- Compliance assessment plans – the plans set out national, sector and site-specific objectives together with the resource allocation for each generic compliance activity (including inspections).

The Environment Agency also has a Compliance Enforcement Model which describes the compliance attitude of firms (top performers; generally compliant; generally non-compliant and criminals), and indicates the overall level of regulatory effort required and the Agency's approach.

Opra is a risk screening methodology based on assessments of five risk attributes:

(i) Complexity:

- Potential for significant releases to one or more media.

- Use of one or several interconnected but distinct processes.

- Potential for accidental emissions.

- Inventory of potentially hazardous materials.

- Size relative to its sector and other criteria mentioned here.

- Whether significant regulatory effort is required to assess and maintain compliance and to maintain public confidence.

(ii) Emissions and inputs:

- The type and quantity of the substance in question.

- The media into which the release takes place (e.g. air, water, land).

- The input of waste into an operation.

- The relative impact of substances on media.

(iii) Location:

- Proximity and nature of human habitation.

- Proximity to sites designated under wildlife, countryside or habitats location.

- Sensitivity of receiving waters.

- Potential for direct release to waters and presence of control measures.

- Potential for and consequences of flooding.

- Inclusion within an air quality management zone.

(iv) Operator performance/management systems:

- Presence or absence of management systems or recognized procedures covering areas such as operation and maintenance; competence and training; emergency planning; monitoring, auditing and evaluation.

- Compliance record.

(v) Compliance rating (using compliance classification scheme).

Firms are asked to complete the assessment questionnaires with respect to each of their sites or facilities. Complexity is determined by a "look up" table which assigns risk bands to particular types of activity. The answers given in the assessments are assigned risk bands from A-E, with A as requiring minimal intervention and E the highest level of intervention. Each of the lettered bands can be translated into a risk score. These are aggregated to give an Opra banded profile or risk score. The profile or score is used to determine the risk posed by the facility and to set associated fees and charges.

9.4 FINANCIAL SERVICES AUTHORITY (UK)

The FSA initial version of their current risk-based framework, Arrow I, in 2001. This was revised in 2006. The current risk-based framework is known as Arrow II (FSA, 2006). Arrow II is designed to identify the main risks to FSA's objectives as they arise, measure the importance of those risks, mitigate them where their size justifies it, and monitor and report on progress. Firms are initially put into one of four categories based on impact. Low impact firms are assessed under the "small firms" model. They are monitored on the basis of returns and are dealt with through a contact centre. Medium-low impact firms (other than those with high probability) are assessed under "Arrow-light". Medium high and high impact firms, and medium low impact firms with high probability, are subject to the Arrow Firm Risk Assessment Process.

Individual risk assessments involve an assessment of probability for individual issues and for the firm as a whole. The model has vertical and horizontal dimensions. On the vertical dimension, in assessing probability, FSA assesses the gross risk inherent in the business and then the adequacy of controls addressing that particular risk. There are ten(10) high-level business and control "risk groups" which are further divided into risk elements.

Business risks are grouped into three categories:

- customers, products and markets;

- business processes; and

- prudential risks.

Control risks are categorized into three categories:

• customer, product and market controls;

• financial and operating controls;

• prudential risk controls.

To these assessments are added assessments of oversight and governance, the secondary and pervasive controls in the firm, and other mitigants, namely the amount of excess capital and liquidity that can be used to absorb risks. Running across these assessments at the horizontal level are assessments of environmental risk, control functions and management, governance and culture.

Supervisory response is linked to the risk category in that all high impact firms have a relationship manager. However, for those high impact firms that were assessed under Arrow to be high risk, there was no specific set of supervisory measures that should be taken. Following the FSA's internal audit of its handling of Northern Rock (FSA, 2008), a new supervisory response of "heightened supervision" has been introduce for those high impact firms that are assessed to be high risk on the ARROW model.

9.5 FOOD STANDARDS AGENCY (ENGLAND)

The Food Standards Agency is a non-ministerial department with responsibility for issuing codes of practice concerning the execution and enforcement of the food safety legislation by food authorities (local authorities). Local authorities are required by law to have regard to the Code in discharging their responsibilities. The Food Standards Agency is empowered, after consulting the Secretary of State, to give a food authority a direction requiring them to take specified steps in order to comply with the Code. The latest version of the Code was published in April 2008 (Food SA, 2008).

Food inspectors are required to determine the food hygiene intervention frequencies of food establishments using the risk criteria in the Code. Following recent changes in European legislation an "intervention" is now regarded by the Food Standards Authority as being broader than an inspection, and including other types of activities such as partial audits. At the European level, regulators are required to have official controls to ensure compliance. These include monitoring, surveillance, verification, audit, inspection and sampling analysis. In addition, the Food Standards Agency will allow local authorities to include all other activities which are effective in supporting food businesses to achieve compliance with food law, such as the provision of targeted education and advice, or information and intelligence gathering.

The Code of Practice sets out a risk-based scoring system for food hygiene and for food standards. The food hygiene system has four elements:

• The potential hazard:

- Type of food and method of handling.
- Method of processing.
- Consumers at risk – based on number and vulnerability.

• Level of current compliance.

• Confidence in the management/control procedures.

• Additional score where there is a risk of contamination from Clostridium botulinum micro-organism and any other micro-organism which is pathogenic to humans.

The scores translate into 5 risk bands, A-E, with A as the highest. Minimum intervention frequencies are set for each band, ranging from at least every 6 months for Band A to at least once every 3 years for Band E.

The food standards intervention rating scheme is based on the same principles. Its elements are:

• The potential risk:

- Risks to consumers and/or other businesses.

- Extent to which the activities of the business affect any hazard.

- Ease of compliance - i.e. volume and complexity of relevant food standards law to which the firm is subject.

- Consumers at risk.

• Level of current compliance.

• Confidence in management/control systems.

Again, the scores are translated into risk bands, here A-C with A as the highest. Minimum intervention frequencies are set for each frequency, ranging from at least every 12 months for Band A to once every 5 years for Band C.

9.6 FOOD SAFETY AUTHORITY OF IRELAND

The Food Safety Authority of Ireland introduced its risk-based code of practice for inspections in 2006. The framework focuses on the types of different food establishments, following the categories required for annual statistical returns to the European Commission.
These are:

• Primary producers.

• Manufacturers and packers.

• Distributors and transporters.

• Retailers (retail trade).

• Service sector (restaurants, canteens, caterers and public houses).

• Manufacturers selling primarily to the final consumer.

Within these producer groups, different types of producers are categorized as high, medium or low risk depending on the risks that their activities pose to consumers. The frequency of inspections is linked to the risk category. Those in the highest risk category must be inspected is one full inspection and two surveillance inspections every year; those in the lowest must receive one full inspection a year. Inspection frequencies may be reduced by a stipulated amount if there is a good compliance record and the firm has complied with all requirements relating to Hazard and Critical Control Points analysis and training.

9.7 HEALTH AND SAFETY EXECUTIVE (FIELD OPERATIONS DIVISION) (UK)

The Health and Safety Executive is responsible for monitoring compliance with the health and safety legislation, together with local authorities, and for investigating accidents at work. It is also responsible for monitoring hazardous activities including nuclear installations and hazardous chemical plants. The research here focused on its occupational health and safety remit relating to non-hazardous activities, which is run by its Field Operations Division. It is responsible for monitoring compliance in approximately 2 million business premises in the UK.

The HSE has an extensive body of data on work-related fatalities, injuries and ill health which it uses to develop indicators of the industries and activities which pose the greatest risk. It has used this data to build a strategic program of interventions, known as Fit 3: Fit for Work, Fit for Life; Fit for Tomorrow. As part of this strategy it has introduced a topic based inspection system, focusing on the most common types of risks, such as "slips and trips", falls from height, stress or workplace transport. The Fit 3 topic packs provide a framework for conducting inspections and assessing firms.

The risk-based assessment has four elements:

• Competence and attitude of management.

• Safety compliance and actual risk.

• Health compliance and actual risk.

• Welfare compliance gap.

The number of inspections has steadily declined from 70 000 in 2002-03 to 35 000 in 2006-07. The HSE has been progressively moving to other types of intervention strategies, notably targeted information campaigns using a variety of delivery mechanisms.

9.8 IGAOT (PORTUGAL)

The Portuguese environment regulator, IGAOT, had introduced a risk-based system in 2009. The system was developed in conjunction with IMPEL, the European Network for the Implementation and Enforcement of Environmental Law. It was based on IMPEL's guidance for environmental inspections, Doing the Right Things, and was influenced by the frameworks used by the environmental regulators in Ireland and the Netherlands.
All sites with an integrated pollution control license will be assessed under the framework. The framework will thus apply to emissions, waste management and discharges into water/sewers.

There are 5 groupsof risk:

- Complexity.
- Emissions and inputs.
- Location.
- Attitude of operator to the environment and sustainability of the attitude.
- Compliance behaviour.

Compliance behaviour is given additional weight in arriving at the overall risk score. There are three categories scores, high, medium and low. It is envisaged that most resources will be focused on the high-risk entities.

9.9 OFFICE OF ENVIRONMENTAL ENFORCEMENT OF THE ENVIRONMENTAL PROTECTION AGENCY (EPA) (IRELAND)

The EPA introduced its risk-based framework, the Environment-Based Assessment Tool in 2007 (EPA, 2007). It was developed drawing on frameworks used in Norway, the Netherlands, England and Wales, and Scotland. The Environment Agency of England and Wales' model was used as the basis for the EPA's framework.

The framework allocates an enforcement priority to licensed facilities on the basis of 5 risk elements:

- Complexity.
- Location.
- Emissions.
- Operator management.
- Enforcement record.

There are three categories of broad enforcement, high (A), medium (B) and low (C). These are further subdivided thus: A1-A3; B1-B3; and C1-C2. An enforcement category is derived for each risk element; these are then combined to give an overall enforcement category. The EPA will use the categorisation to determine its inspection priorities and its enforcement approach.

The framework operates together with the Environmental Liability Risk Assessment, to be performed by all licensed facilities on an annual basis, and used in conjunction with the enforcement category to determine the EPA's response.

9.10 OFFICE OF FAIR TRADING (UK)

The Office of Fair Trading is responsible, amongst other, for the regulation of consumer credit. Those engaging in consumer credit business in the UK require a licence. There are currently over 240 000 licence holders. The OFT has recently been given new powers under the Consumer Credit Act 2006 to carry out fitness and competence checks of licence holders. It has also received powers and responsibilities under the Act to supervise approximately 22 000 credit institutions. It is intending on contracting out some of this work to Trading Standards offices, which are funded by and accountable to local authorities. The OFT is introducing a risk-based system to the monitoring of consumer credit licences in 2008-09.
The 2006 Act introduced a new competence requirement for consumer credit licence holders. Credit competence is defined by the OFT to mean whether the licence holder can demonstrate that he/she or those employed by them have adequate knowledge and experience to carry on credit business concerned, and whether the applicant or licence holder has established or maintained management and financial systems which would enable it to meet its obligations to customers, and to comply with the legislation and generally accepted business practices. The intention is that the OFT will be able to refuse a licence or licence renewal application on the grounds of lack of competence alone.

It will inspect only high-risk activities. The primary factors which affect the level of risk to consumers are the transparency of the market and the consumer's ability to shop around. Based on these principles, the OFT divides activities into three categories of risk.

High risk Category A – high risk activity where problems and solutions are well documented and understood; full Credit Competence Plan and on-site visit usually required:

- 3rd party debt collection.
- Debt counselling.
- Debt adjusting.
- Credit information services.

High RISK Category B – high risk activities where there is a potential for serious consumer detriment but the issues are less clear cut. Credit Risk Profile Form and on-site visit sometimes required:

- Lending/broking - secured subprime.
- Lending/broking - at home.
- Debt administration - secured subprime.
- Credit reference agencies.

Low Risk category: all activities other than the above on the basis that the risks are considered to be lower and can be dealt with adequately ex post or through different means than inspections.

9.11 THE PENSIONS REGULATOR (UK)

The Pensions Regulator was established in 2004 and responsible for the supervision of work-based pension schemes in the UK, with a focus on employers and trustees. It is not responsible for regulated the financial services providers related to such schemes; that is the responsibility of the UK Financial Services Authority. Its objectives are to protect the funds in pension schemes, to reduce the risk of situations that may lead to compensation being payable from the Pension Protection Fund and to promote and improve understanding of good administration of work based pension schemes.
Its risk-based approach has two dimensions: level of risk and scheme size. Schemes are considered small if they have less than 1 000 participating members. Risk is defined as the negative impact of the failure of a scheme on the member and the market.

The Pensions Regulator has an intervention matrix which comprises four scenarios of three different levels of risk intensity.

- High risk, large scheme: Active intervention; high intensity intervention.
- High risk, small scheme: Intelligence based action; medium intensity intervention.
- Low risk, large scheme: Proactive monitoring; medium intensity intervention.
- Low risk, small scheme: Focus on education and support; low intensity intervention.

The regulator adopts a "triage" approach to organise its workflow and identify the appropriate supervisory response. As information comes in, it is initially handled by customer support. That unit refers more complicated or serious matters to the triage unit.

Triage then assesses the risk and then forwards the issue to one of the three supervisory groups: scheme specific funding, corporate risk management, or pension administration and governance, depending on the issue.

9.12 VROM (NETHERLANDS MINISTRY OF HOUSING, SPATIAL PLANNING AND THE ENVIRONMENT INSPECTORATE)

The VROM inspectorate is responsible for enforcing some of the rules that still fall under the responsibility of the Minister; it also oversees performance of the municipal and provincial authorities in implementing and enforcing the legal requirements. It mainly focuses on the transportation of environmentally hazardous materials into, out of and within the Netherlands.

VROM organise its activities under its Compliance Strategy, introduced in 2004 (VROM, 2004). The Compliance Strategy is based on seven principles:

- Risk assessments.
- Non-compliance rate.
- Determination of priorities.
- Reasons for non-compliance.
- Smart enforcement.
- Co-operation.
- Feedback.

The Strategy translates these principles into two "tracks". These are the "task oriented track" and the "problem-oriented track". The "task oriented track": inside – out comprises six assessments:

- What rules must be enforced?
- Are the rules enforceable, executable and fraud resistant?
- What are the risks of not enforcing the rules?
- What is the scale of the non-compliance rate and what is the reason for it?
- What is an appropriate intervention?
- What has been learned and who should be informed about it?

The problem-oriented track (outside-in) comprises a further six assessments:

- What risks exist for the sustainable environment?
- What causes the problem and who is involved?
- What mix of intervention is needed and how will it be organised?
- Is work taking place according to a plan and will the goal be achieved?
- What has been learned and who should be informed about it?
- How will the achieved results be maintained?

Based on the "task oriented track" the VROM inspectorate can prioritise its tasks and concentrate on high risks and high non-compliance rates. The "problem-oriented track" is used to focus attention on which societal problems require attention and how they should be addressed.

REFFERENCES

Florentin B. (2012). Inspection Reforms: Why, How and with What Results. www.oecd.org/gov/regulatory- policy/reform%20of%20inspections%20-%20Web%20-F.%20Blanc.pdf

Government of Malaysia, (2013). Best Practice Regulation Handbook. Petaling Jaya, Selangor: Malaysia Productivity Corporation.

Government of Malaysia, (2014). Guideline on Public Consultation Procedures. Petaling Jaya, Selangor Darul Ehsan: Malaysia Productivity Corporation.

Government of Malaysia, (2013). National Policy on the Development and Implementation of Regulations. Petaling Jaya, Selangor Darul Ehsan: Malaysia Productivity Corporation.

Government of Malaysia, (2017). A Guideline to Reducing Unnecessary Regulatory Burdens: Core Concepts (4th ed.). Petaling Jaya, Selangor Darul Ehsan: Malaysia Productivity Corporation.

Julie M. (2012). Reform of Regulatory Enforcement and Inspections in OECD Countries. www.oecd.org/gov/regulatory-policy/reform%20of%20inspections%20-%20Web%20-%20Julie%20Monk.pdf

Malaysia Standard. (2010). Risk Management – Principles and Guidelines. Cyberjaya, Selangor Darul Ehsan: Department of Standards Malaysia.

OECD, (2014). The Governance of Regulators, OECD Best Practice Principles for Regulatory Policy, OECD Publishing. http://dx.doi.org/10.1787/9789264209015-en

OECD, (2015). Implementing Good Regulatory Practice in Malaysia, OECD Publishing, Paris. http://dx.doi.org/10.1787/9789264230620-en

OECD, (2010). Risk and Regulatory Policy, Reviews of Regulatory Reform, OECD Publishing. http://dx.doi.org/10.1787/9789264082939-en

Richard M. S., Frank J. M., Miles E.A.E & Lucy, E.N. (2004). Enterprise Risk Management – Integrated Framework. Committee Of Sponsoring Organizations of the Treadway Commission.

PKF CEOPE Sdn. Bhd. (2017) Risk Response Procedures Manual.

www.mpc.gov.my

Transformation • Innovation • Partnership

MALAYSIA PRODUCTIVITY CORPORATION (MPC)

Lorong Produktiviti, Off Jalan Sultan, 46200 Petaling Jaya,
Selangor Darul Ehsan, Malaysia

+603 7955 7266/7050/7085 +603 7954 0795 regulatoryreview@mpc.gov.my