Risk Assessment and Audit Plan

PEMPAL IACOP and IIA Belgium – 5 October 2022
Internal Audit in Transition: The Public Sector Perspective

Unit 01 Quality Assurance, IAS

Overview

- IA Principles: IIA Standards and IAS Mission Charter
- Auditee(s)
- From risk to audit plan: process
- From risk to audit plan: mid-year and annual updates
- From risk to audit plan: audit cycle
- Challenges and opportunities

IA Principles: IIA Standards

- **Implementation Standard 2010**

  'The chief audit executive must establish a **risk-based plan** to determine the **priorities of the internal audit activity**, consistent with the organization's goals.'

- **Implementation Standard 2010.A1**

  'The internal audit activity's plan of engagements must be based on a **documented risk assessment**, undertaken at least **annually**. The input of senior management and the board must be considered in this process.'

Source: Revised IPPF Standards, January 2017

Implementation Standard 2120

The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

- Organizational objectives support and align with the organization's mission.
- Significant risks are identified and assessed.
- Appropriate risk responses are selected that align risks with the organization's risk appetite.
- Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.

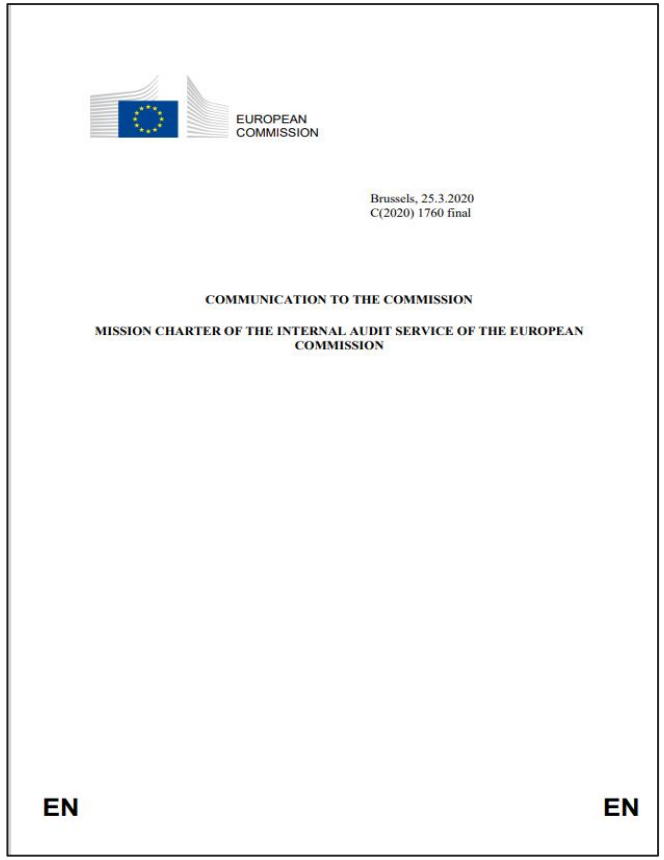
IA principles: IAS Mission Charter

- ‘The mission of the Internal Audit Service is to enhance and protect organisational value by providing **risk-based and objective assurance**, advice and insight.’
- ‘For its assurance services, the Internal Audit Service will rely on **risk-based planning** and provide a conclusion, and where appropriate an opinion, in each assurance audit report.’
- The IAS shall […] report at least annually to the Audit Progress Committee on the Internal Audit Service mission, authority and responsibility and performance in relation to the annual audit plan. Reporting should also include **significant risk exposures and control issues**, corporate governance issues and other matters needed or requested by the Commission’

IA principles: IAS - Mission Charter of the EC

‘The IAS has responsibility to […]

- develop a **three-year audit plan** and an **annual audit plan** using **appropriate and updated risk-based methodology**, including any risks or control concerns identified by management’
- ‘update the three-year audit plan at least **annually to take into account new and/or emerging risks** that could impact the organisation and submit these updated plans to the Audit Progress Committee for consideration;’


EUROPEAN COMMISSION

Brussels, 25.3.2020
C(2020) 1760 final

COMMUNICATION TO THE COMMISSION

MISSION CHARTER OF THE INTERNAL AUDIT SERVICE OF THE EUROPEAN COMMISSION

EN EN

Source: Mission Charter of the IAS of the EC, 25.3.2020

European Commission

Auditee(s)

- European Commission (**56** Directorates-General and Executive Agencies)
- **50+** Decentralised agencies and other bodies (JUs, European Schools, EEAS, EPF, EPPO, etc.)

Different entities with **different reporting** mechanisms and **different methodologies** (risk assessment and planning)

Harmonisation,
wherever possible,
is key

From risk to audit plan: process

Steps of IAS multi-annual plan:

From risk to audit plan: process

- Desk review and interviews with key staff and stakeholders
- Understand the auditee's strategy, objectives and structure
- Standardisation of audit universe into set **auditable entities** (set of **organisational structures, IT systems, policies and procedures, financial and human resources** that an entity implements to direct, execute, monitor and report upon its activities/processes)

From risk to audit plan: process

Auditable entities

European Commission and EAs

Financial audit universe:
- Procurement
- Grants
- Revenue
- …

Non-financial audit universe:
- HR management
- Business continuity
- ICT
- Policy development
- …

Decentralised Agencies and Other Bodies

Financial audit universe
- Procurement and grants
- Revenue

Non-financial audit universe
- HR management
- Business continuity
- ICT
- …

- EU Framework programme for research and innovation
- Publications and technical guidelines
- Supervision, certification and law enforcement
- …

Revision of audit universe

From risk to audit plan: process

- Consider management's RA, declaration of assurance, among others
- Identify, describe and score risks (impact and likelihood)

From risk to audit plan: process

- **Bottom-up approach** aimed at identifying individual risks for each entity via a risk assessment of the entire audit universe and to propose areas for audit having the highest risk exposure.

- **Top-down steer** aimed at better structuring the risk assessment exercise and at covering more consistently key themes/risks identified as top priorities.

  ↳ Auditee is consulted on the key risks/themes

The top-down steer **complements** the bottom-up approach.

From risk to audit plan: process

- **Inherent risks:** risks in the absence of any mitigating actions or controls management might take or put in place
- **Residual risks**: remaining risks after controls to mitigate the inherent risk have been implemented
- **Cross-cutting risks** affect several services/bodies, and
  - can be evaluated or addressed more effectively by a group of entities rather than by an individual entity,
  - not necessarily limited to internal organisation aspects and can relate to the external environment (e.g. pandemic).

From risk to audit plan: process

- Audit tool

Title		Impact	Likelihood	Inherent	Comments
EU Institutions				0.000	
European Commission				0.000	
Administration and support - security					
[redacted]				0.000	
DG [redacted]				0.000	
DG [redacted]				0.000	
DG [redacted]				0.000	
[redacted]				0.000	
Administrative expenditure				0.000	
[redacted]				0.000	
Direct management - grants					
Ineffective [redacted]		●●●○○	●●●●○	12.000	The impa...
[redacted]		●●●○○	●●●○○	9.000	The impa...
Inadequate design [redacted]		●●●○○	●●●●○	12.000	The impa...

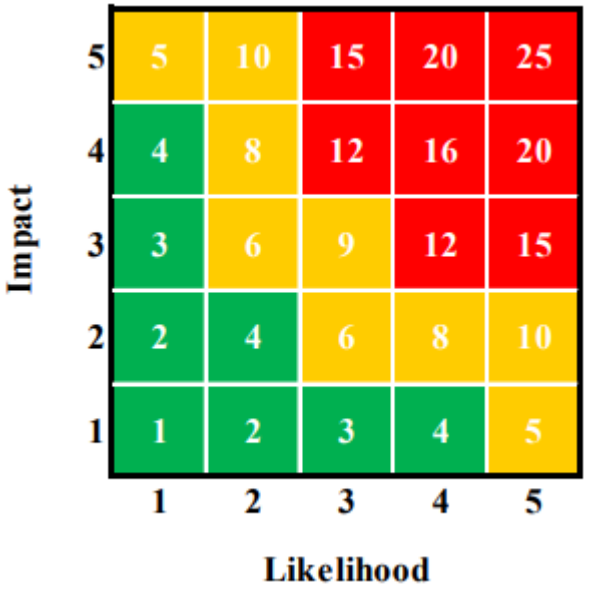
European Commission

From risk to audit plan: process

- Are there cross-cutting risks? Could these be addressed by multi-entity audits?
- Some areas need to be periodically covered (fundamental in nature or materiality)

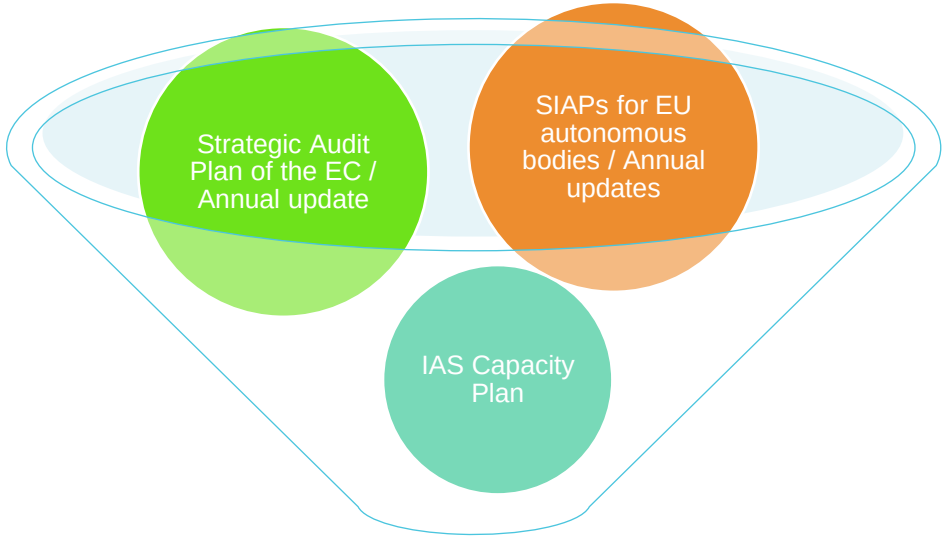
From risk to audit plan: process

- Focus on main risks (high or medium)
- How can the IAS add-value on these areas?



European Commission

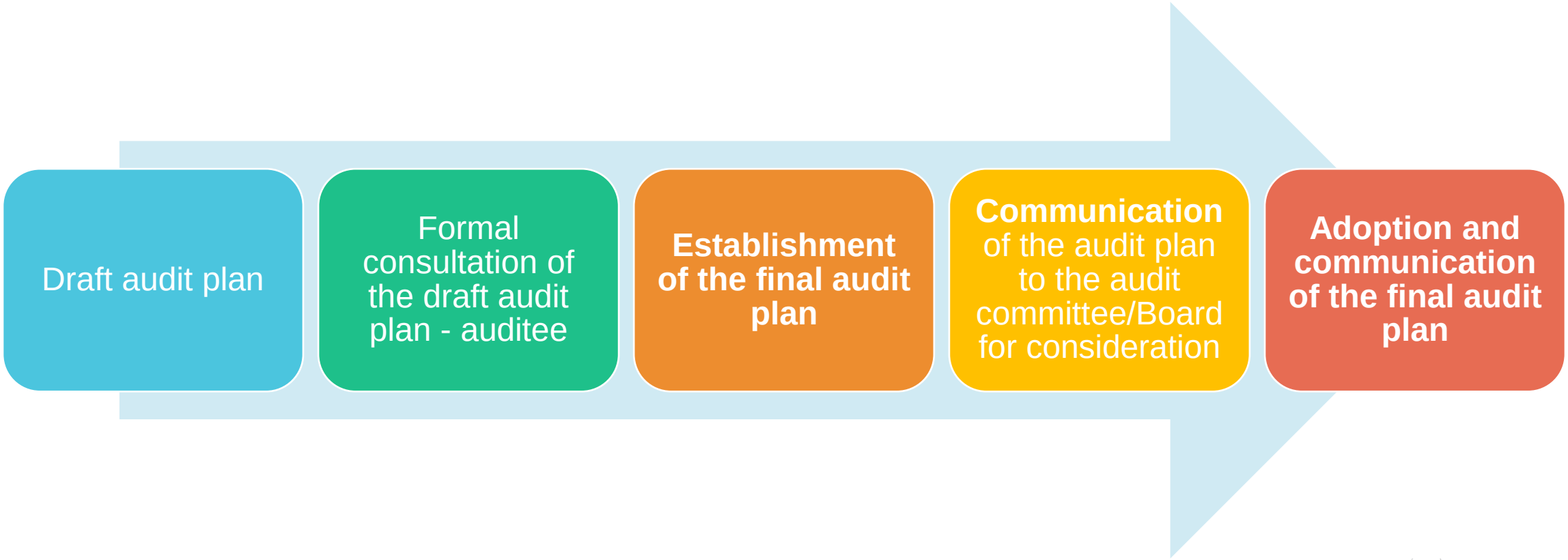
From risk to audit plan: process



IAS Consolidated Annual Audit Plan

European Commission

From risk to audit plan: process



European Commission

From risk to audit plan: mid-year update

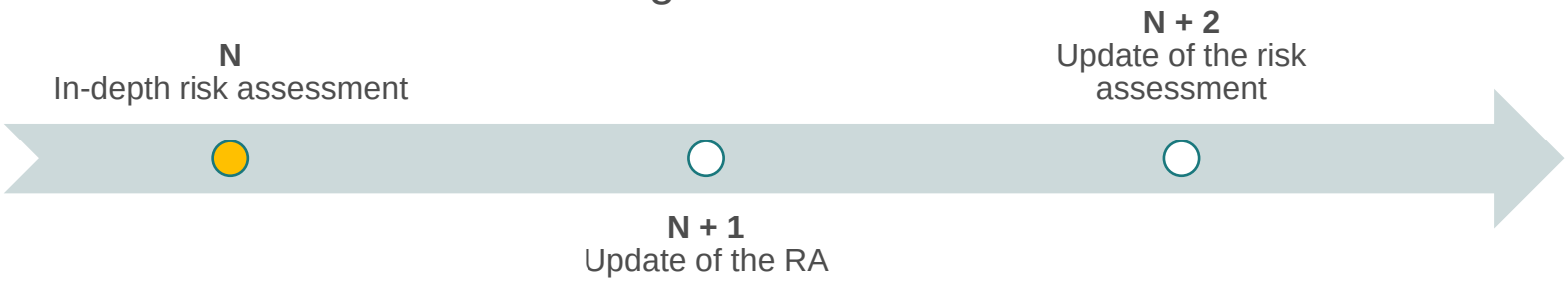
- Mid-year in-depth analysis of actual vs performed
- Consideration of constraints (and emerging key issues)
- *Not an update of the risk assessment*
- Update of the plan, communication to APC/Board and communication to auditee

From risk to audit plan: annual update

- Annual update of the audit plan based on a **light risk assessment**
- Analysis of emerging risks, new activities, changes in the legislative and operating environment, etc. (Not an in-depth risk assessment)
- Update of the plan, communication to APC / Board and communication to auditee

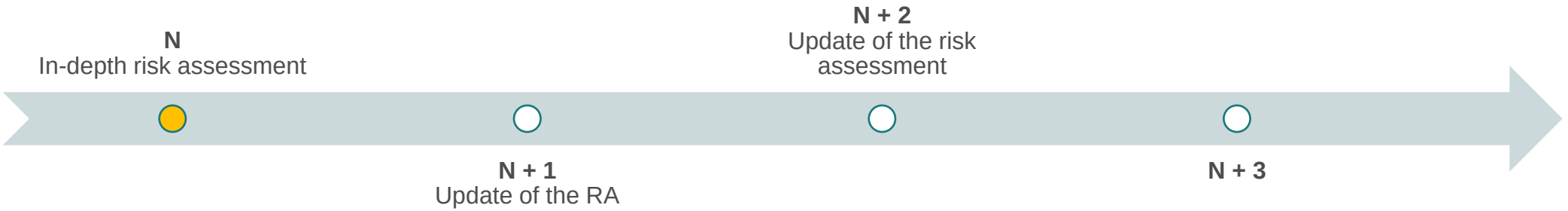
From risk to audit plan: audit cycle

- European Commission and Executive Agencies



Other audit engagements conducted between N and N+2

- Decentralised agencies and other bodies



Other audit engagements conducted between N and N+3

European Commission

Challenges and opportunities

- Clear **focus on high risks**: providing re-assurance or recommendations for improvement
- **Integrated approach**, where possible: Commission (56) – Other bodies (50+)
- **Realistic objectives**: resource constraints, volatile audit environment, high workload of auditees, new emerging risks
- Close **coordination with ECA and IAC**: limiting over-auditing

  - **Standard 2050 – Coordination and Reliance**

  ‘The chief audit executive should share information, coordinate activities, and consider **relying upon the work of other internal and external assurance and consulting service providers** to ensure proper coverage and minimize duplication of efforts.’

Thank you

European Commission