Enterprise Risk Management

|	
Version:	1.0
Issued:	17 October 2017
Copyright:	Advanced Electronics Company

Table of Contents

SECTION 1. AEC'S POLICY ON ENTERPRISE RISK MANAGEMENT

1.1 Introduction

AEC defines risk as the "effect of uncertainty on objectives". Also it states that an effect may be positive, negative or a deviation from the expected, and that risk is often described by an event, a change in circumstances or a consequence. AEC's framework for Enterprise Risk Management (ERM) is based on the international standard ISO 31000, other standards and best practices from elsewhere are also considered as applicable.

SECTION 2. APPROACH TO MANAGE ENTERPRISE RISKS

Enterprise risks can impact an organization in the short, medium and long term. These risks are related to operations, tactics and strategy, respectively. The following diagram depicts AEC's approach towards managing enterprise risks.
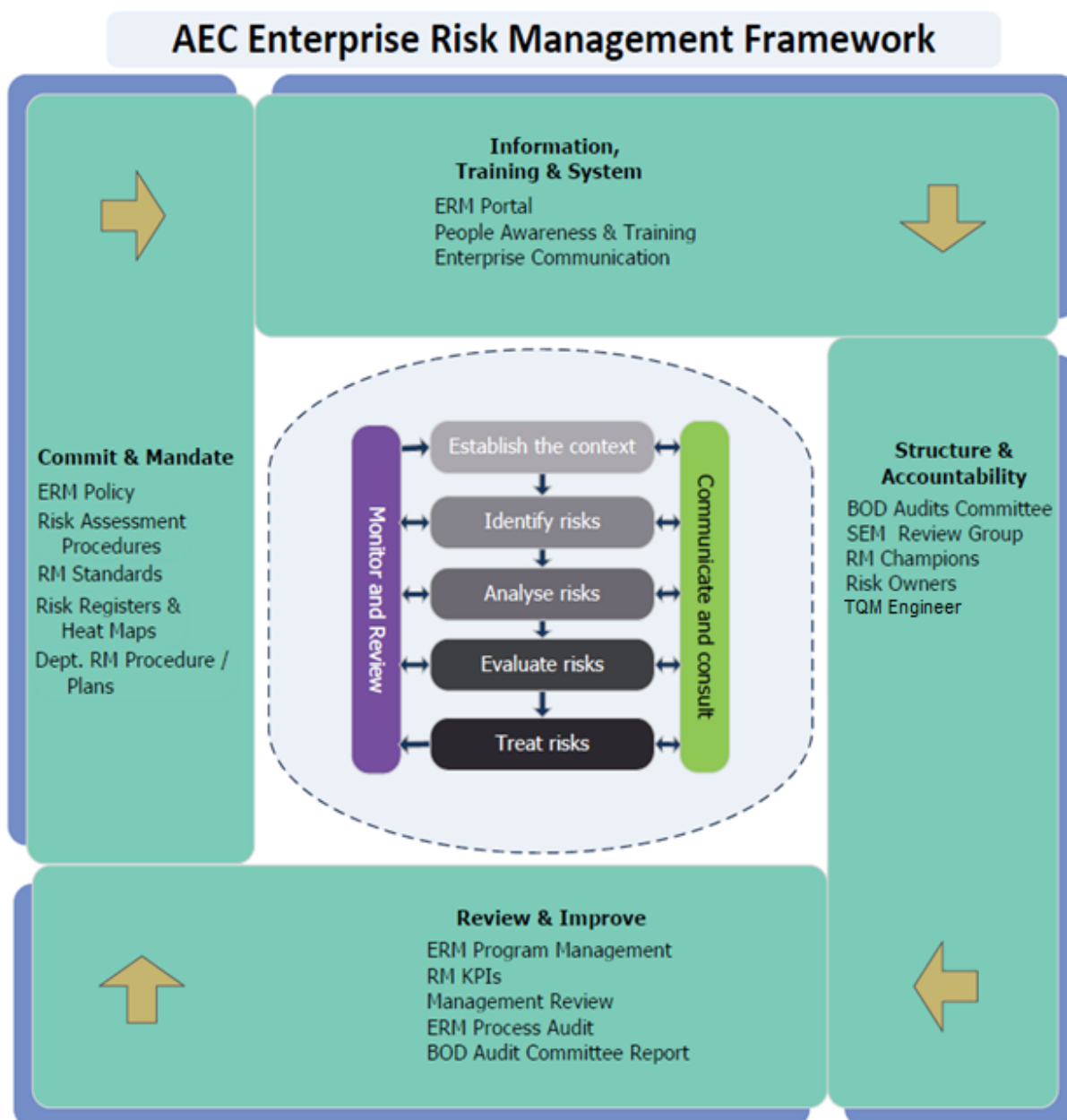
2.1 Establish the Context

Establish the context by identifying the objectives, events or relationships and then consider the internal and external parameters within which the risk must be managed. Establishing the context sets the framework within which the risk assessment should be undertaken, ensures the reasons for carrying out the risk assessment are clearly known, and provides the backdrop of circumstances against which risks can be identified and assessed.

2.2 - Risk identification

Identification of risks Involves identifying sources of risk, areas of impact, events and their causes and consequences. The risk (event) identification defines the universe of risk for AEC. These risks might create, enhance, prevent, degrade, accelerate or delay the achievements of AECs objectives.

2.3 - Risk analysis

All risks identified within each risk register shall be analysed. The likelihood and impact of consequence(s) for each risk and other factors such as effectiveness of existing controls shall be taken into consideration, as appropriate. The output of risk analysis will result in a level of risk expressed in appropriate term that is compatible with associated risk criteria

2.4 - Risk evaluation

The level of risk as determined during the risk analysis is compared with the relevant Risk criteria during this step. AEC risk criteria and thresholds, either qualitative or quantitative, shall be in terms of financial, reputational, regulatory, health and safety, security, environmental, employee, customer and operational measures. The prioritized risk register and attendant heat map depicts the risk profile for the relevant area / department and are used by the risk owners and concerned stakeholders for making decision as regards to risk treatment.

2.5 - Risk Response and Control

AEC is committed to address all its risks by appropriate responses. Risks with exposure below a predefined minimum level may not be subjected to formal risk treatment, but be attended to by the risk owner by other means such as procedural controls, check lists etc. Those that exceed this threshold shall be candidates for formal risk treatment.

SECTION 3. MONITORING AND REVIEWING

AEC Risk profile and established controls undergo changes with the ongoing changes in its internal and external environment. These are therefore continually monitored by the assigned risk owners; in doing so the risk owners shall identify emerging new risks, modification to and expiration of existing risks and changes to the effectiveness of controls, and update the risk register accordingly. Risk champions for respective areas shall review the updated risk register with the stakeholders periodically.

AEC risk management framework, process, risks and controls shall also be reviewed / monitored by the internal audit mechanism and by periodic SEM reviews.

SECTION 4. RISK AWARE CULTURE

Risk management must be integrated into the culture of the organisation and in order to obtain engagement from all employees, continuous awareness sessions on enterprise risk management are conducted. Encouraging risk-based thinking ensures that all AEC risks are identified, considered and controlled.

SECTION 5. RISK REPORTING AND RECORDING

AEC shall implement adequate internal and external reporting of significant risks and on risk management performance as appropriate. This includes reports from risk champions, Reports generated for SEM and Board of Directors.

All deliverables of ERM program including risk registers, risk assessment results and monitoring and review results shall be documented by appropriate tools and templates.