## Annex II - Reference Maturity Model for Risk Management

(ii) Summary Matrix
III. Process and Integration:
A comprehensive risk-based control framework is in place that recognises and reflects the links of all controls to the risks they mitigate which enables identification of control gaps as well as redundancies or inefficient controls.

The organisation has developed and put in place some elements of a risk governance structure, in accordance with a three lines of defence (TLOD) structure or similar, to oversee the ERM framework.

Governance structure
The organisation has a fragmented, informal risk governance structure.

Delegation of authority
Certain staff members perform risk management functions without being formally designated that responsibility.

Function
A comprehensive risk-based control framework is in place that recognises and reflects the links of all controls to the risks they mitigate which enables identification of control gaps as well as redundancies or inefficient controls.

The organisation has implemented an ERM framework including risk analysis, assessment, treatment and monitoring, including risk appetite, tolerance and other criteria, and the charges that the risk functions are based on.

The organisation has fully integrated its risk governance structure (TLOD or similar) in applying its risks to its operations (including HQ, field, programs, projects).

The organisation encourages continuous governance improvement and innovation, making it a leader among its peers. Independent reviews of the risk process are undertaken regularly.

The risk processes are continually shaped based on peer evaluation, making the organisation a leader among its peers. Independent reviews of the risk process are undertaken regularly.

The risk governance structure is integrated with the ERM framework and risk appetite, tolerance and other criteria are reflected in the ERM framework.

The organisation is able to identify and take some viable opportunities based on an assessment of whether it can manage residual risk levels within its risk appetite, tolerance (or criteria).

The organisation is striving to improve its ERM capabilities through training and education, and by encouraging staff to engage in risk-related activities.

Risk governance structure
The organisation has in place a fragmented, informal risk governance structure.

Delegation of authority
Accountsabilities for managing risk are informal.

Function
Certain staff members perform risk management functions without being formally designated that responsibility.

Process
The organisation undertakes certain elements of the risk management process on an ad hoc basis. There may be inconsistencies in the methodologies applied for risk assessment, monitoring and reporting.

Interconnection with other functions
Risk-based internal controls are recognised and implemented across the organisation.

Integration with planning
There is limited recognition of the need for integration between risk assessment and results-based planning.

Planning with risk
There is recognition of the need for integration between risk assessment and results-based planning. The importance of integration of risk assessments with the organisation’s strategic and annual plans is communicated throughout the organisation.

Integration with internal controls
There is a lack of integration between risk assessment and internal controls which are primarily managed separately to risks.

There is a lack of integration between risk assessment and internal controls which are primarily managed separately to risks although generally key controls identification includes identification of the risks that they mitigate.

Risk culture
Unstructured, managed informally/ inconsistently,

Structured implementation, basic architecture, some reporting and repeatable management processes.

A risk scale (e.g. rating) is established for the organisation in the context of its programme/project management.

Ad hoc, reactive.

The links are recognised between (i) business continuity and crisis; and (ii) control effectiveness with risk reduction. Controls for certain administrative processes are documented and assigned ownership.

Advanced risk (and data) modelling and forecasting tools are used to support scenario analysis and strategy setting.

The organisation has an in place a fragmented, informal risk governance framework.

The links to recognised between (i) internal controls and risk; and (ii) control effectiveness with risk reduction. Controls for certain administrative processes are documented and assigned ownership and control criteria are established to measure the control effectiveness and subsequent residual risk assessments.

The evaluation of risk and reward is undertaken in an ad hoc and intuitive manner.

The organisation is able to identify and take some viable opportunities based on an assessment of whether it can manage residual risk levels within its risk appetite, tolerance (or criteria).

The organisation identifies and tackles its major and minor risks, and identifies the level of risk that is acceptable.

Dynamic risk information dashboards and risk appetite, tolerance (or criteria) are self-improved and proactively used across the organisation’s operations (including HQ, field, programmes, projects).

The organisation is able to identify and take some viable opportunities based on an assessment of whether it can manage residual risk levels within its risk appetite, tolerance (or criteria).

The organisation is in place a fragmented, informal risk governance framework.

Risk impacts management and its implications for risk management, including the effectiveness of risk governance structures in place.

The organisation is in place a fragmented, informal risk governance framework.

Risk impacts management and its implications for risk management, including the effectiveness of risk governance structures in place.

The organisation is able to identify and take some viable opportunities based on an assessment of whether it can manage residual risk levels within its risk appetite, tolerance (or criteria).