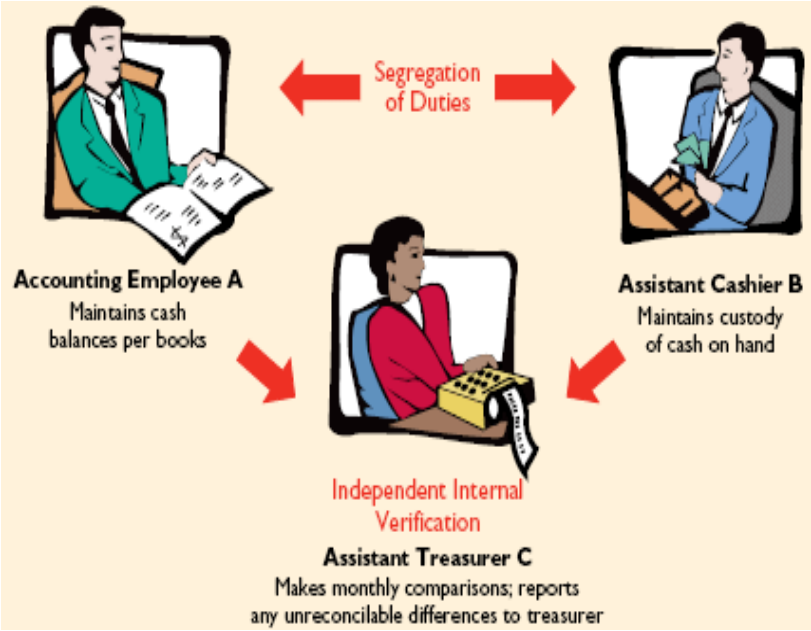
What does the Audit Committee need and expect from the Internal Audit function in terms of coverage of risk management?

Josiane VAN WAESBERGHE,
Head of Internal Audit, Federal Public Service Mobility and Transport.
Member of 3 Audit Committees in the Public Sector.

24/01/2013 - Exchange - Risk Management v. Audit

- How to avoid excessive (negative) risks without compromising or crippling our “entrepreneurship” aimed at responding to useful opportunities
- How do I do this with minimal overhead for everyone
- What is the right balance between risk (averse) management and creative (risk taking) entrepreneurship ?

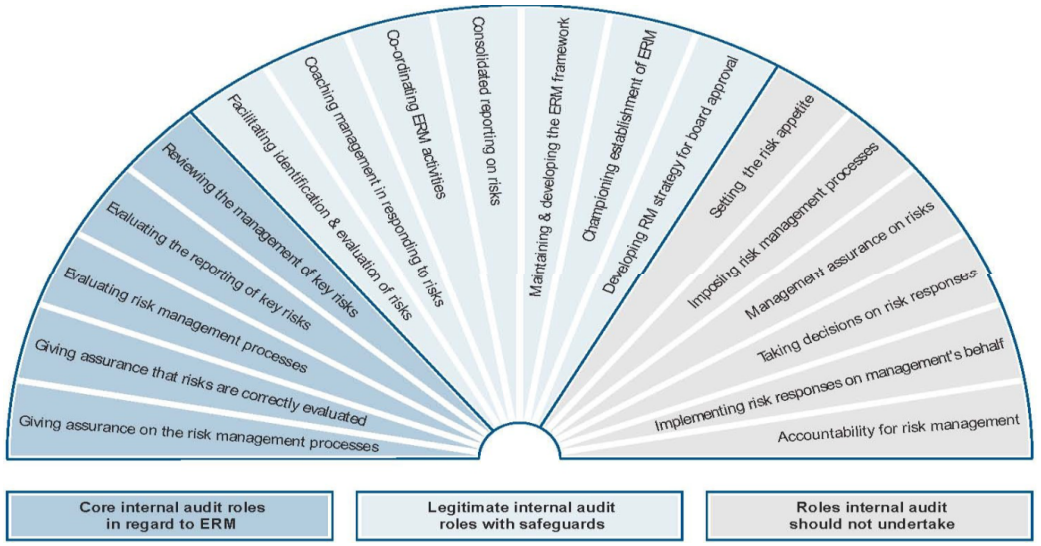
- Risk management (RM) should start from the core activities of the agency or policy area to which it belongs and be tailored to the organization
- RM is part of the decision process
- RM should address different types of risks (strategic and operational - business risks)



- Completeness
- Accuracy
- True and fair view of the accounting
- Timeliness (including timely data processing)
- Segregation of duties
- Clear responsibilities

- Do we have a system or method to detect and treat risks?
- What are those risks?
- Can we discuss them openly?
- Do we ask the right questions?
- Are we sufficiently « armed » against significant risks ?
- How are RM results presented?
- Can we evaluate and monitor RM ?

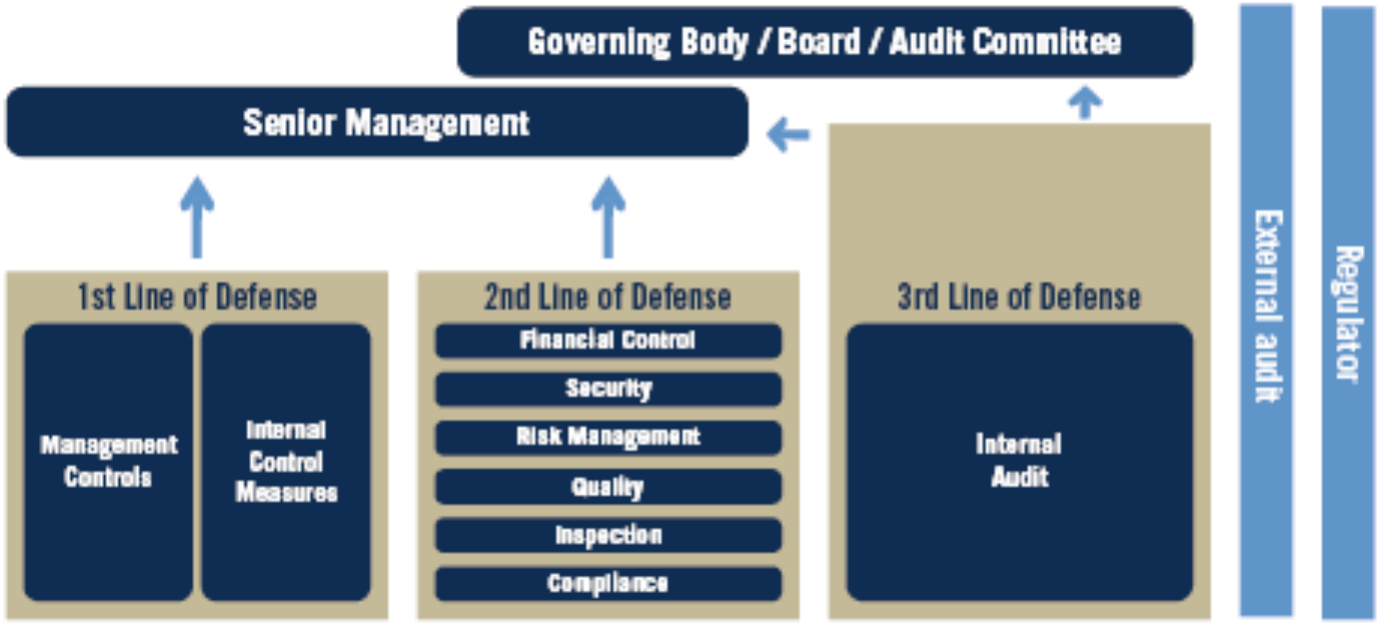
- Is internal audit competent in RM?
- Does IA coordinate with RM? Does IA use RM's input?
- Has internal audit sufficient authority and maturity to talk to management about risks?
- Safeguards in IA RM activities?
- IA risk analysis ok?
- IA RM evaluation ok?



- Corporate Governance
  - Code Daems: reference code for listed companies and autonomous public companies
  - Code Buysse: for unlisted companies
- Public sector: IA and RM in legislation

- **Governing bodies and senior management are responsible and accountable**
  - Establishing governance structures
  - Setting objectives
  - Defining strategies
  - Defining and implementing processes to best manage risk to accomplish the objectives
  - Risk management oversight

The Three Lines of Defense Model



Adapted from ECIIA/FERMA *Guidance on the 8th EU Company Law Directive, article 41*

First line of defense : operational management

- Operational managers **own** and **manage** risks
  - Responsible for implementing corrective actions to address process and control deficiencies
  - Maintaining effective internal controls and executing risk and control procedures on a day-to-day basis
  - Identify, asses, control and mitigate risks
  - Guide the development and implementation of internal policies and procedures, that serve as controls
  - Ensuring that activities are consistent with goals and objectives
  - Supervise execution of those procedures

Second line of defense: risk management and other “assurance” functions

- To ensure that first line of defense is properly designed and is operating as intended
- Each function has some degree of independence from the first line of defense but they are management functions
- Assisting management in developing processes and controls to manage risks
- Providing guidance, facilitation and training on risk management
- Monitoring the adequacy and effectiveness of internal control, accuracy and completeness of reporting and timely remediation of deficiencies

Third line of defense : Internal audit

- Independent and objective assurance on the effectiveness of governance, risk management and internal controls, including the manner in which the first and second lines of defense achieve risk management and control objectives
- Conditions: establish and maintain an independent adequately and competently staffed Internal audit function
    - IIA standards
    - Reporting lines

Additional lines of defense: External auditors, regulators and other external bodies

- Outside but important role in governance and control structure
- When coordinated effectively: providing additional assurance
- ***When not coordinated: significant weight on the organization***
- Risk information is generally less available to the organization (independence) or extensive than that of the internal lines of defense

Coordinating the three lines of defense

All 3 lines should exist in some form

•Risk management is strongest with 3 separate and clearly identified lines of defense, which are using a **common ground**

- e.g. a common risk model, with independent positions regarding the risks in this model and the risk analysis

•Combining of functions: clear communication of the impact, also to the governing body

•Dual responsibilities: consider separating them

•**Sharing** of information and knowledge

•Coordinating activities to foster efficiency and effectiveness: **beware of "overload"**

"Sometimes I think the collaborative process would work better without you."

Thank you for your attention

Josiane Van Waesberghe
josiane.vanwaesberghe@mobilit.fgov.be