ERM AND INTERNAL CONTROL SYSTEM: A FINAL REVIEW

SPEAKER:

DOTT. FABIO ACCARDI

UNIVERSITA' degli STUDI di ROMA
TOR VERGATA

COURSE OF BUSINESS AUDITING
UNIVERSITY OF ROME TOR VERGATA

DECEMBER 2015

Enterprise-wide Risk Management

"ERM is a structured, consistent and co-ordinated framework for assessing, responding to and reporting on all risks that affect the achievement of an organisation's objectives"

From Position Statement, The Institute of Internal Auditors

Steps in the Risk Management Implementation Tool

Determine the corporation's **objectives**

Identify the risk exposures

Quantify the exposures

Assess the **impact**

Examine alternative risk management **tools**

Select appropriate risk management approach

Implement and **monitor** program

The Evolution Of Enterprise Risk Management

Traditional	***Emerging***
Risks managed in silos	Centralized mgt., with exec-level coordination
Concentrates on physical hazards and financial risks	Integrated consideration of all risks, firm-wide
Insurance orientation	Opportunities for hedging, diversification
Ad hoc / one-off projects	Continuous and embedded

Issues in ERM Implementation

- Different corporate ***cultures*** require different ERM approaches
- Who is going to be the ERM ***champion*** within the company
  - Among senior executives
  - Among departments / functions
- How to ***embed*** a risk management culture and responsibilities throughout the firm

Keys to Success in ERM

- Senior management commitment and sponsorship
- Embed a “risk management culture” in the corporation at the operational level
- Provide for accountability, both specific and widespread
- Clearly defined responsibilities for coordination and maintenance
- Adequate communication

The activities included in ERM

- Articulating and communicating the objectives of the organization;
- Determining the risk appetite of the organization;
- Establishing an appropriate internal environment, including a risk management framework;
- Identifying potential threats to the achievement of the objectives;
- Assessing the risk (i.e. the impact and likelihood of the threat occurring);
- Selecting and implementing responses to the risks;
- Undertaking control and other response activities;
- Communicating information on risks in a consistent manner at all levels in the organization;
- Centrally monitoring and coordinating the risk management processes and the outcomes
- Providing assurance on the effectiveness with which risks are managed.

From IIA Position Paper, The Role of Internal Auditing in ERM

Internal Audit and Risk Managemement

Two most important ways that internal auditing provides value to the organization are:

From IIA Position Paper, The Role of Internal Auditing in ERM

Internal Audit and ERM

Internal auditing is an independent, objective assurance and consulting activity.

Core Roles

objective assurance to the board on the **effectiveness of risk management**

- Risk reporting, evaluation, management

Assurance regarding handling of key risks

Internal Audit and ERM (cont.)

NOT Roles

- Establishment of “risk appetite”
- Imposing / implementing risk responses / management

Internal Audit and ERM (cont.)

Possible Roles

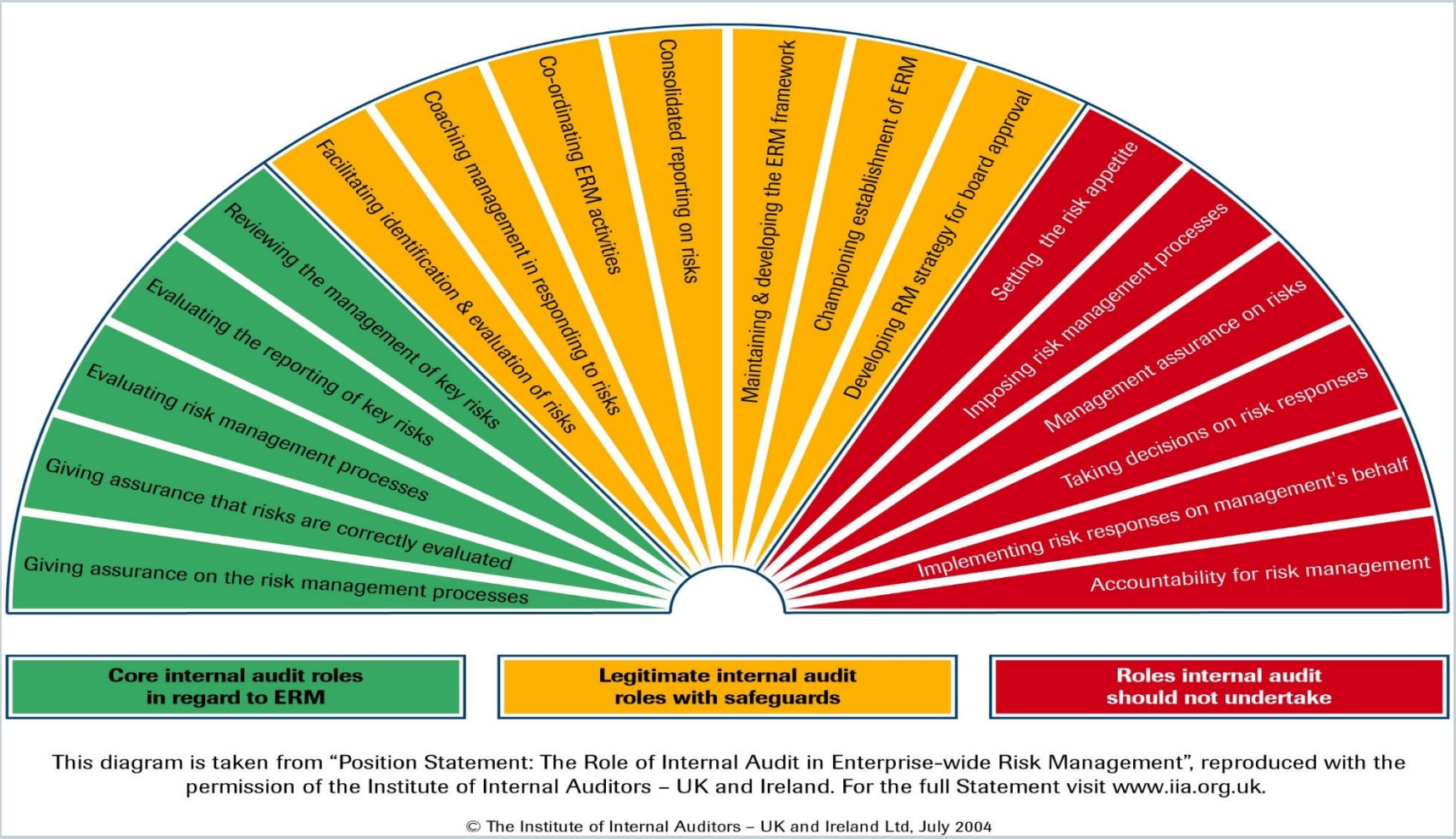
Facilitating risk management

- Identification, evaluation, championing

Coordinating ERM

"Developing risk management strategy for board approval"

Internal Auditing's Role in ERM



This diagram is taken from "Position Statement: The Role of Internal Audit in Enterprise-wide Risk Management", reproduced with the permission of the Institute of Internal Auditors – UK and Ireland. For the full Statement visit www.iia.org.uk.

From IIA Position Paper, The Role of Internal Auditing in ERM

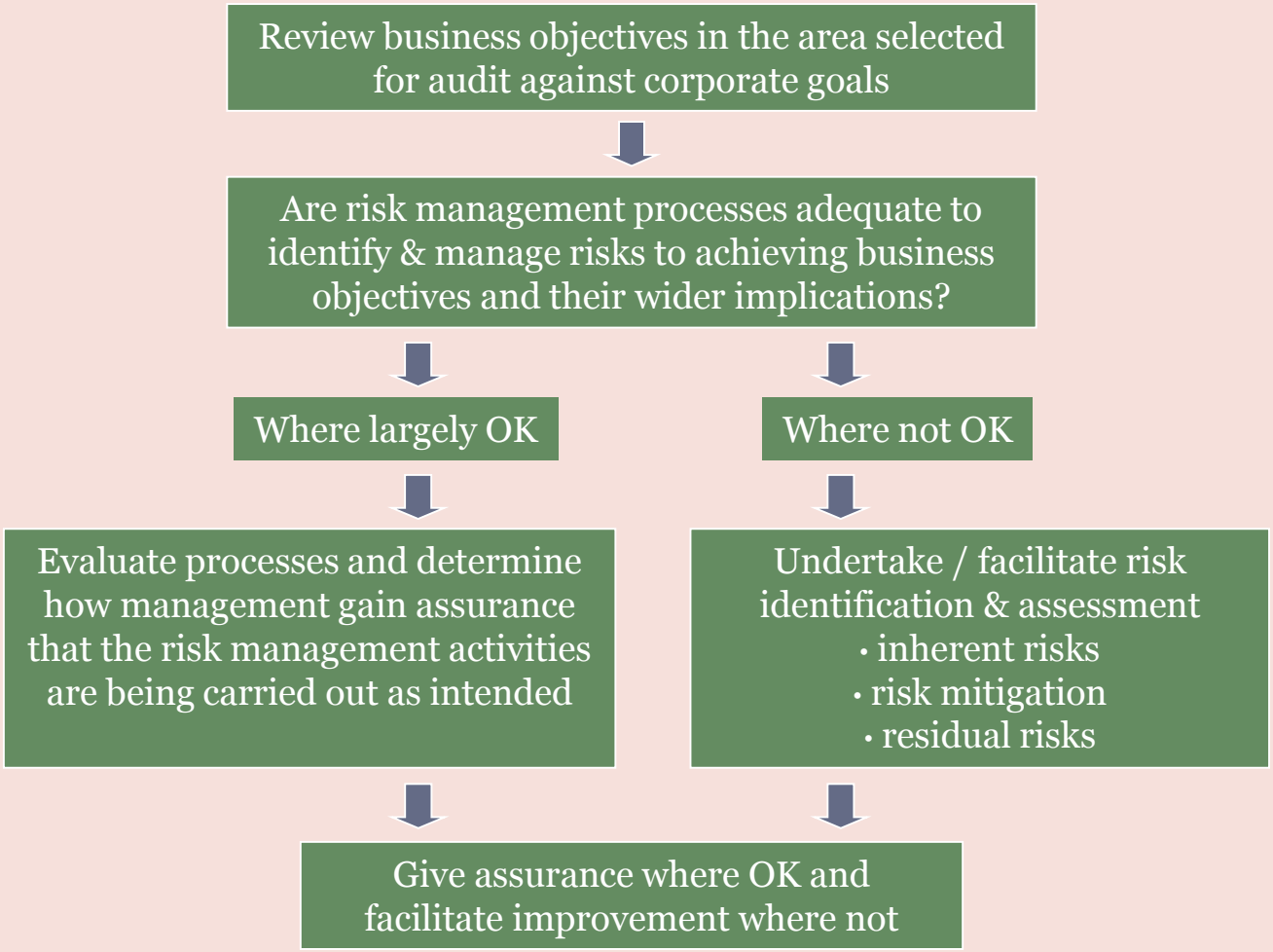
Benefits of ERM

- ✓ Greater likelihood of achieving an organisation's objectives
- ✓ Reduction in management time spent fire fighting
- ✓ Concise/consolidated reporting of disparate risks
- ✓ Greater management focus on the things that matter
- ✓ Fewer surprises or crises
- ✓ Understanding the key risks and their wider implications
- ✓ More informed risk taking / decision making
- ✓ Seizing opportunities / competitive advantage

From IIA Position Paper, The Role of Internal Auditing in ERM

Risk based auditing – risk framework / planning

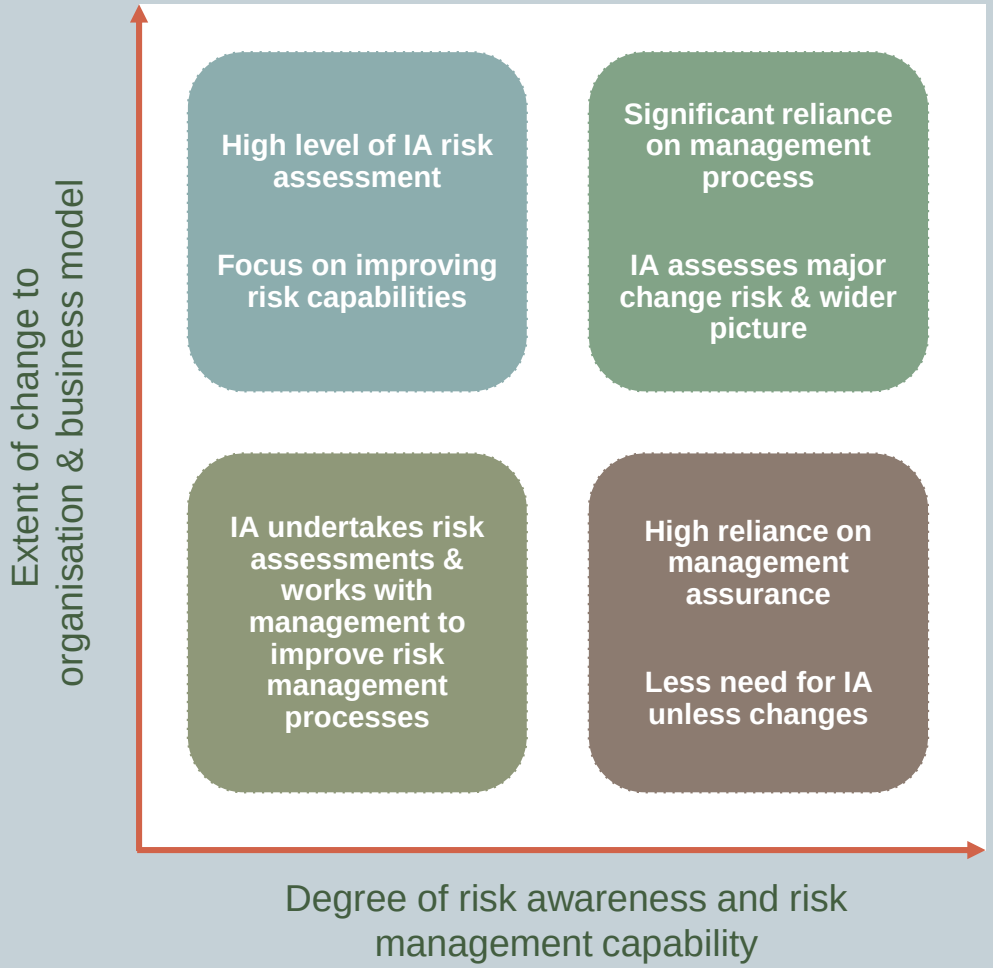
Risk based auditing - assignments



Risk based auditing – the environment

Is the organisation ready?

Every organization is different, with a different attitude to risk, different structure, different processes and different language. Experienced internal auditors need to adapt these ideas to the structures, processes and language of their organization in order to implement Risk based internal auditing (RBIA).



Advantages

By following RBIA internal audit should be able to conclude that:

- Management has identified, assessed and responded to risks above and below the risk appetite
- The responses to risks are effective but not excessive in managing inherent risks within the risk appetite
- Where residual risks are not in line with the risk appetite, action is being taken to remedy that
- Risk management processes, including the effectiveness of responses and the completion of actions, are being monitored by management to ensure they continue to operate effectively
- Risks, responses and actions are being properly classified and reported.

Position Statement, The Institute of Internal Auditors – UK and Ireland, Risk Based Internal Auditing

Implementation of RBIA

The implementation and ongoing operation of RBIA has three stages and we have produced detailed guidance on each of them:

Assessing risk maturity

- Obtaining an overview of the extent to which the board and management determine, assess, manage and monitor risks. This provides an indication of the reliability of the risk register for audit planning purposes.

Periodic audit planning

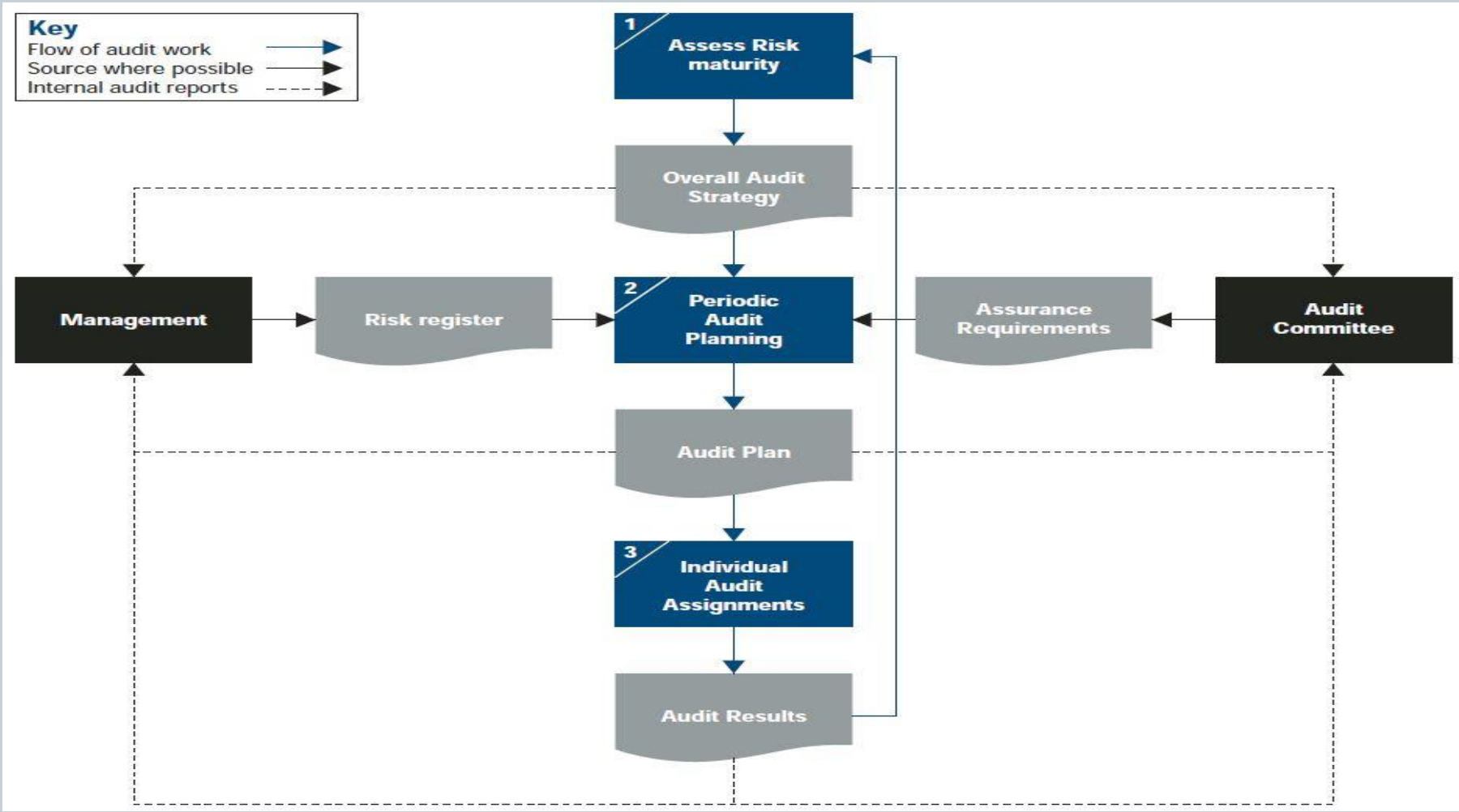
- Identifying the assurance and consulting assignments for a specific period, usually annual, by identifying and prioritising all those areas on which the board requires objective assurance, including the risk management processes, the management of key risks, and the recording and reporting of risks.

Individual audit assignments

- Carrying out individual risk based assignments to provide assurance on part of the risk management framework, including on the mitigation of individual or groups of risks.

Position Statement, The Institute of Internal Auditors – UK and Ireland, Risk Based Internal Auditing

Overview of the stages



Position Statement, The Institute of Internal Auditors – UK and Ireland, Risk Based Internal Auditing

The definition of Audit Plan: Objectives

- ✓ **Compliance with the Code of Conduct for Listed Companies**
- ✓ **Alignment with the Professional best practices (Standard IPPF)**
- ✓ **Significance of assurance in terms of adequate coverage in Italy and foreign**

The definition of the Audit Plan: Operational tools

The Audit Plan based on the prioritization of risks

For compliance with the Code of Conduct and Best Practices Professional (Standard IPPF) verification activities on the operation and suitability of the internal control and risk management system must be based on

1	AUDIT PLAN	ANNUAL / MULTIANNUAL
2	BASED ON A STRUCTURED ANALYSIS PROCESS AND PRIORITIZATION OF THE MAIN RISKS	SYNERGY WITH ERM
3	PREPARED BY INTERNAL AUDIT HEAD	INDEPENDENCE OF IA
4	APPROVED BY BOD	CONSISTENCY WITH THE MANDATE

Identification of Audit Universe

Identification of Audit Universe

Identification of all possible objects of audit, by defining a hierarchy of business processes, that:

1. Considering the actual company reorganization
2. is consistent with the business model adopted by the company
3. is aligned with the structure and methods used in the risk management process ensuring information flows bijective

Evaluation of S.G.R.C.I.

Evaluation of S.G.R.C.I.

Structured analysis and mapping of business processes that can:

1. detect existing controls within the audit identified
2. associate the risks universe and related risk assessments provided by the risk management process if it exists
3. evaluate the adequacy of existing controls

Prioritization of audit's objects

Prioritization of audit's objects

Determination of:

- Priorities for action;
- Mode of action;

through:

1. the evaluation of the residual risks, taking into account the acceptable limits defined by management;
2. assessing the significance of the controls to contain risks;
3. The consolidation of the results for process / audited

PROCESS CONTROL RISK PANEL

Audit Plan & Action Plan

Audit Plan & Action Plan

Identifying areas on which:

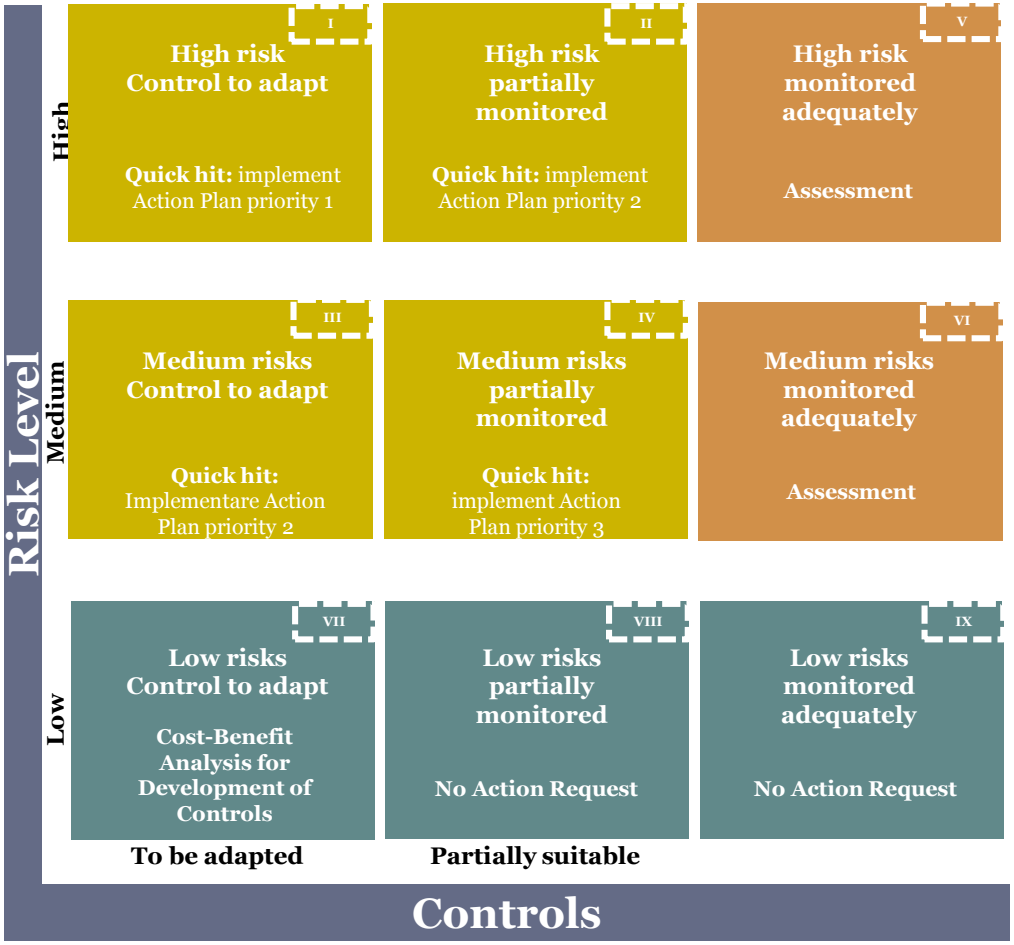
1. carry out audits (significant risks and effective controls);
2. provide suggestions for improvement (significant risks and inadequate controls)

In the definition and timing of the audits it is taken into account other factors (demand management, prior audit, the CRM information on the main risks, etc.)

PROCESS CONTROL RISK PANEL

The definition of the Audit Plan: (continued)

- ✓ **Consolidated experience (Prior Audits)**
- ✓ **Follow Up**
- ✓ **input CRM**
- ✓ **Process Control Panel (risk level for all Controls)**



The definition of the Audit Plan: (continued)

The annual planning process, which allows you to define "Auditable Unit", ie the areas, processes and / or clusters of business operations that can be audited, is articulated in following main stages:

1. Obtaining the documents made available by CRM
2. Association of the risks to business processes
3. Analysis and evaluation of control tools on specific business processes
4. Selection of countries / projects in which to conduct the audit
5. Identification of the processes being audited within the countries / projects selected
6. Preparation of the Draft Plan
7. Approving and communication of the Plan

- The assessment of controls help to identify the processes "manned" by those whose are needed improvement actions by the internal control system
- As a result, it will be included in the audit plan processes / areas that have a control adequate, considering the assessment of the relative risks.