PEMPAL

IT audit:
Standards, key risks, objectives and expectations

November 23, 2020

Jean-Pierre Garitte, CIA, CISA
World Bank expert

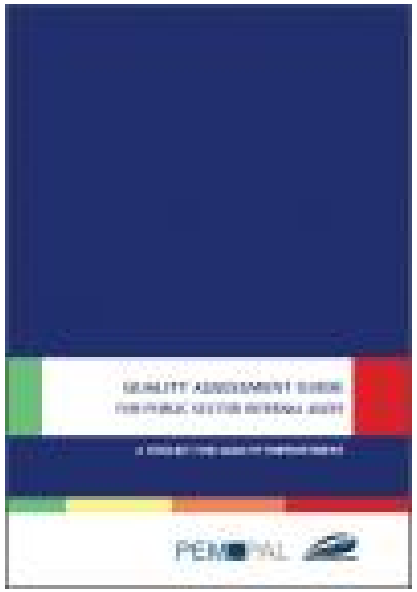
Content

- Link to existing frameworks
- Risks as identified by Heads of Internal Audit and stakeholders
- Objectives and expectations of IT audit
- Efforts needed

Link to existing frameworks

Link to existing frameworks

- The International Professional Practices Framework
  - The ISPPIA
  - The Code of Ethics
  - The Core Principles of Internal Audit
- PEMPAL guidance



The ISPPIA

- 1210 – Proficiency Internal auditors must possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit activity collectively must possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities.

- 1210.A3 – Internal auditors must have sufficient knowledge of key information technology risks and controls and available technology-based audit techniques to perform their assigned work. However, not all internal auditors are expected to have the expertise of an internal auditor whose primary responsibility is information technology auditing.

International Standards for the Professional Practice of Internal Auditing (Standards)

The Code of Ethics

- Competency

Internal auditors:

4.1. Shall engage only in those services for which they have the necessary knowledge, skills, and experience.

4.2. Shall perform internal audit services in accordance with the International Standards for the Professional Practice of Internal Auditing.

4.3. Shall continually improve their proficiency and the effectiveness and quality of their services.

The Core Principles for the Professional Practice of Internal Auditing

- Demonstrates integrity.
- Demonstrates competence and due professional care.
- Is objective and free from undue influence (independent).
- Aligns with the strategies, objectives, and risks of the organization.
- Is appropriately positioned and adequately resourced.
- Demonstrates quality and continuous improvement.
- Communicates effectively.
- Provides risk-based assurance.
- Is insightful, proactive, and future-focused.
- Promotes organizational improvement.

PEMPAL guidance

- 31. To ensure that internal auditors possess the necessary skills and competencies to audit the IT environment.

Review steps

- a. Assess whether internal auditors possess appropriate knowledge of the IT environment.
- b. Check whether the internal audit unit has a certified IT specialist.
- c. Assess whether an appropriate framework, such as, Control Objectives for Information Related Technology (COBIT) is being applied.
- d. Check whether IT audits are outsourced.
- e. Check whether proper training on IT audit is provided to internal auditors.
- f. Check whether the prescribed methodology contains adequate guidance on IT audit.

PEMPAL guidance

- 32. To ensure that internal auditors use appropriate IT tools and techniques when performing internal audit engagements.

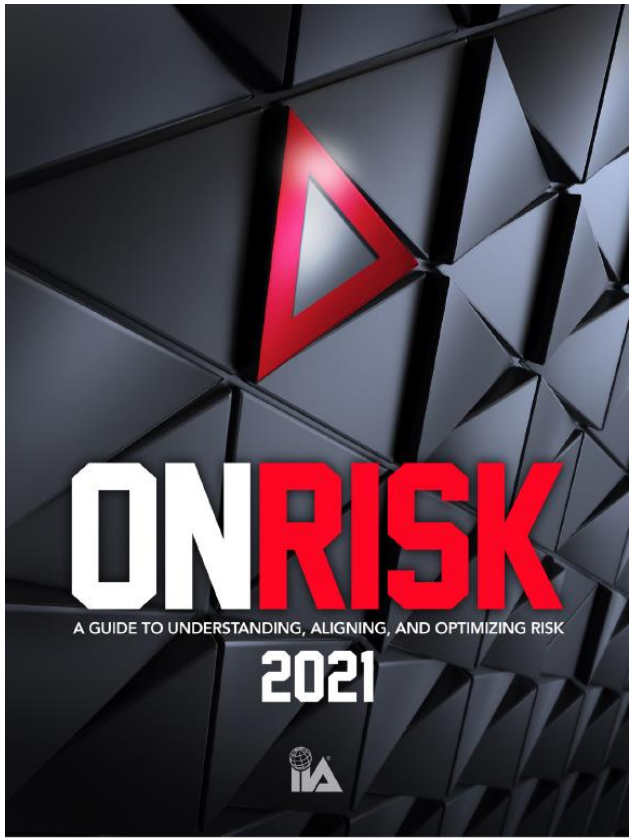
Review steps

- a. Check whether the use of IT tools and techniques is properly described in the internal audit manual.
- b. Check that IT tools and techniques are currently used by internal auditors to conduct internal audit engagements.
- c. Assess whether internal auditors are fully aware of the advantages of using proper IT tools and techniques.
- d. Check whether proper training on IT tools and techniques is included in the training plan for the period under review.

Risks as identified by Heads of Internal Audit and stakeholders

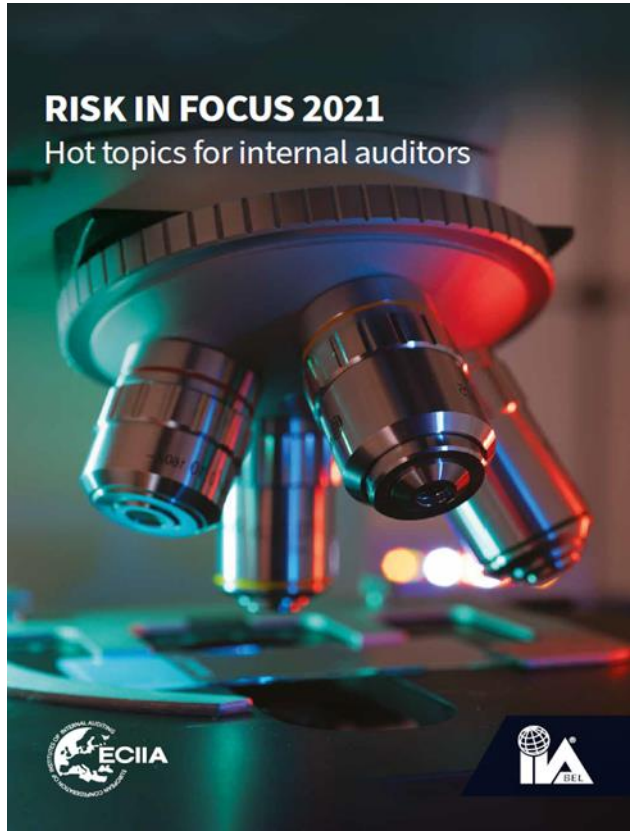
Risks as identified by Heads of Internal Audit and stakeholders

- Risk in Focus by ECIIA
- OnRisk by IIA



Risk in Focus by ECIIA

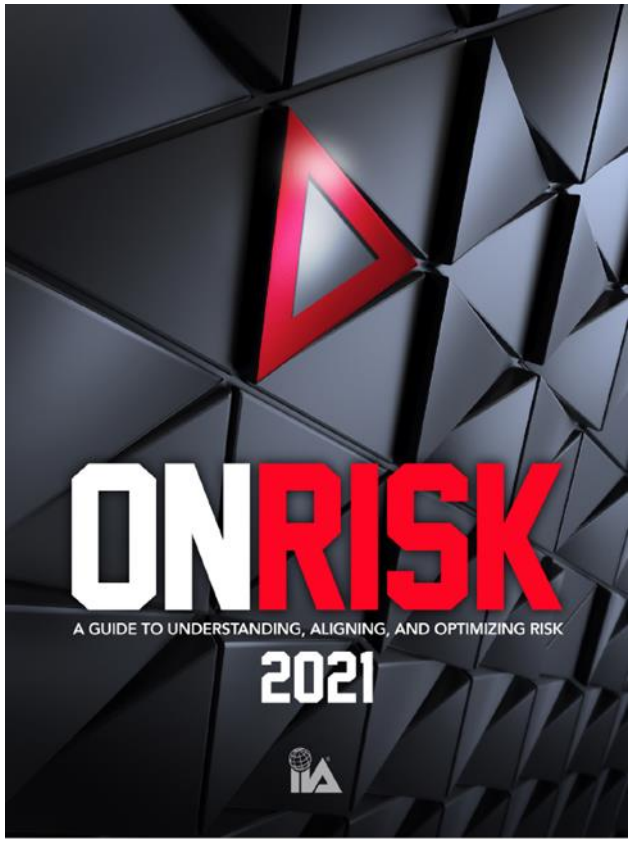
- ‘Cybersecurity and data security’ came out on top in this year’s survey, with 79% of CAEs saying it is a top five risk.
  - Information security in the expanded work environment



OnRisk by IIA

- Business continuity and crisis management and cybersecurity are the top-rated risks for 2021.

Unprecedented challenges brought on by the COVID-19 pandemic as well as expanding reliance on technology and data drove these two risks to the top of the list. They often were paired as some cyber threats were heightened by the sudden relocation of employees to less secure work-from-home environments as well as an intense shift to e-commerce brought on by the pandemic response.



Objectives and expectations of IT audit

Objectives and expectations of IT audit

- Our mandate is to provide reasonable assurance at least on the riskiest components of our audit universe.
- Almost all components of our audit universe are driven by IT.
- Without looking at IT we can never provide comfortable assurance.
- IT will further dominate our working and personal environment.
- Without a serious knowledge of IT risks and controls we will become irrelevant.
- Efforts needed:
  - Elevate the level of knowledge of all internal auditors and members of CHU.
  - Create a Center of Excellence on IT

Efforts needed

Efforts needed

- Elevate the level of knowledge of all internal auditors and members of CHU.
- Create a Center of Excellence on IT by (within?) the CHU.
- Ask the IACOP to develop guidance on IT audit: IT audit steps for non-IT auditors.

THANK YOU!