AmRest

RISK MANAGEMENT POLICY

Table of contents

1. Introduction

There can be two types of events i.e. negative events are classified as **risks** while positive events are classified as **opportunities**.

Risk is a probability or threat of quantifiable damage, injury, liability, loss or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through pre-emptive action. Risks can come from various sources including uncertainty in financial markets, threats from project failures (at any phase e.g. design, development, production or sustainment of life-cycles), legal liabilities, credit risk, accidents, natural causes and disasters, deliberate attack from an adversary, or events of uncertain or unpredictable root-cause.

Opportunity is exploitable set of circumstances with uncertain outcome, requiring commitment of resources and involving exposure to risk.

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

2. Objectives of the Risk Management Policy

The purpose of the risk management policy is to provide guidance regarding the management of risks and opportunities to support the achievement of AmRest corporate objectives, protect staff and business assets and ensure financial sustainability.

3. Scope of the Risk Management Policy

This policy applies to all AmRest Group activities. It forms part of AmRest corporate governance framework and applies to all employees and co-workers, including Directors, Executives and Officers of companies belonging to the AmRest Group in each country in which AmRest operates.

4. Risk Governance at AmRest

The risk governance structure in AmRest Group is following:

Who:	What:
Board of Directors	Provides oversight and review of risk management.
Audit Committee	Oversees regular review of risk management activities.
Top Management (CEO, CFO, COO, CPO, CIO, etc.)	Promotes risk management culture.
Management	Responsible for designing and executing of risk strategy and control mechanisms which decrease negative impact and/or probability of risks and increase positive impact and/or probability of opportunities. Ensure employees comply with the risk management policy and support a culture where risks and opportunities can be identified, addressed and escalated.
Internal Audit and Internal Control Department	Analyses and evaluates risk management, internal controls and corporate governance and provides recommendations supporting: • risk reduction of not realizing AmRest objectives; • increase of efficiency of business processes; • optimizing control mechanisms.
Employees and Co-workers	Comply with risk management policies and procedures.

5. Risk Management Process at AmRest

AmRest Management is accountable for daily identifying, analysing, evaluating, monitoring and addressing the risks and opportunities in areas of their responsibilities. Internal Audit Department (IA) acts according to the Internal Audit Articles of Association and Internal Control Department (IC) according to Internal Control Charter. IA and IC support AmRest Management by:

- realizing planned audit assignments according to the Annual Audit Plan,
- performing ad-hoc audit assignments;

Main purpose of planned and ad-hoc audit assignments is to identify risks and opportunities and provide recommendations which will support AmRest in risk management.
Management is responsible for preparing action plans addressing identified by IA and IC risks and opportunities. Internal Audit and Internal Control regularly monitor and verify implementation of action plans declared by the Management.

In addition, Internal Audit Department with the engagement of AmRest Management up-dates AmRest Risk Map on a regular basis. The objectives of the AmRest Risk Map project are to:

- collect comprehensive and structured information about risks at AmRest Group **(identification)**;
- perform risk prioritization of the identified risks **(assessment);**
- have an updated and integrated risk map for AmRest Group.

6. Risks Structure and Risk Matrix

The AmRest Risk structure includes a 3-level risk classification system:

- The first level (main categories of risks) is divided into 4 areas:
  - Strategic,
  - Operational,
  - Financial,
  - Compliance.
- The second level includes specific categories;
- The third level contains specific risks.

The risks are evaluated by using the consistent parameters: vulnerability, impact and probability:

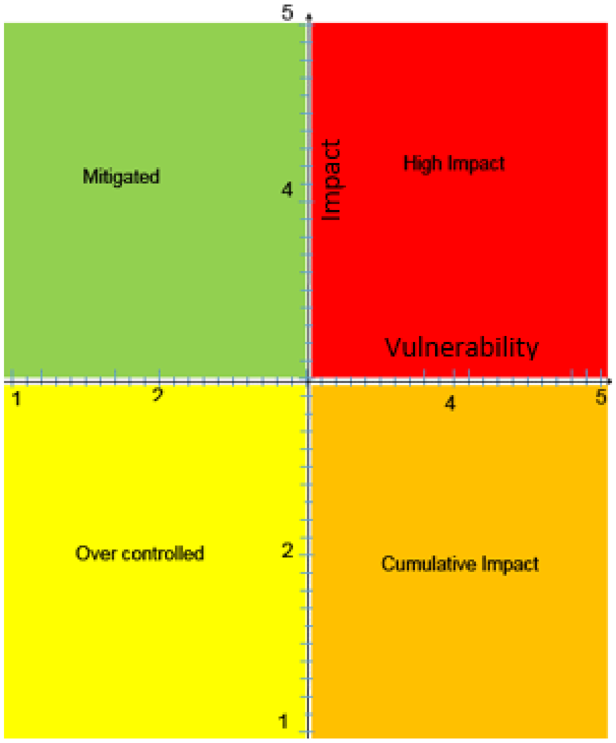
VULNERABILITY TO RISK (ranging from 1 (the lowest) to 5 (the highest)) is the measure assuming effectiveness/efficiency of implemented control system (it answers to a question: "How vulnerable is AmRest Group in case of risk materialization and will AmRest be ready if the event occurs?").

IMPACT OF RISK (ranging from 1 (the lowest) to 5 (the highest)) is an effect of an event resulting in materialization of specific risk, in case of the failure of existing control systems. An event may have influence on one or more of areas including:

- Finance,
- Stakeholder,
- Reputation and community,
- Health & Safety,
- Environment,
- Regulatory.

PROBABILITY OF RISK (ranging from 1 (the lowest) to 5 (the highest)) is defined as frequency of occurrence of given event in a defined period. It answers to a question: "How often and in which period risk will materialize?"

Risks can be classified to one of the areas: High Impact, Cumulative Impact, Over Controlled or Mitigated and can be presented graphically as follows:



Risk matrix used at AmRest:

Area	Description
High Impact	In this area control mechanisms do not exist or are not working. In case when risk materializes, it has significant negative impact on the company. For risks classified in this area it is necessary to implement new or enforce existing working mechanisms.
Mitigated	In this area control mechanisms exist and are evaluated as efficient. In case there are no control mechanisms or they are not working, negative impact on company would be high. It means there is a need to monitor effectiveness of the existing control mechanisms and risk responses.
Over controlled	In this area control mechanisms are excessive in relation to the existing risks. It means there is a possibility to redeploy resources to higher risk impact areas.
Cumulative impact	Control mechanisms do not exist or are not working. Impact of one individual risk is low but cumulative impact of individual risks could be high. It means there is a need to evaluate these risks periodically and to measure their impact and vulnerability.

7. Risks and Opportunities Reporting

The Risk Map and the reports from Internal Audit and Internal Control Department audit assignments are communicated to the AmRest Management for review and undertaking of adequate action plans addressing identified risks and opportunities. The reports together with the declared action plans are communicated to the Audit Committee and Top Management for overseeing.

Internal Audit reports on a regular basis to the Top Management and to the Audit Committee results of the monitoring and verification of action plans implementation.

8. Risk Management Performance

Internal Audit communicates to the Audit Committee and the AmRest Management, evaluation of design and execution of the audited processes. The scale is from 1 to 5:

Evaluation	Key elements of the evaluation
Very Good (5)	• Control objectives are clearly defined and effectively communicated to employees. • Management has adopted a full and permanent responsibility for designing, implementing and maintaining internal control. Control mechanisms have been established and are constantly modified, based on the information and knowledge of those responsible. • There are no critical control weaknesses or other deficiencies which require immediate intervention by the Board. The IA recommendations propose alternative or additional control procedures. The existing system of internal control provides reasonable assurance that objectives will be achieved. • Policies and procedures are updated and implemented as intended. • All transactions are properly documented and archived. • All findings identified in previous audits have been timely and properly resolved.
Good (4)	• Most of the control objectives are clearly defined and communicated to all employees. • Management has assumed responsibility for the system of internal control. Periodically take action to improve and strengthen the internal control system. • There are no critical control weaknesses or other deficiencies which require immediate action by the Board. IA findings relate to the improvement of existing controls and proposals for alternative or additional inspection procedures. The existing system of internal control provides reasonable assurance that objectives will be achieved • Policies and procedures are current and are generally implemented as planned. The IA recommendations are customized for individual cases. • The main transactions are properly documented and archived. • Most of the shortcomings noted in previous audits, including all critical is timely and properly addressed.
Requires improvement (3)	• The main control objectives were defined. Employees are aware of the main control objectives. • Management has adopted partial responsibility for the system of internal controls and manages some control mechanisms. • There are critical weaknesses in internal control system. Although the existing internal control system meets the main requirements. IA findings identify areas for improvement. The existing system of internal controls supports the achievement of most major objectives. • Policies and procedures are current and are generally implemented as planned. IA recommendations relate to few weaknesses. • The main transactions are documented, however, may be difficult to recreate all the elements of the transaction. • Not all weaknesses identified in previous audits have been timely and properly resolved, however, does not apply to critical deficiencies.
Requires significant improvement (2)	• Some control objectives were defined. Employees are not aware of the validity of a number of monitoring activities. • Management is aware of its responsibility for the system of internal control, however, did not take systematic measures for permanent and effective management of the area. • There are from one to few critical weaknesses in internal control system requiring immediate management intervention. There are other controls that need improvement or need additional control mechanisms to ensure the appropriate management response to the risk. • Policies and procedures are not current and / or are not followed. There was a critical departure from the procedure and / or there are significant areas not covered by the procedures. • There are gaps in the documentation of transactions and / or problems getting to documents and restoration of all elements of the transaction.
Not acceptable (1)	• Management is not aware of its responsibility for the system of internal control. Actions to manage this area in effective manner are taken occasionally or not taken at all. • Control objectives are not defined by management. No or little responsibility for complying with the provisions of the existing procedures. • There are more than few critical weaknesses in the internal control system • Policies and procedures do not exist or are not followed. There was critical departing from the procedures and / or there are significant areas not covered by the procedures. • Documentation of transactions does not exist. It is not possible to recreate all the elements of the transaction. • No action taken to eliminate the anomalies identified in previous reports.

In addition, Internal Audit and Internal Control Department calculates risk management performance indicators which are regularly reported to the CFO and the Audit Committee. Risk management performance indicators include the number of:

- internal audits completed per annum,
- internal controls completed per annum,
- internal audit recommendations accepted by management (according to risk classification),
- internal audit recommendations not accepted by management (according to risk classification),
- management action plans (addressing identified risks and opportunities), implemented (according to risk classification),
- management action plans abandoned (according to risk classification),
- management action plans in progress (according to risk classification),
- management action plans not started or at early stage of implementation (according to risk classification),
- investigations performed,
- employees dismissed in effect of investigations.