A methodology for Fraud Risk Assessment

Recovery and Resilience Facility

29 November 2021

I. Introduction, key concepts and definitions

European Commission

Fraud risk assessments and EU funds

- The experience of the ESI Funds (CPR 125(4)c)

  "*managing authority shall put in place effective and proportionate anti-fraud measures taking into account the risks identified*"

- Is fraud risk assessment the weak link?

  PWC: Some authorities may underestimate the risks during the self-assessment …

  ECA: for some managing authorities (MA) the approach is still too mechanical and does not include additional input from other knowledgeable parties … Mas generally conclude that their existing anti-fraud measures are good enough to address fraud risks. We consider that this conclusion may be too optimistic

- Guidelines - Check list for the NRRPs

  Is there a specific description of the anti-fraud measures, including fraud prevention? Is there an indication whether a Fraud Risk assessment and the definition of appropriate anti-fraud mitigating measures has been/will be implemented for the RRP as a whole or specific measures?

Risk analysis in the anti-fraud cycle

- Risk analysis is precious fuel for the anti-fraud engine
- Risk analysis and fraud prevention
- Risk analysis and fraud detection
- Risk analysis is a live process
- Risk analysis is a collective exercise

Definitions (1)

- Fraud: intentional deception to secure unfair or unlawful gain, or to deprive a victim of a legal right (common legal definition)[1]
  - RRF regulation refers to serious irregularities: fraud, corruption, conflict of interest
- Risk assessment: a systematic process of evaluating the potential risks that may be involved in a projected activity or undertaking[2]

[1] "Legal Dictionary: fraud". Law.com

[2] Oxford languages

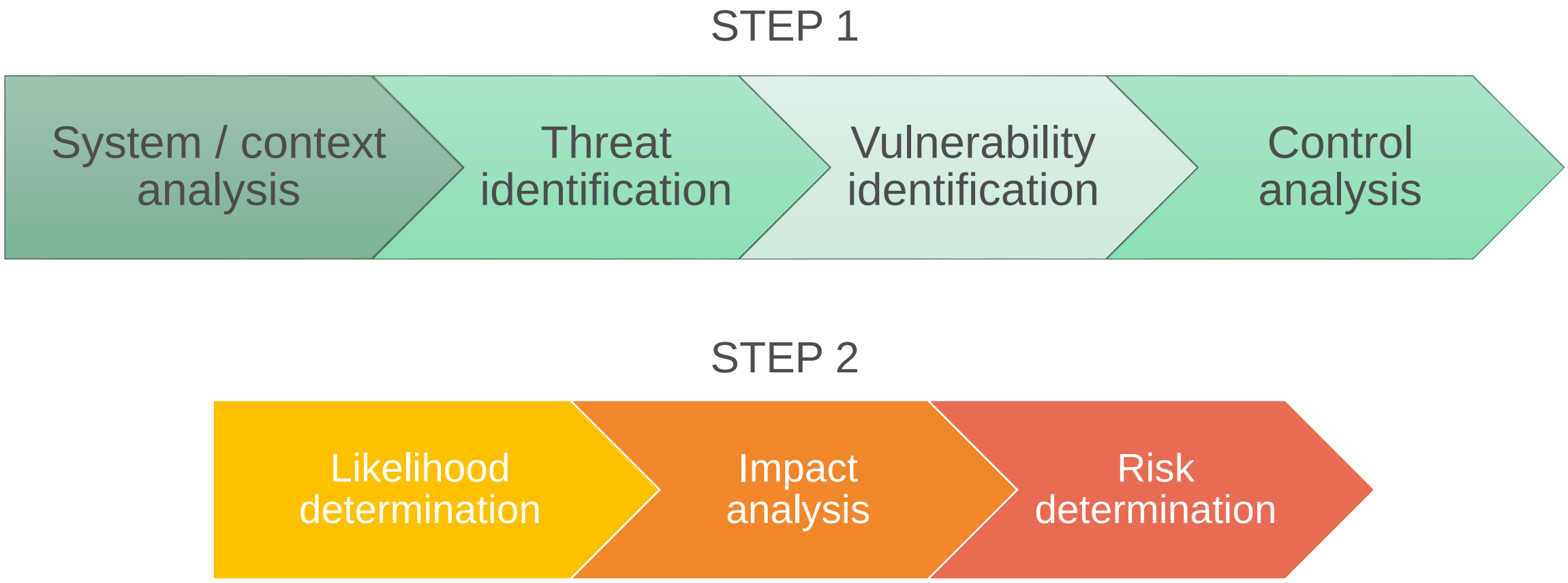
Definitions (2)

- System: focus of the analysis
- Context: External relevant factors
- Threat-source: Individuals, groups or companies with the potential to cause fraud
- Vulnerability: Weakness in the system that can be exploited
- Risk: a threat-source exploiting a particular vulnerability
- Impact: magnitude of harm that could be caused by a threat-source exploiting a vulnerability

II. The fraud risk assessment process

European Commission

The fraud risk assessment process



II.a Step 1

Understanding

European Commission

System / context analysis

- System analysis
  - to develop a thorough understanding of the relevant system
  - provides a clear view of the processes, players and roles
  - covers the management and control of the relevant funds
- Context analysis
  - to identify the external factors that may have an influence on the system
  - PESTEL analysis
  - Conceptual model

Threat identification

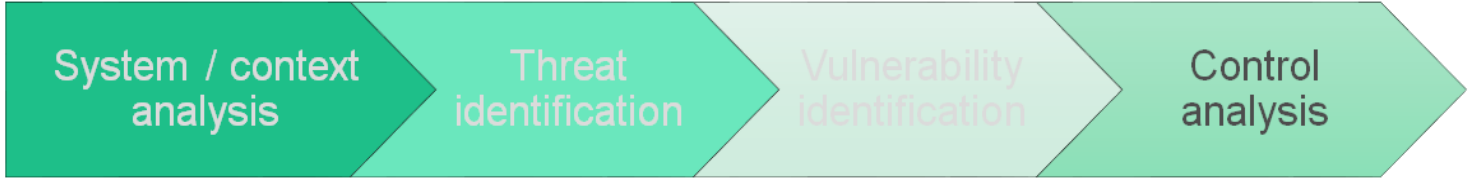
- Listing potential threat-sources that are applicable to the system being evaluated
- Who? What? How?

WHO?	WHAT?	HOW?
Employee dealing with procurement procedure	Fraudulently favour a specific tenderer	Tailoring tender specifications, as a result of corruption
Employee dealing with procurement procedure	Fraudulently favour a specific tender	Leaking priviledged/confidential information before the official launch of the procedure, as a result of corruption

Vulnerability identification

- develop a list of system vulnerabilities (weaknesses) that could be exploited
- arising from the following areas:
  - Regulatory system
  - Management system
  - Financial control mechanism
  - Human resources
  - IT systems
  - Other (as relevant)

Area	Vulnerability	Potential	Occurred
HR	High rotation / mobility of personnel, causing untrained / inexperienced staff to occupy also key posts		



Control analysis

- qualitative and quantitative overview of the audits/controls of the given field
- Quantitative (percentage of transactions /beneficiaries/operators subject to control) and qualitative (the depth of the control) analysis of the control
- Assessment of the capability to address/mitigate the identified vulnerabilities

Specific consideration

Two payment requests per year ~ each summary of audits would cover a roughly 6 months period

Initial payment request:

- can be submitted shorty after the approval of the Plan, hence such period will be shorter. Therefore, the Commission will take into account the length of time between the approval of the Plan and the payment request for the assessment of summary of audits
- for measures implemented before the approval of the Plan, the MS may use the audit results from other national bodies (Supreme Audit Institution, audit authorities at federal, national, regional, provincial or municipal level) to help to close the assurance gap

II.b Step 2

Assessing

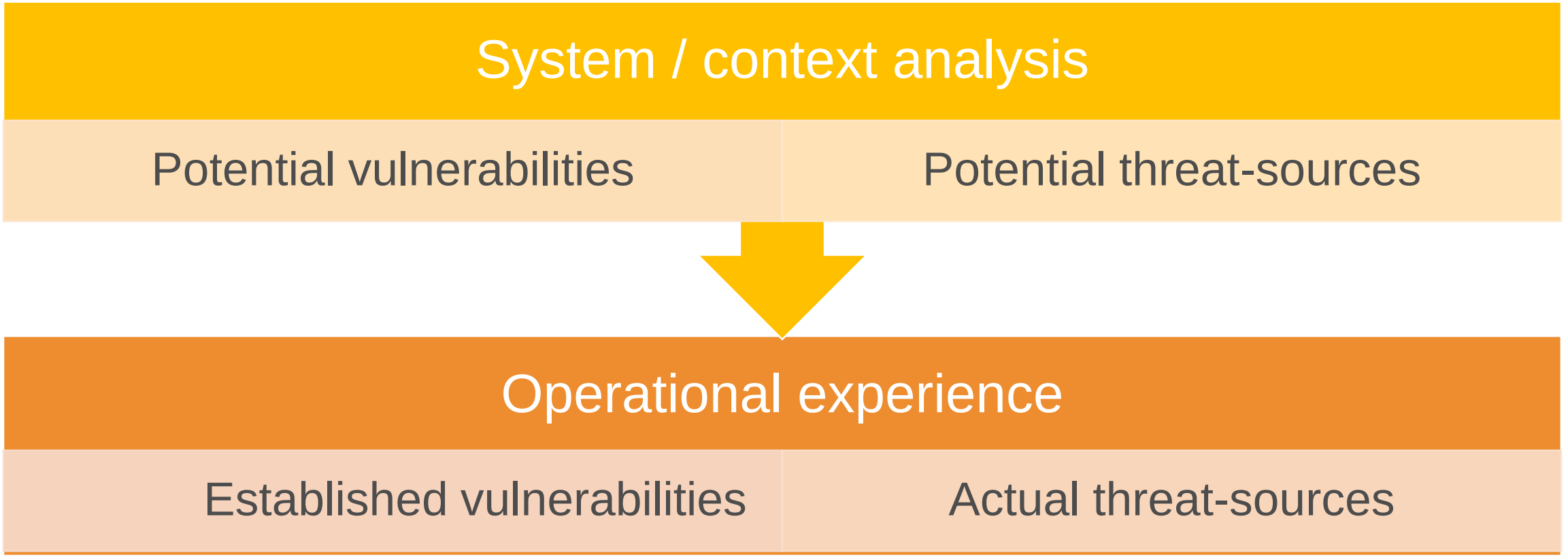
European Commission

Likelihood determination (1)

- To determine likelihood of a threat, threat sources, potential vulnerabilities and existing control must be considered
  - Threat-source motivation and capability
  - Seriousness of the vulnerability
  - Existence and effectiveness of current control framework
- No vulnerability means likelihood = 0, therefore no risk

Likelihood level	Likelihood definition
High	Threat source is motivated and sufficiently capable, existing vulnerability, controls to mitigate ineffective
Medium	Threat-source is motivated and capable, controls in place impede successful exploitation of vulnerability
Low	Threat-source lacks motivation or capability, or controls in place prevent, or significantly impede, exploitation of vulnerability
Null	No vulnerability to be exploited

Likelihood determination (2)



Impact analysis

- Some impacts can be measured quantitatively
- Other impacts (e.g. loss of public confidence, loss of credibility, damage to an organisation's interest) cannot be measured in specific

Magnitude of impact	Impact definition
High	Exploitation of vulnerability (1) may result in **highly** costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organisation's mission, reputation, or interest
Medium	Exploitation of vulnerability (1) may result in costly loss of tangible assets or resources; (2) may violate, harm, or impede an organisation's mission, reputation, or interest
Low	Exploitation of vulnerability (1) may result in the loss of some tangible assets or resources; (2) may affect an organisation's mission, reputation, or interest

Risk determination

- Example of risk-level matrix

	Impact		
Likelihood	Low (10)	Medium (50)	High (100)
High (1.0)	Medium 10 x 1.0 = 10	High 50 x 1.0 = 50	High 100 x 1.0 = 100
Medium (0.5)	Low 10 x 0.5 = 5	Medium 50 x 0.5 = 25	High 100 x 0.5 = 50
Low (0.1)	Low 10 x 0.1 = 1	Low 50 x 0.1 = 5	Medium 100 x 0.1 = 10

- Description of risk level

II.c Step 3

Acting

European Commission

Reducing risks

- Action must be taken to mitigate or eliminate the identified risks, as appropriate to the intervention
- The goal is to minimise the level of risk to the analysed intervention

Resources

European Commission

Useful document

Fraud Risk assessment and Effective and Proportionate Anti-Fraud Measure

(*European Structural and Investment Funds – Guidance for Member States and Programme Authorities*)

European Commission

Thank you for your attention

Andrea Bordoni

Deputy Head of Unit C.1 – Anti-corruption, anti-fraud strategy and analysis

European Anti-Fraud Office

European Commission