RISK MANAGEMENT POLICY

- At FSNL Risk management is Continuous Process and not an end product hence FSNL consider Risk management as a journey and not a destination.

- FSNL is committed to effective management of risks across the organization by aligning its risk management strategy to its business objectives through instituting a risk management structure for timely identification, assessment, mitigating, monitoring and reporting of risks.

- Risk management at FSNL is the responsibility of every employee both individually as well as collectively.

GUIDELINES FOR RISK MANAGEMENT

GUIDELINES FOR RISK MANAGEMENT

1. PURPOSE

Purpose of these guidelines is to ensure that an effective risk management program is established and implemented within FSNL.

2. SCOPE

These guidelines will cover activities pertaining to Risk Management across the FSNL.

3. REFERENCES

The detailed procedure for Risk Management are annexed to these guidelines.

DEFINITIONS

4.1 RISK

" Any uncertain event that could significantly enhance or impede a Company's ability to achieve it's current future objectives, including failure to capitalize on opportunities…….." Accordingly Risk Management is recognized as being concerned with both negative and positive aspects of risk.

At FSNL Risk is considered as the combination of the probability of an event and its consequences. Risk originates from uncertainty with the potential to threaten the success or survival of the company.

4.2 RISK MANAGEMENT

Risk Management is the process of defining all the risks that company faces and then building a framework to monitor and mitigate those risks.

4.3 OBJECTIVE OF RISK MANAGEMENT

- Minimisation of Risks leading to losses.
- Maximum availment of Opportunities available by not missing on the opportunities existing.
- Full utilization of resources.
- By timely analysis of risks – upside one's or downside one's.

To use risk management to increase value and provide stability for all stakeholders by managing the risk.

5.0 METHODOLOGY

The guidelines are intended to ensure that an effective risk management program is established and implemented within the company and to provide regular reports on the performance of that program, including any exceptions, to the board of Directors by Audit Committee after reviewing the reports of the Risk Management Committee.

The guidelines contain the purpose of risk management, company's approach to risk management and the risk organization structure for identification, escalation, and minimization of risks. The guidelines also specify the roles and responsibilities of the various authorities, committees and functionaries of the company.

The guidelines are complementary and not in substitution of to all other existing compliance programs, such as those relating to environmental quality, and regulatory compliance matters.

5.1 PURPOSE OF RISK MANAGEMENT

Risk management is a process, applied across the organization, to identify potential events that may affect the achievement of objectives of the company.

5.2 OBJECTIVES OF RISK MANAGEMENT

FSNL's policy is to pursue a structured approach to the effective management of risk in pursuit of business objectives. This approach and the framework for its achievement is set out in more detail below, which covers the continuous process of integrated activities by which the potential impact of risks to the achievement of company's objectives are managed. FSNL's policy is to adopt good practices in the identification, evaluation and cost effective control of risks to ensure that they are eliminated where possible, reduced to an acceptable level or managed and contained, and to embed risk management practices within management and planning activities.

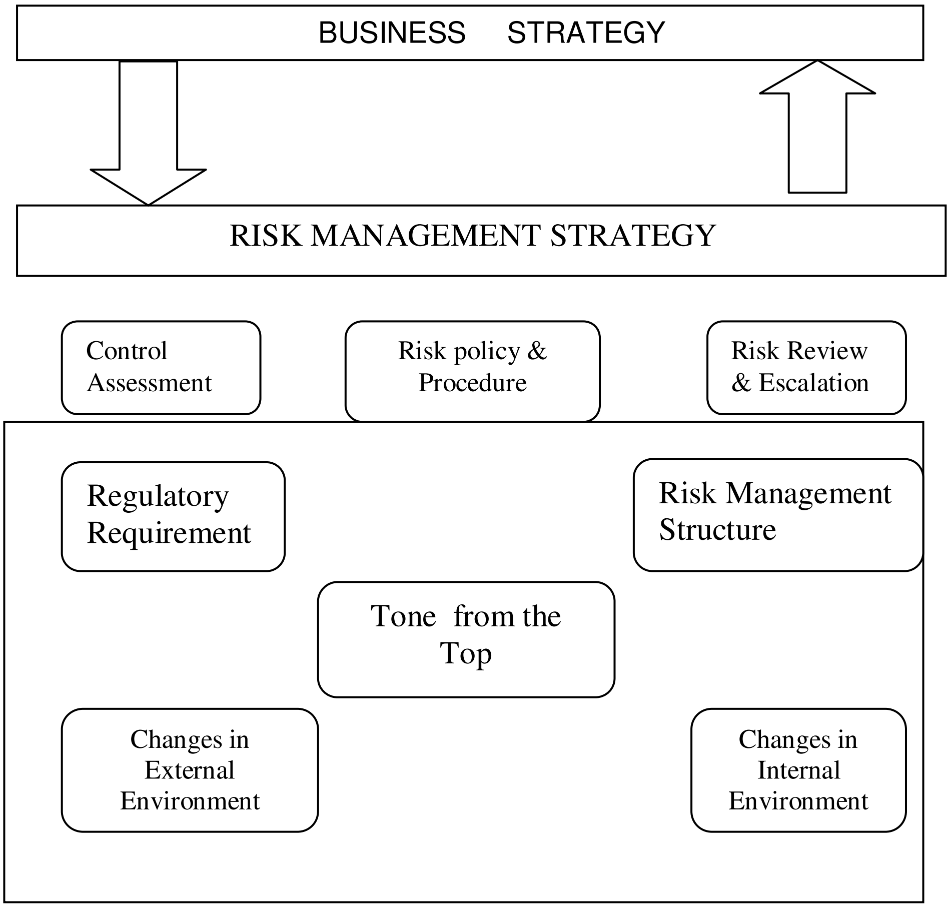
This policy is designed to ensure that the following objectives are met:

1. Identification and assessment of key risks in the context of the company's risk appetite.
2. Financial, operational and management systems directly support the management of risks that threaten the achievement of the company's objectives.
3. Identification and assessment of key risks in the context of the company's risk appetite by actively involving all employees to develop a "risk" culture that encourages all staff to identify risks and associated opportunities and respond to them with appropriate actions within and outside their own areas of responsibility.
4. Staff objectives are set in terms that reflect the company's strategic and operational risk priorities.
5. Responsibility for the management of risks is assigned to staff who have the authority to ensure that they are managed.
6. Resources are assigned to the management of risks in such a way to optimize value for money.
7. The Executive Management Board priorities in respect of risk are fully communicated down the Agency.
8. The Executive Management Board's view is informed by upward reporting of risks through the Agency. To identify, assess and manage existing as well as new risks in a planned and coordinated manner.
9. To increase the effectiveness of FSNL's internal and external reporting structure. The risk management system is functioning efficiently and effectively integrates with the Corporate and Business Planning processes.

5.3 APPROACH TO RISK MANAGEMENT

The Risk Management Strategy is developed and approved by the top management and is significantly influenced by the regulatory requirements. The strategy is implemented by developing a risk management structure, policies and procedures.

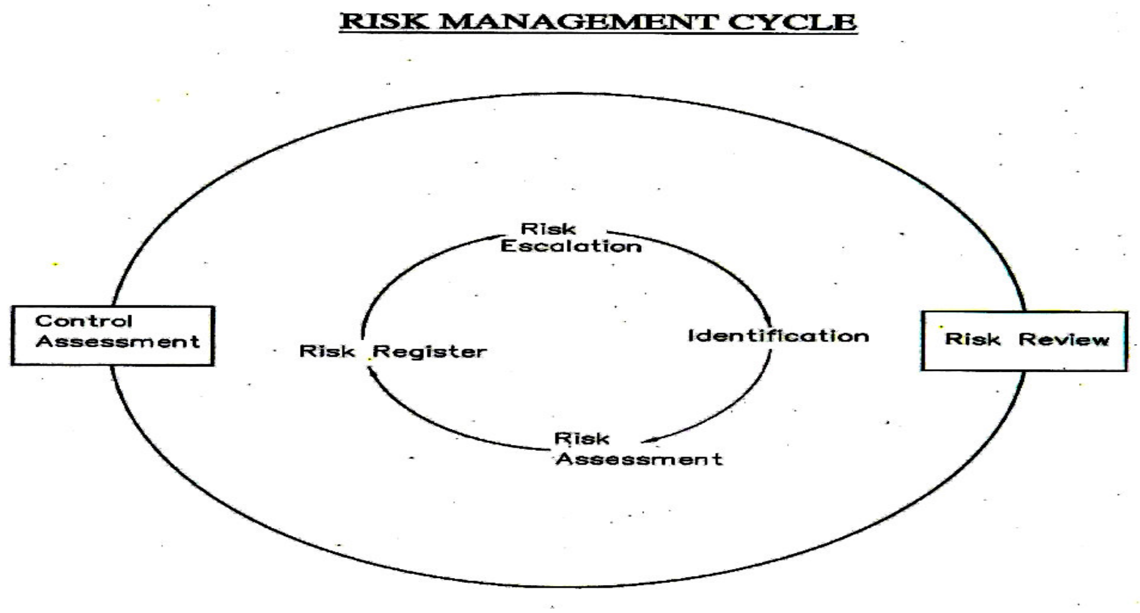
Formal authority, responsibility and accountability for designing, implementing and sustaining effective risk management processes rests with the Board of Directors. The Audit Committee, Risk Management Committee, management and other employees support and assist the Board of Directors in fulfillment of this responsibility.


BUSINESS STRATEGY
RISK MANAGEMENT STRATEGY
Control Assessment
Risk policy & Procedure
Risk Review & Escalation
Regulatory Requirement
Risk Management Structure
Tone from the Top
Changes in External Environment
Changes in Internal Environment

Functional heads of each business or function must periodically review the risks facing their business or function.

Each manager must then implement an effective system of internal controls to manage those risks, including most importantly designating responsibilities, and providing for upward communication of any significant issues that arise.

Risk management is a continuous cycle beginning with risk identification and followed sequentially by risk assessment, addition to the risk register, control assessment, risk review and risk escalation.



5.3.1 RISK IDENTIFICATION

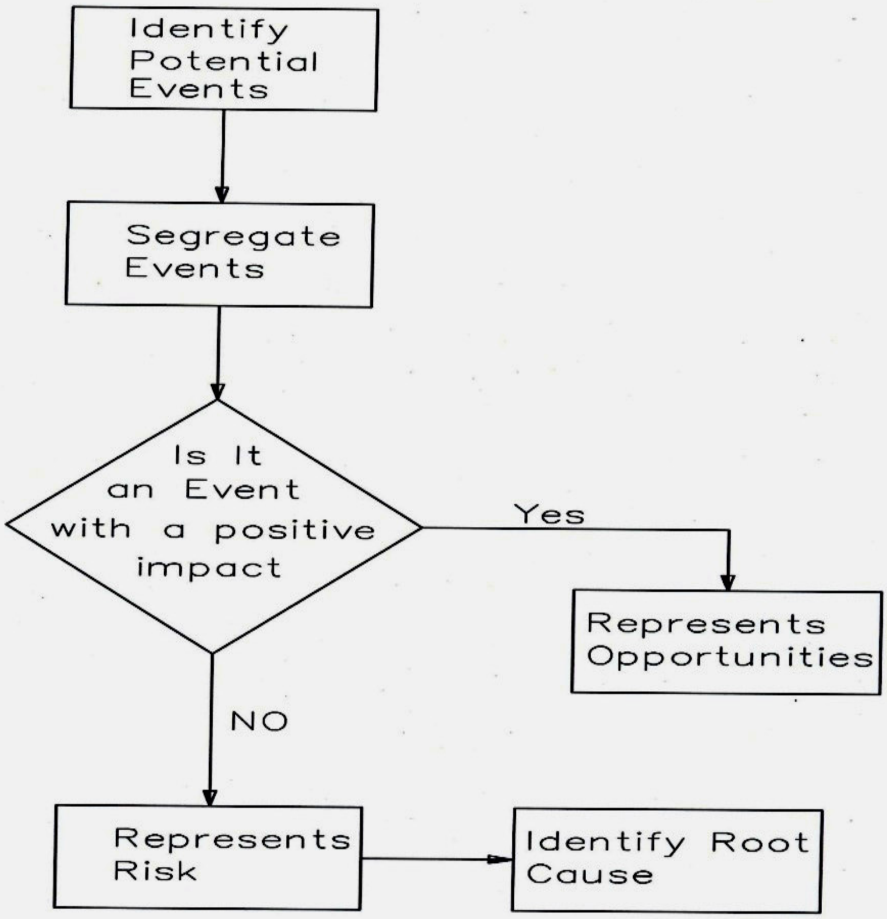
“The purpose of risk identification is to identify the events that have an adverse/bold impact on the achievement of the business objectives. ”

The identification of risks is the first step in the risk management framework. Risk identification must begin with understanding the objectives of FSNL that the process owners are responsible to achieve and the strategies that have been adopted to achieve organizational objectives. The purpose of identification of risks is to identify the events that have an adverse impact on the achievement of the business objectives.

In order to identify risks, a range of potential events will be considered while taking into account past events and trends as well as future exposures.

An event identified may have negative or positive impact. An event with positive impacts represents an opportunity and an event with a negative impact represents a risk.

ACTIVITY FLOW AT RISK IDENTIFICATION



5.3.2 RISK ASSESSMENT

“Assessment involves quantification of the impact of risks to determine potential/bold severity and probability of occurrence”

Each identified risk is assessed on a 5 point scale with respect to the following criteria for determining inherent and residual exposure:

a) Likelihood of event occurrence.

b) Impact if the event occurs

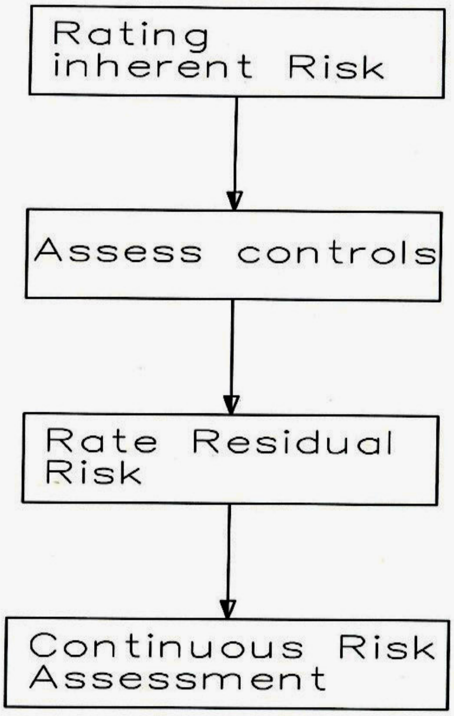
Both inherent and residual risks are to be considered in the process of risk assessment. **Inherent risk is defined as the risk faced by the organization in the absence of any actions that management might take to alter the risk’s impact or likelihood.** The combination of likelihood of event occurrence and impact provides the inherent risk exposure.

The components of gross risk i.e. the probability of occurrence and magnitude of impact are sought to be altered by putting in place certain controls. The risk that remains after the controls are put in place is termed as residual risk. The combination of residual likelihood and residual impact provides the residual risk exposure.

The Risk Assessment Table below depicts the risk exposure.

As part of the risk identification and assessment, the risk category and the treatment option for minimization is determined by the HOD.

ACTIVITY FLOW AT RISK ASSESSMENT



I RISK TREATMENT OPTIONS

The following are key risk treatment options:

a) Risk Acceptance : Risks which cannot be avoided, reduced or transferred are to be accepted by the Company.

b) Risk Avoidance: Risks whose likelihood, consequences or organizational impact is significant hence management may choose to avoid them altogether.

c) Risk Mitigation: It is an approach to reduce either the likelihood or the consequences of the risk event.

d) Risk Transfer. Transferring means soliciting the involvement of a third party to take on the impact should a risk event occur.

II RISK CATEGORIZATION

“Categorization assists in identification and assessment of the risk”

Risks are generally categorized into the following categories:

a) **Strategy & Governance Risk** – The risk threatening the achievement of the company objectives or the goals which support the vision and mission of the organization.

b) **Operational Risk** – Risks arising from the normal processes/activities of the company fall in this category.

c) **Financial Risk** – All risks which have a financial implication.

d) **Human Resource Risk** – Risks that are part of the personnel related processes (for example recruitment and performance measurement) in the company.

e) **Legal, Compliance and Regulatory Risk** – Risks arising out of non fulfillment of/non compliance with applicable compliance, legal and statutory requirements.

f) **Technology and Information Systems Risk** – Risks pertaining to storage, safety and retrieval of information and date.

g) **External Risk** – Risks arising out of the external environment. Generally, the company exercises minimal or no control over such external risks.

(Refer Annexure – 1 for checklist of key factors to be considered by senior management during risk identification and assessment)

5.3.3 RISK REGISTER

"Risk Register acts as a central repository for risks"

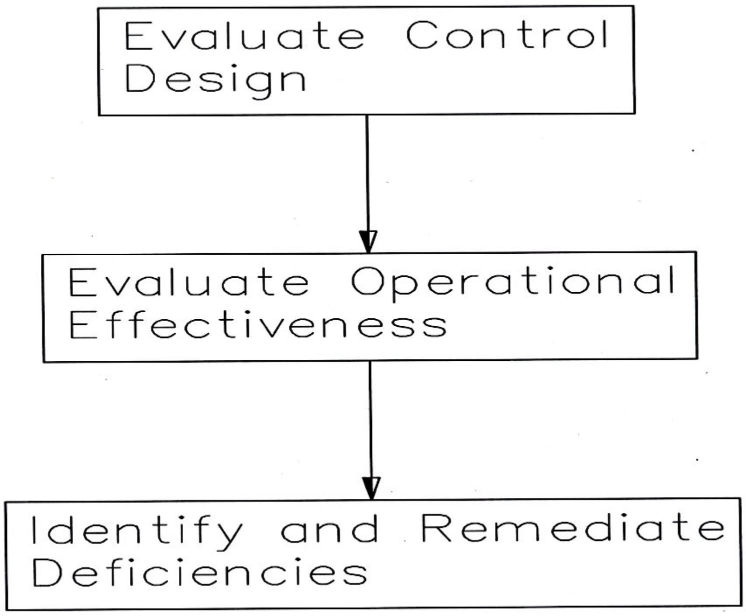
The purpose of the Risk Register record identified risks and related information in a structured manner. Reports drawn from the register are used to communicate the current status of all known risks and are vital for assessing management control, reporting and reviewing the risks faced by FSNL.

The Risk Register contains the following information with respect to each identified risk: Risk Description, Risk Owner, Root Causes, Risk Category, Inherent Risk Evaluation, Controls to mitigate the risk, Residual Risk Evaluation, Action Plan, owner, Timelines and status of action plans.

5.3.4 CONTROL ASSESSMENT

"The purpose is to assess the effectiveness of risk minimization procedures implemented by the process owners."

ACTIVITY FLOW FOR CONTROL ASSESSMENT


Evaluate Control Design
Evaluate Operational Effectiveness
Identify and Remediate Deficiencies

The control assessment is carried out in the following manner:

I EVALUATING CONTROL DESIGN:

Involves consideration of key control attributes like preventive, detective, automated and manual while designing an approach to effectively address risks. The process owner should evaluate the appropriateness of the control taking into consideration feasibility (both commercial and operating) of implementing the same and its effectiveness in addressing the risk. Key control attributes are explained below:

- **Preventive:** The controls that are put in place before the event occurs and can either be automated or manual. For example – a) physical access control to confidential data storage areas b) Specification of rigorous pre-qualification and background check procedures with respect to vendor selection activity.

- **Detective**: The controls that are to detect the risks after occurrence of the event and can either be automated or manual for example undertaking casual analysis for deviation of actual cost from budget cost.

- **Auto control:** The controls that are put in place by the computer systems. For example – Automatic serial numbering of purchase orders issued by the procurement department is an automated preventive control, while automatic exception report on performance of unauthorized activity is a detective automated control.

- **Manual controls:** These controls are implemented by the employees of organization. For example-Estimated cost /man-hours is approved by the concerned functional head.

II EVALUATING OPERATIONAL EFFECTIVESS

To check the operating effectives of the control activities testing of actual transactions is performed by persons independent of functional responsibility. The extent of testing will be decided on the basis of assessment of inherent risk. For a high rated risk the controls should be tested extensively and frequently.

III IDENTIFY AND REMEDIATE DEFICIENCES

On the basis of testing results the deficiencies are identified. For identification of deficiencies various factors need to be taken into consideration for example.

- The size of operations,
- Complexity and diversity of activities,
- Organizational structure, and
- Likelihood that the control deficiency could result in a misstatement of the company's financial records.

5.4 RISK REVIEWS

"Risk review involves re-examination of all risks recorded in the risk register to ensure that the risk assessment as currently recorded remain valid" The risk review will be conducted by the management to monitor the effectiveness of the risk assessment framework.

Risk review also involves the following:

- Assessment of completeness and validity of risks recorded in the risk register
- Assessment of changes in the business processes, operating and regulatory environment since the last risk assessment and corresponding changes required in the risk profile, risk appetite and risk management procedures of the organization.

- Reviewing efficacy and implementation status of actions plans for identified risks and revision in action plans.

5.5 RISK ESCALATION

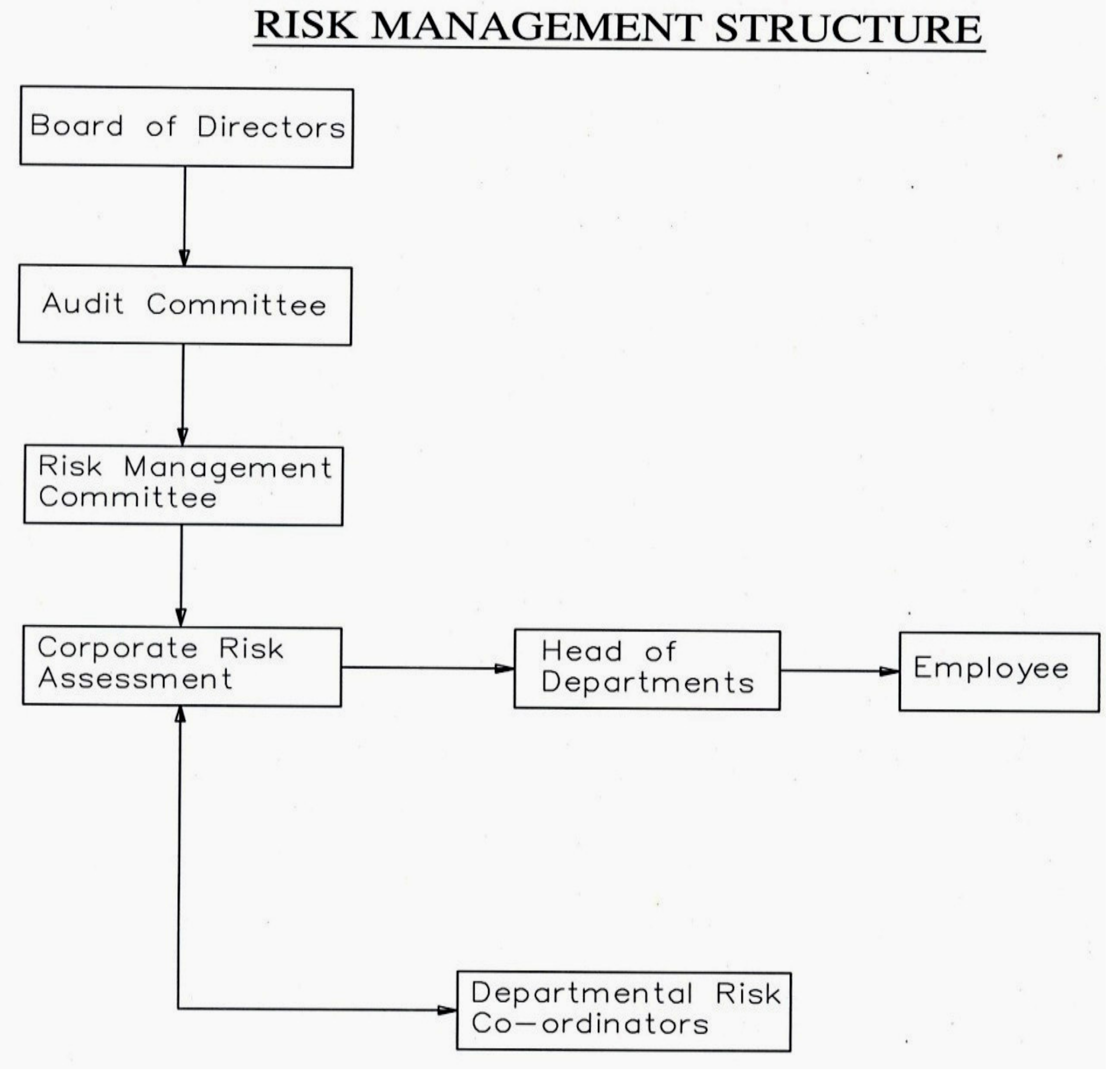
"The Escalation matrix is a tool which links the results of risk assessment with the organization structure and responsibility levels"

For prompt communication and timely follow up of specific issues, risk escalation is critical for effective risk management. The communication of key risk information is also important to ensure that all significant risks identified in a department are considered in the context of the overall operations of FSNL in a coordinated and consistent manner.

The Escalation Matrix is a tool which links the results of the risk assessment with the organization structure and responsibility levels. It specifies the levels in the organization structure to which the risks with different magnitude and impact recorded in the risk register are to be escalated based on the significance arrived at as part of the risk assessment process.

5.6 RISK MANAGEMENT STRUCTURE

A formal Risk Organization Structure with defined roles and responsibilities for risk management activities is an essential prerequisite for effective risk management framework 2.


RISK MANAGEMENT STRUCTURE
Board of Directors
Audit Committee
Risk Management Committee
Corporate Risk Assessment
Head of Departments
Employee
Departmental Risk Co-ordinators

5.6.1 RISK MANAGEMENT – ROLES AND RESPONSIBILITIES

The risk management roles and responsibility are shown in annexure-II

5.6.2 RISK MANAGEMENT COMMITTEE(RMC)

I COMPOSITION

The RMC shall comprise of following:

- Executive Director(P&C)/ CGM is appointed Chairman of RMC.
- Representative executives from all directorates of the company.
- In addition, the Chairman of the RMC may invite other personnel.

II FREQUENCY OF MEETINGS

The RMC shall ordinarily meet on a quarterly basis or as required for urgent or other matters. Reports of RMC's activities (agendas, decisions) and meetings (including attendance and minute record) will be maintained for each meeting by the Risk Management Committee secretary.

III DELIVERABLES

At a minimum, the RMC shall deliver the following:

- Highlight significant changes in the risk profile to the Audit Committee.
- Changes/events outside the risk appetite of FSNL.
- Changes/modifications to the risk management process.
- Changes to be made in the risk register.
- Quarterly report on testing of controls highlighting compliance/non compliance with controls set out.
- Updates on action plan status.

The RMC will ensure and deliver the following:

- Filling and maintenance of risk identification/deletion/modification forms.
- Summary of proposed changes to risk profile for validation by the RMC.
- Periodic reports of risks, controls and action plans identified in the risk register.
- Periodic detailed and summary reports on control testing carried out, gaps identified and action plans agreed with heads of departments.
- Centrally maintain risk register as per the prescribed format for the entire organization as a whole.

5.7 RISK MANAGEMENT PROCEDURES

- Risk Management procedures have been developed by the management to assist in establishing and maintaining an effective risk management framework.

- These are intended to act as standard reference guides for designated employees in effectively discharging their risk management responsibilities.

- Detailed risk management procedures are specified in a separate document Titled 'Risk Management Procedures' approved by the management.

5.8 WHISTLE BLOWER

The whistle blower policy is a communication channel for employees to report to the Management the concerns about unethical behaviour, actual or suspected fraud or violation of the company's code of conduct or ethics policy.

Employees are assured that corrective action will be initiated after due diligence of reported incidents. By closely guarding the identity of the provider of information, the concerned employee is protected from any retaliation.

5.9 IMPLEMENTATION OF THE GUIDELINES:

The Guidelines shall be applicable as soon as it is adopted by the Board of Directors.

5.10.1 ESTABLISHING A RISK CULTURE WHICH INCORPORATES THE FOLLOWING:

- Using common risk language and concepts.

- Communicating about risk using appropriate channels and technology.

- Developing training programs for risk management.

- Identifying and training risk experts.

- Developing suitable knowledge sharing system.

- Include risk management activities in job description.

- Embed, Measure and Monitor.

5.10.2 IDENTIFY KEY PERFORMANCE INDICATORS AND CRITICAL SUCCESS FACTORS RELATED TO RISK

- Establish success measures for risk strategy and activities.

- Provide a periodic process measuring risk and return.

- Identify and implement monitoring processes and methods of feedback.

- Establish feedback mechanism and amend system and methodology as per requirement.

5.11 VALIDITY OF THE GUIDELINES

- The guidelines are valid indefinitely in its entirety unless amended by the Board Of Directors.

Annexure – I

Identifying and Assessing Risk

Checklist of Key Factors to be considered by the Senior Management during risk identification and assessment

Strategic Risk	* Are the critical strategies appropriate to enable the organization to meet its business objectives? * What are the risks inherent in those strategies, and how might the organization identify, quantify, and manage these risks? * How muck risk is the organization willing to take?
Operational Risk	* What are the risks inherent in the processes that have been chosen to implement the strategies? * How does the organization identify, quantify and manage these risks given its appetite for risk? How does it adapt its activities as strategies and processes change?
Human Resource Risk	* What are the risks inherent in the selection, training and separation process of the company?
Legal, Compliance and Regulatory Risk	* What risks are related to compliance with regulations or contractual arrangements?
Financial Risk	* Have operating processes put financial resources at undue risk? * Has the organization incurred unreasonable liabilities to support operating processes? * Has the organization succeeded in meeting business objectives?
Technology and Information Risk	* Is our data/information/knowledge reliable, relevant, and timely? * Are our information systems reliable?
External Risk	* What risks have yet to develop? (These might include risks from new competitors, recession risks, outsourcing risks, political or criminal risks, and other crisis and disaster risks.

10 Risk Registers

FSNL has adopted a standard format risk register, a sample of which is shown below:

Sample Alternative 1

Risk No.	Key Business Risk	Risk Proximity	Absolute Risk Assessment			Miti-gation	Residual risk Assessment			Risk Owner	Review Date
			Impact	Like lihood	Risk-score		Impact	Like lihood	Risk Source		
1											
2											
3											
4											

Sample Alternative 2

Sr. No.						
Process	Human Resource	Division	Personnel			
Sub Process	Manpower Planning	Department	HR Planning & Management			
Risk Category	Human Resource					
Risk Description	Shortfall/Surplus in Manpower as against actual organizational needs					
Risk Owner	Chief General Manager– Personnel & Administration					
Control Objective	Minimise deviations of actual manpower from required Manpower strength					
	Inherent impact	Inherent Likelihood	Inherent Exposure			
Inherent Evaluation						
Root cause	Key controls	Control Assessment	Action Plan	Action Plan Owner	Target	Action Plan Status

Procedure

For

Risk

Management

PROCEDURE FOR RISK MANAGEMENT

1.0 PURPOSE

Purpose of this procedure is to define the approach and process of Risk Management in FSNL.

2.0 SCOPE

This procedure will cover activities pertaining to Risk Management in all Divisions / Departments of FSNL.

3.0 REFERENCES

None

4.0 DEFINITIONS

Risk

The possibility of an event occurring that will have an impact on the achievement of business objectives of FSNL. Risk emanates from uncertainty with the potential to threaten the success or survival of the company.

Risk Management

Risk Management is structured, consistent and continuous process for identification and assessment of risks, deciding the control assessment and continuous monitoring of exposure of the risk.

Risk Management Structure

A formal Risk Organization Structure with defined roles and responsibilities of FSNL and its employees for risk management activities.

5.0 METHODOLOGY AND CONTROLS

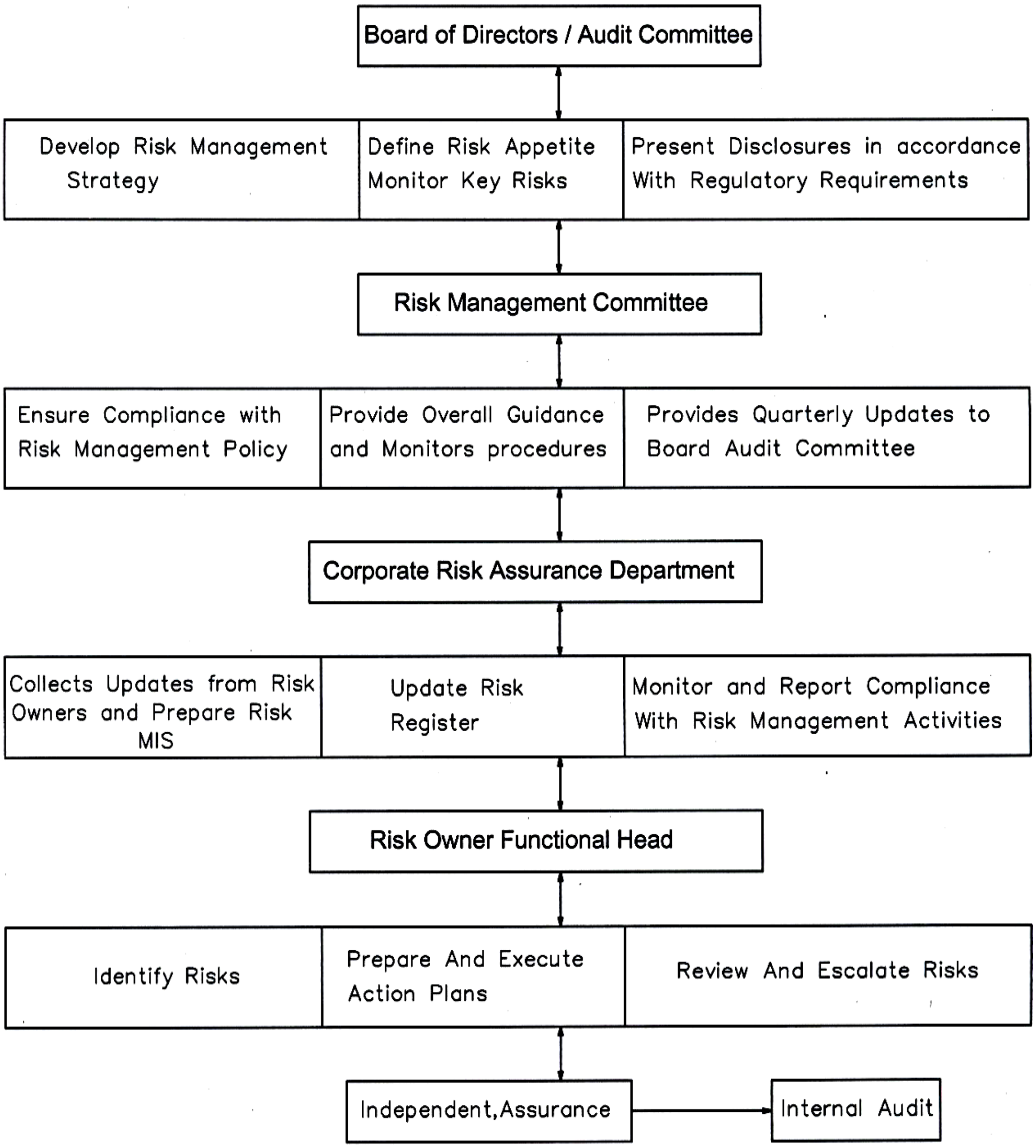
5.1 Overall Risk Management Process at FSNL

Risk Management at FSNL begins with approval of the risk management strategy by the Board of Directors. The responsibility of overseeing and ensuring compliance with the Risk Management Policy at FSNL is entrusted to the Risk Management Committee (RMC) at the ED(P&C) /CGM level. In addition to providing overall guidance and monitoring risk management procedures, the RMC also provides Quarterly updates to the Board of Directors and the Audit Committee.

The Risk Management Committee (RMC) is responsible for day to day implementation of the risk management process and collates updates from the risk owners and prepares the relevant MIS. RMC is also responsible for updating the risk register and monitoring and reporting compliance with risk management activities.

Head of department are responsible for identifying risks and preparing and executing actions plans within their own areas of responsibility. Head's of department are also responsible for reviewing and escalating risks. The overall Risk Management process at FSNL is shown in Figure.

OVERALL RISK MANAGEMENT PROCESS
RISK MANAGEMENT GUIDELINE AND PRODUCE


Board of Directors / Audit Committee
Develop Risk Management Strategy
Define Risk Appetite Monitor Key Risks
Present Disclosures in accordance With Regulatory Requirements
Risk Management Committee
Ensure Compliance with Risk Management Policy
Provide Overall Guidance and Monitors procedures
Provides Quarterly Updates to Board Audit Committee
Corporate Risk Assurance Department
Collects Updates from Risk Owners and Prepare Risk MIS
Update Risk Register
Monitor and Report Compliance With Risk Management Activities
Risk Owner Functional Head
Identify Risks
Prepare And Execute Action Plans
Review And Escalate Risks
Independent,Assurance
Internal Audit

5.2 Overall Procedure for Risk Management at FSNL

5.2.1 The board of directors approves the risk management policies and procedures.

5.2.2 All risks / issues identified by employees or the CRA department are forwarded to the concerned.

5.2.3 Risks identified are validated by the Head's of Department in a validation meeting with representatives from the CRA department.

5.2.4 RMC Forwards the appropriate 'Summary of Proposed Changes to the Risk Register'-MIS to the concerned Head's of department, Executive directors.

5.2.5 RMC also forwards control testing reports to the head's of department, Executive Directors.

5.2.6 Executive Directors seek clarifications (if required0 on proposed changes to the risk registers from the concerned head of department.

5.2.7 The Risk Management Committee reviews the proposed changes to the risk register and approves changes as required.

5.2.8 RMC carries out changes to the risk register.

5.2.9 RMC prepares periodic reports on changes in the key risk portfolio and proposed changes in risk management procedures and forwards them to the directors and the audit committee.

5.2.10 The risk management committee reports to the audit committee/committee of functional directors.

5.2.11 The audit committee/committee of functional directors seeks clarifications (if required) from the risk management committee.

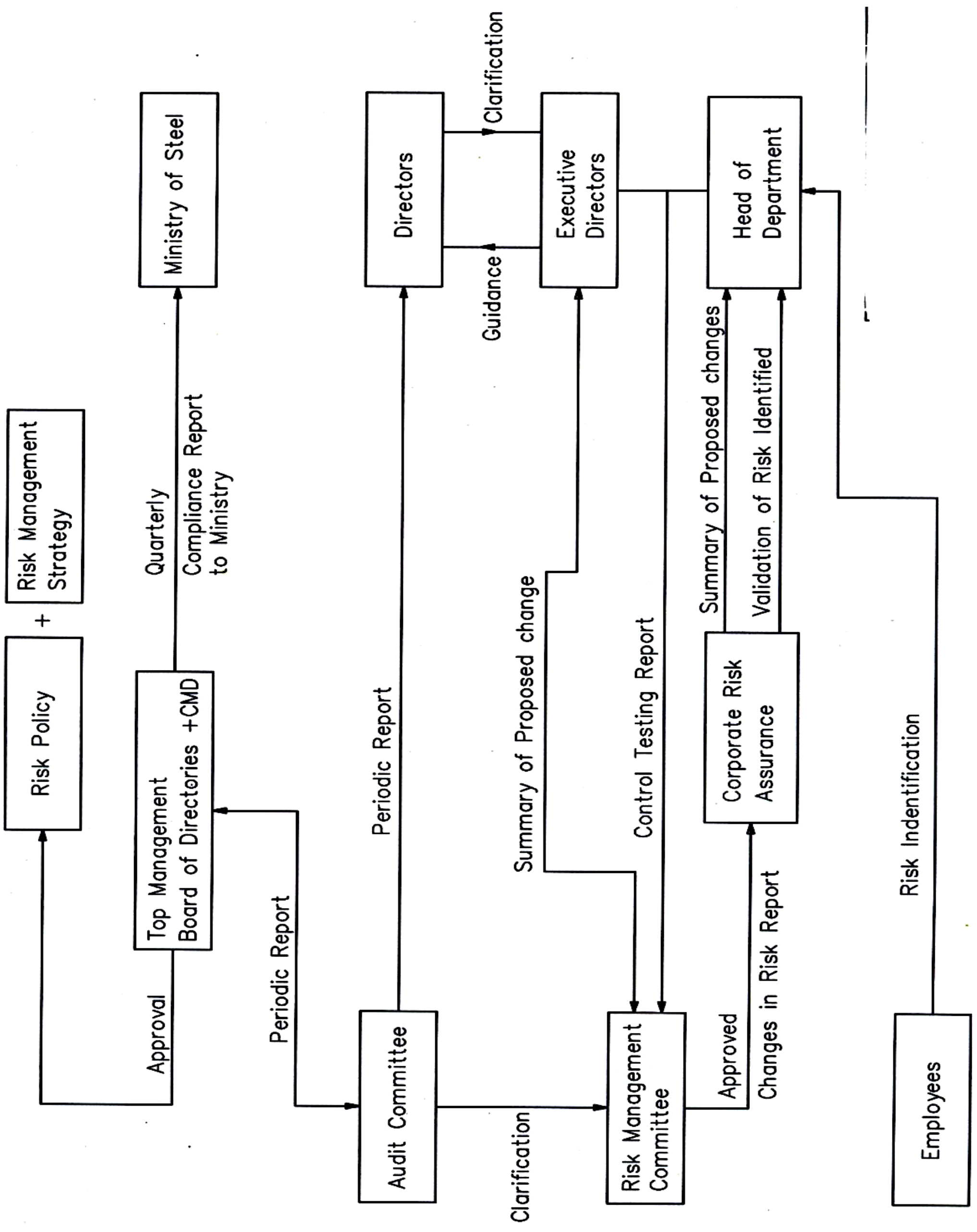
5.2.12 The Directors seeks clarifications (if required) from the concerned Executive Directors.

5.2.13 Directors provide guidance and inputs to the Executive Directors.

5.2.14 The Audit Committee sends a periodic report to the Board of Directors.

5.2.15 The flow of information for risk management and reporting activities across FSNL is depicted in the diagram below;

OVERALL FLOW OF INFORMATION FOR RISK MANAGEMENT ACTIVITIES AT FSNL



5.3 Risk Management Approach at FSNL

Risk Management Approach at FSNL includes the following five activities i.e. Risk Identification, Risk Assessment, Risk Register, Control Assessment and Risk Review. Figure 5.3 depicts the process for Identification, Assessment and Recording.

5.3.1 Risk Identification

a) Identification of risks is a continuous process and is carried out by employees.

b) Common sources for identification of risks for example include the following:
Operating and financial results, reports and analysis of the company.
Concern areas highlighted during operational meetings.

- Complete Quarterly Risk Questionnaires.

- Triggers for Identification/Modification in Risk Portfolio.

Relevant information from public domain

c) Each identified risk is required to be formally validated by respective HOD and if applicable is escalated within the organization as per the prescribed Escalation matrix for validation by designated officials.

d) Corporate Risk Assurance personnel facilitate in risk identification process by undertaking the following activities:

- Holding risk and control awareness workshops for the employees at periodic intervals.

- Providing consultation/guidance with respect to risk identification process and its application to employees and process owners as applicable.

Provide relevant extracts from Risk Register of FSNL to the concerned process owner upon receipt of a formal requisition in this regard.

Record identified risks in specified standard formats in consultation with the respective process owners.

e) Respective HOD is responsible for timely identification and escalation of the risks in his functional domain.

5.3.2 Risk Assessment

a) HOD of the respective functional area is responsible for determining both the inherent and residual risk rating for each identified risk (in own domain) by undertaking the following:

Determine inherent likelihood of event occurrence and the severity level of the impact if the event occurs on the basis of selected rating parameters from the valid risk rating criteria.

Inherent exposure is arrived at by multiplying the ratings for inherent likelihood and inherent impact.

Engage concerned employees in determination of the risk rating.

Identify the existing/required key controls for minimizing the identified risk.

Determines the responsibility, type, extent of control required for each identified risk.

Develop action plans for implementing and strengthening the related key controls.

Determine residual likelihood of event occurrence and the severity level of the impact if the event occurs on the basis of selected rating parameters from valid risk rating criteria.

Residual exposure is arrived at by multiplying the ratings for residual likelihood and residual impact.

b) RMC actively facilitates the risk assessment process by providing functional support in terms sharing knowledge with respect to risks and controls and maintenance of related records.

c) Respective HOD is required to escalate the identified risk as per the risk escalation matrix prescribed for FSNL.

5.3.3 Risk Register

a) RMC centrally maintains the record of risks, controls and action plans identified, compiles and approval regular basis.

b) RMC is the owner of risk register at FSNL, hence all identified risks, related controls and action plans are discussed and approved by the RMC in the Quarterly Meeting.

c) Clarifications/Explanations required by the RMC (if any) are provided by the process owners.

d) Changes in key risks, related controls and action plans are escalated by RMC to the Audit Committee for approval.

e) Audit committee accords approval to the change in key risks profile in discussion with RMC and process owners as applicable.

f) RMC is responsible for updating the risk register (maintained centrally) in terms of approval accorded by Audit Committee as applicable.

5.3.4 Control Assessment

The Purpose of Control Assessment is to assess the effectiveness of risk minimization Procedures implemented by the process owners. Control assessment at FSNL is carried out as follows:

a) Respective HOD is responsible for identification and implementation of effective and efficient key controls for minimization of identified risks.

b) RCM assists in implementation of key controls by undertaking the following:

Developing an annual calendar for control assessment activities, including periodic testing of controls ensuring adequate coverage and frequency of testing of all key controls implemented at FSNL.

Determine nature, timing and extent of control testing required and agree the testing and reporting schedule with the respective process owners. Provide support to respective process owners (as required) in designing effective and efficient controls.

Timely submission of reports on testing of key controls to the respective process owners highlighting the weaknesses and recommend improvements.

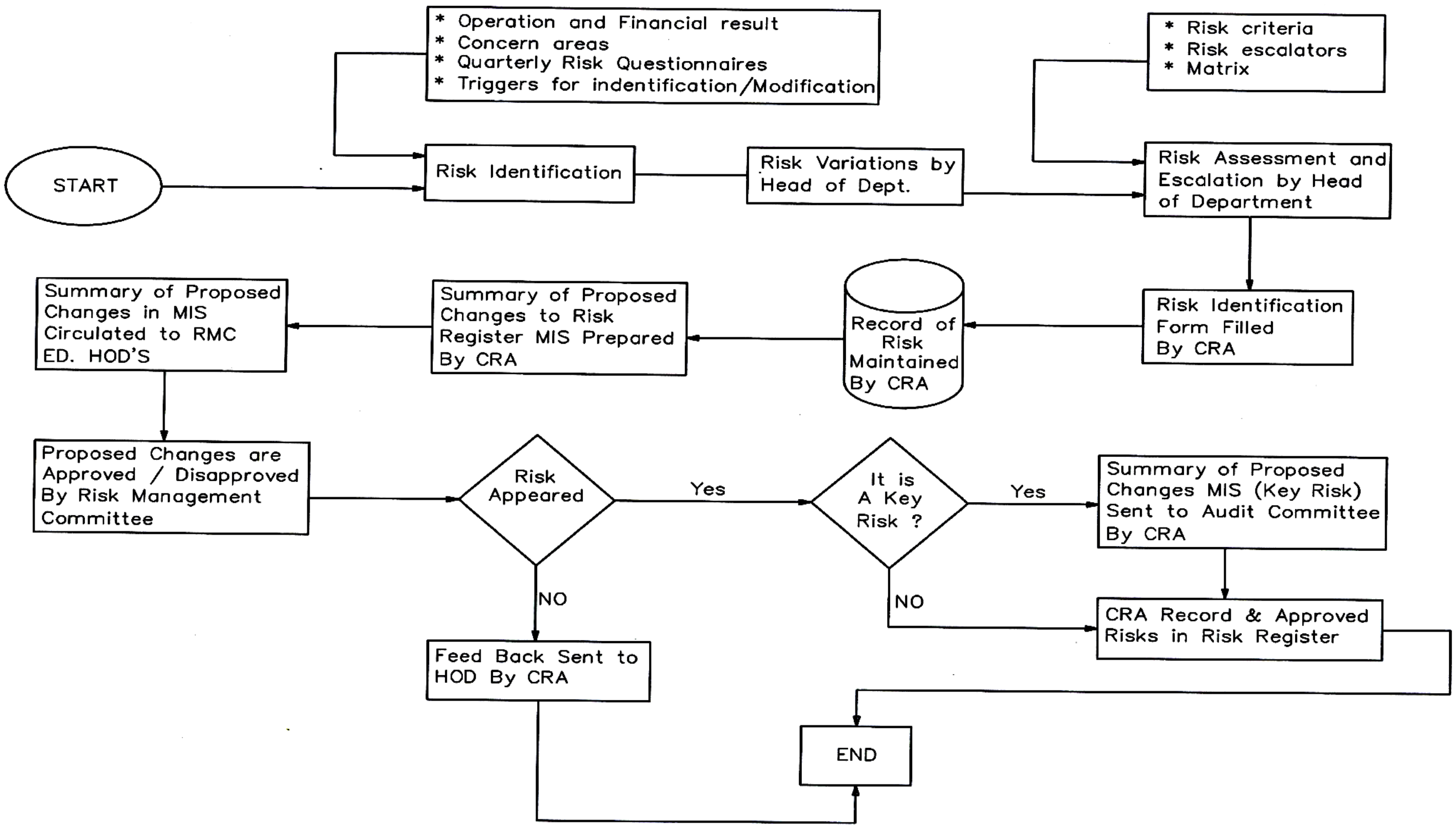
Preparation and submission of periodic reports to respective HOD, concerned Executive Director and to the RMC on implementation status of agreed key controls.

Obtain comments from respective process owners with respect to delays, difficulties and non-implementation of key controls for review by RMC and the Audit Committee as applicable.

- RMC reviews the process for control assessment, results of the control testing carried out by process owners and implementation status of approved controls.

- Audit Committee reviews the process for control assessment as part of the periodic assessment of overall risk management framework at FSNL.

ACTIVITY FLOW FOR CONTROL ASSESSMENT


* Operation and Financial result
* Concern areas
* Quarterly Risk Questionnaires
* Triggers for indentification/Modification
* Risk criteria
* Risk escalators
* Matrix
START
Risk Identification
Risk Variations by Head of Dept.
Risk Assessment and Escalation by Head of Department
Risk Identification Form Filled By CRA
Record of Risk Maintained By CRA
Summary of Proposed Changes to Risk Register MIS Prepared By CRA
Summary of Proposed Changes in MIS Circulated to RMC ED. HOD'S
Proposed Changes are Approved / Disapproved By Risk Management Committee
Risk Appeared
Yes
NO
It is A Key Risk ?
Yes
NO
Summary of Proposed Changes MIS (Key Risk) Sent to Audit Committee By CRA
CRA Record & Approved Risks in Risk Register
Feed Back Sent to HOD By CRA
END

5.3.5 Risk Review

The risk reviews involve:

a) Assessment of completeness and validity of risks recorded in the risk register.

b) Assessment of changes in business processes, operating and regulatory environment etc. and corresponding changes in the risk profile, risk appetite and risk management procedures.

c) Reviewing efficacy and implementation status of action plans for identified risks and revision in action plans.

Refer Flow Chart of activity flow of Quarterly Risk Review.

The Quarterly and Annual reviews at FSNL are carried out as follows:

I) **Quarterly Risk Review by RMC and Audit Committee**

a) At the end of every quarter each HOD is required to submit completed quarterly risk review questionnaires to the RMC.

b) Subsequent to receipt of completed risk review questionnaires, RMC categories and consolidates the responses for the company as a whole and also fills the modification/deletion forms.

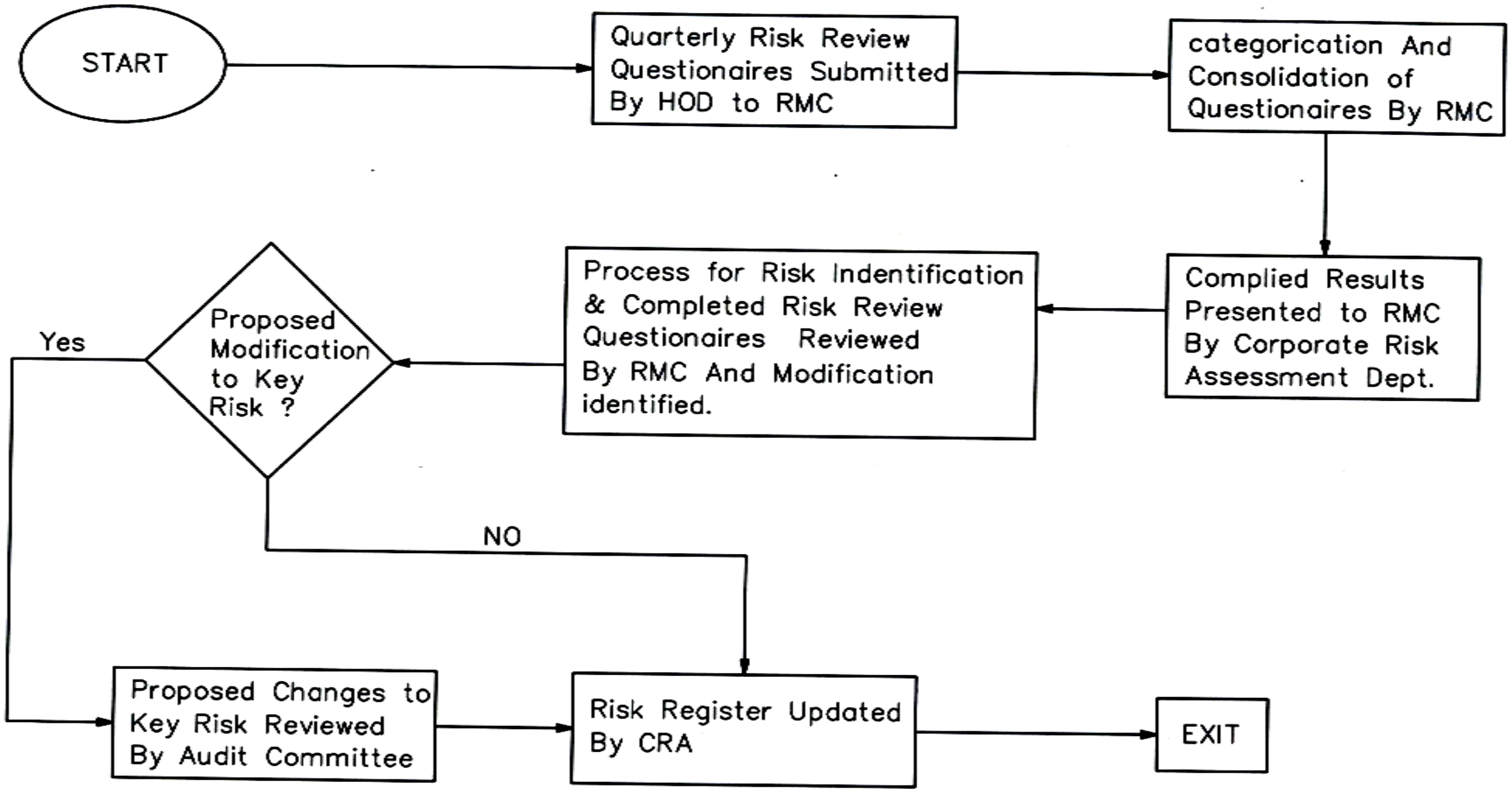
c) RMC reviews the process adopted for identification of risks, completed risk review questionnaires and explanations provided by the process owners. Accordingly the RMC may make suitable modifications in the risk register including addition of new risks, controls and actions plans identified by the RMC itself.

d) Proposed modifications to the existing company wide key risk portfolio i.e. additions, deletions or modification (change in risk description root causes, controls or action plans) are escalated to the audit committee for review and approval before changes are made to the risk register.

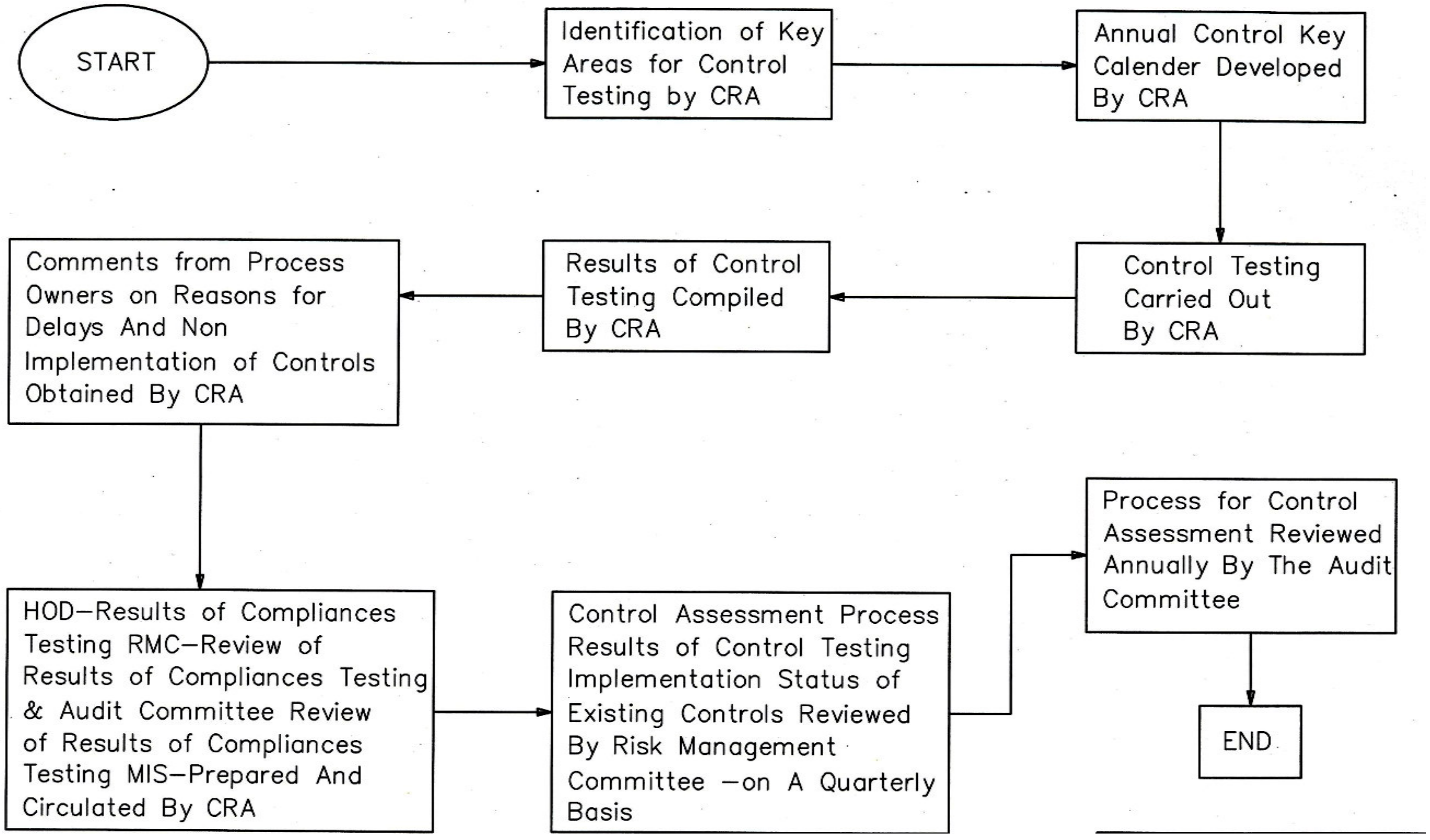
e) Audit committee reviews the proposed changes and may approve/approve with modifications/reject the proposed changes.

f) RMC centrally updates the FSNL Risk Register in accordance with the modifications reviewed by the RMC and Audit Committee as applicable.

QUARTERLY RISK REVIEW BY RISK MANAGEMENT COMMITTEE AND AUDIT COMMITTEE


START
Quarterly Risk Review Questionaires Submitted By HOD to RMC
categorication And Consolidation of Questionaires By RMC
Complied Results Presented to RMC By Corporate Risk Assessment Dept.
Process for Risk Indentification & Completed Risk Review Questionaires Reviewed By RMC And Modification identified.
Proposed Modification to Key Risk ?
Yes
NO
Proposed Changes to Key Risk Reviewed By Audit Committee
Risk Register Updated By CRA
EXIT

ACTIVITY FLOW FOR CONTROL ASSESSMENT


START
Identification of Key Areas for Control Testing by CRA
Annual Control Key Calender Developed By CRA
Control Testing Carried Out By CRA
Results of Control Testing Compiled By CRA
Comments from Process Owners on Reasons for Delays And Non Implementation of Controls Obtained By CRA
HOD–Results of Compliances Testing RMC–Review of Results of Compliances Testing & Audit Committee Review of Results of Compliances Testing MIS–Prepared And Circulated By CRA
Control Assessment Process Results of Control Testing Implementation Status of Existing Controls Reviewed By Risk Management Committee –on A Quarterly Basis
Process for Control Assessment Reviewed Annually By The Audit Committee
END

II) Annual Risk Review by RMC and Audit Committee

a) On an annual basis each HOD is required to carry out an exhaustive review of the existing portfolio of risks for own functional domain, by evaluating changes in internal business processes, internal operating structure and relevant external factors (if any). Identified proposed changes are communicated to the RCM.

b) Parallel to the review by HOD's, RCM on the basis of completed past risk review questionnaires and knowledge of risk profile of the company as a whole, carries out an exhaustive review of the risk register for identification of required changes.

c) RCM in consultation with process owners also identifies required modifications to the existing risk management processes.

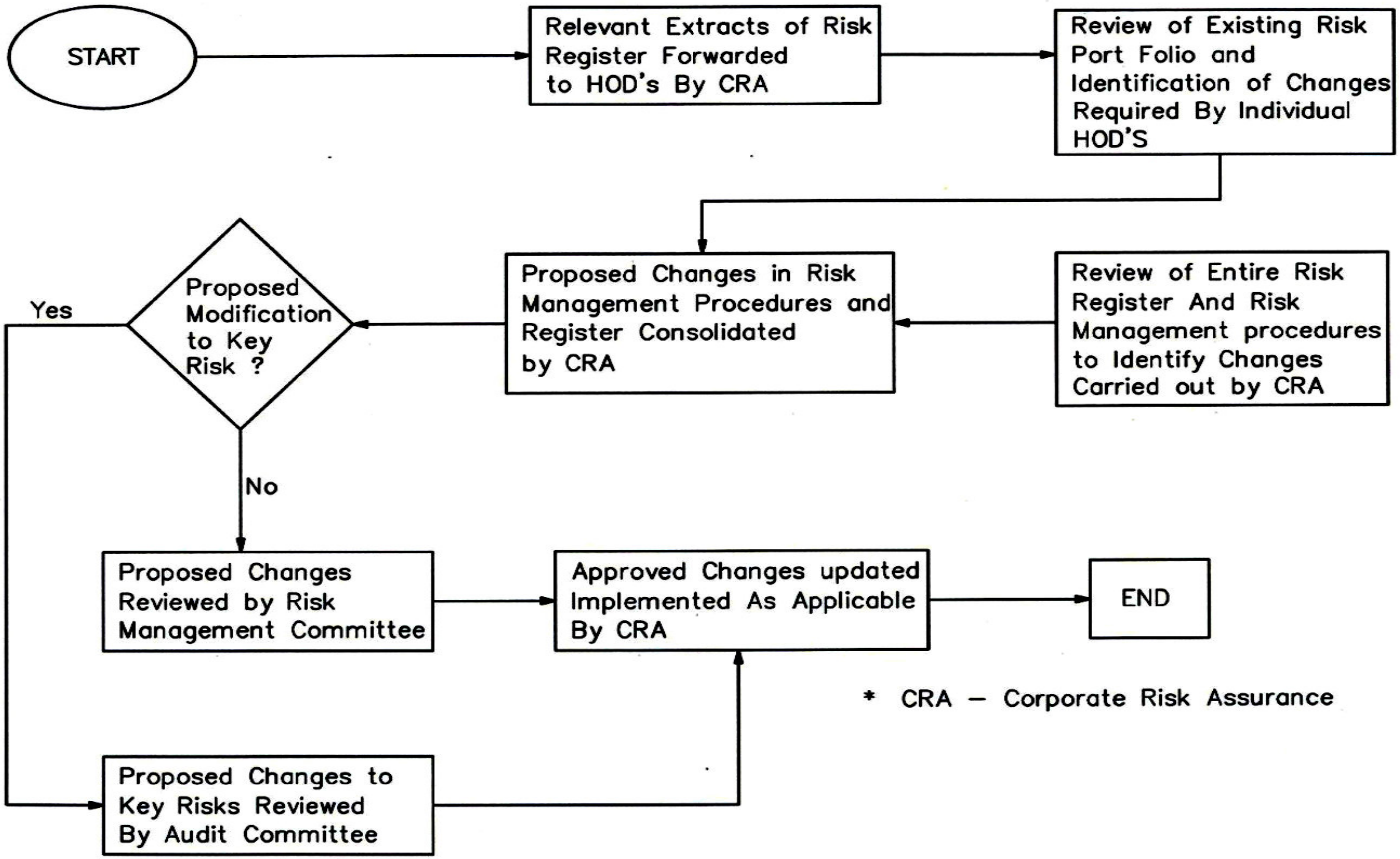
d) Changes to the risk management processes and risk register are consolidated and categorized by RMC.

e) Proposed changes identified by the process owners to the Risk Register are presented to the RMC for its approval and implementation.

f) Proposed modifications to key risks in the risk register are forwarded to the Audit Committee for its approval (in discussion with process owners as applicable).

RCM updates the risk register and risk management procedures as per the recommendations of the Risk Management Committee and the Audit Committee.

ACTIVITY FLOW ANNUAL RISK REVIEW (ANNUAL RISK REVIEW)


START
Relevant Extracts of Risk Register Forwarded to HOD's By CRA
Review of Existing Risk Port Folio and Identification of Changes Required By Individual HOD'S
Proposed Changes in Risk Management Procedures and Register Consolidated by CRA
Review of Entire Risk Register And Risk Management procedures to Identify Changes Carried out by CRA
Proposed Modification to Key Risk ?
Yes
No
Proposed Changes Reviewed by Risk Management Committee
Approved Changes updated Implemented As Applicable By CRA
END
Proposed Changes to Key Risks Reviewed By Audit Committee

* CRA — Corporate Risk Assurance

5.4 Escalation Strategy

a) Matters pertaining to a function identified by employees /during operational meetings are escalated to the respective HOD.

b) The HOD on validating a change in the risk profile together with RCM completes relevant risk identification/modification or deletion form.

c) RCM consolidates the individual addition/deletion/modification forms into the Summary of proposed changes and forwards a copy of the summary to the concerned HOD, ED.

d) RCM modifies the risk register in accordance with the changes approved by RMC/Audit committee as applicable.

e) Risks which materialize are escalated to the concerned authority as per the escalation matrix in accordance with the severity level.

5.5 Agenda for Quarterly meetings (Audit Committee and RMC)

I) Audit Committee Meeting

The Audit committee meets quarterly to review the functioning of the risk management framework implemented at FSNL.

During the meeting the following reports are discussed:

a) Audit Committee – Review of the risk portfolio (Only Key Risks)
b) Audit Committee – Summary of proposed changes to the Key Risks Portfolio.
c) Audit Committee – Review of risk management process.
d) Audit Committee – Review of Compliance Testing.
e) Audit Committee – Review of Default/Delay in completion of action plans (Only Key Risks).

II) RMC Meeting

The RMC meets quarterly for reviewing the risk and control framework implemented at FSNL.

During the meeting the following reports are discussed:

a) Overall Review of Company wide risk portfolio.
b) Default/Delay in completion of Action plan.
c) Review of the results of compliance testing by RCM.
d) Summary of proposed changes to the risk register.

5.6 Reports to be reviewed by HOD

Each HOD should review the following reports on a regular basis:

a) Default/Delay in completion of Action Plan.
b) Review of the results of compliance testing by RCM.
c) Summary of proposed changes to the risk register.

****