

Session 2

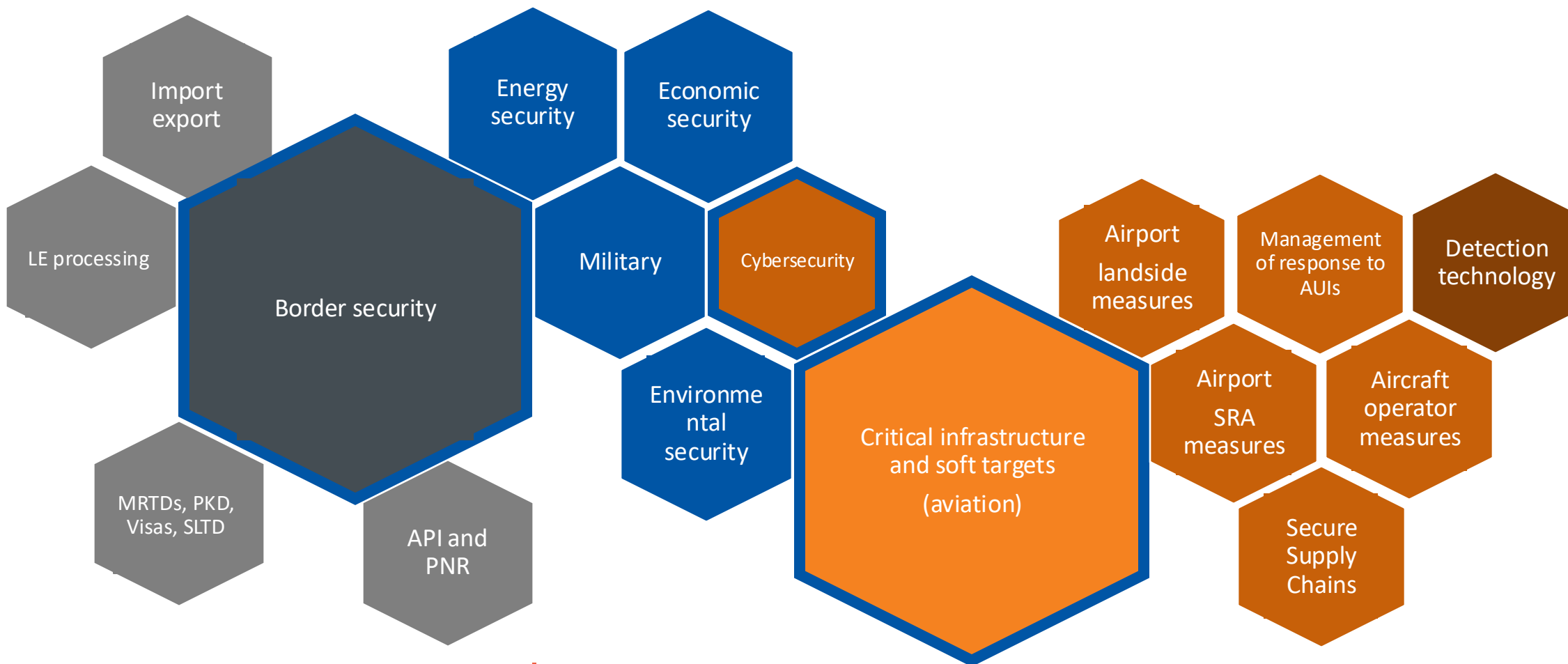
Common approach to risk assessment
inter-agencies cooperation

Ms. Agnieszka Maja Mizgalska
AVSEC Technical Officer, ASP
Section, ICAO

Mr. Philippe MORIO
Cybersecurity expert, ICAO

Dimensions of national security

216



Passenger Data Exchange Systems
Entry and departure of **persons, their baggage and cargo**
Annex 9 – *Facilitation* 1949: 16th edition

Measures applied to **infrastructure, staff, persons, their items carried and cargo**
Annex 17 – *Aviation Security* 1974: 12th edition

ISO definitions*

R

risk - effect of uncertainty on objectives

T

threat/likelihood - chance of something happening

C

consequence - outcome of an event affecting objectives

V

vulnerability - weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat

*SOURCE: ISO 31000:2018 | ISO/IEC 27000]



AVSEC Panel



Threat: The capability and intent of a perpetrator to attack civil aviation with the potential to harm life, systems, information, environment and/or property



Security Risk: The level of exposure to an attack against civil aviation taking into account the likelihood, consequence, and the vulnerability that remains following an evaluation of the effective implementation of the existing aviation security mitigation measures

RCS 3rd Edition



Consequences: the nature and scale of the impact of the specific attack, in human, economic, political, and reputational terms under a reasonable worst-case scenario



Current mitigation measures: the relevant SARPs, which may not all be in Annex 17, and guidance – both of which are assumed to be effectively implemented (where that is clearly not the case, the residual risk will be higher). It is assumed that no threat can be entirely eliminated



Vulnerability: the extent of the remaining vulnerabilities once the current mitigating measures have been taken into account



Residual risk: the overall risk of a successful attack, taking into account the likelihood and consequences of the threat scenario, and considering the remaining vulnerabilities after assuming current mitigating measures have been implemented

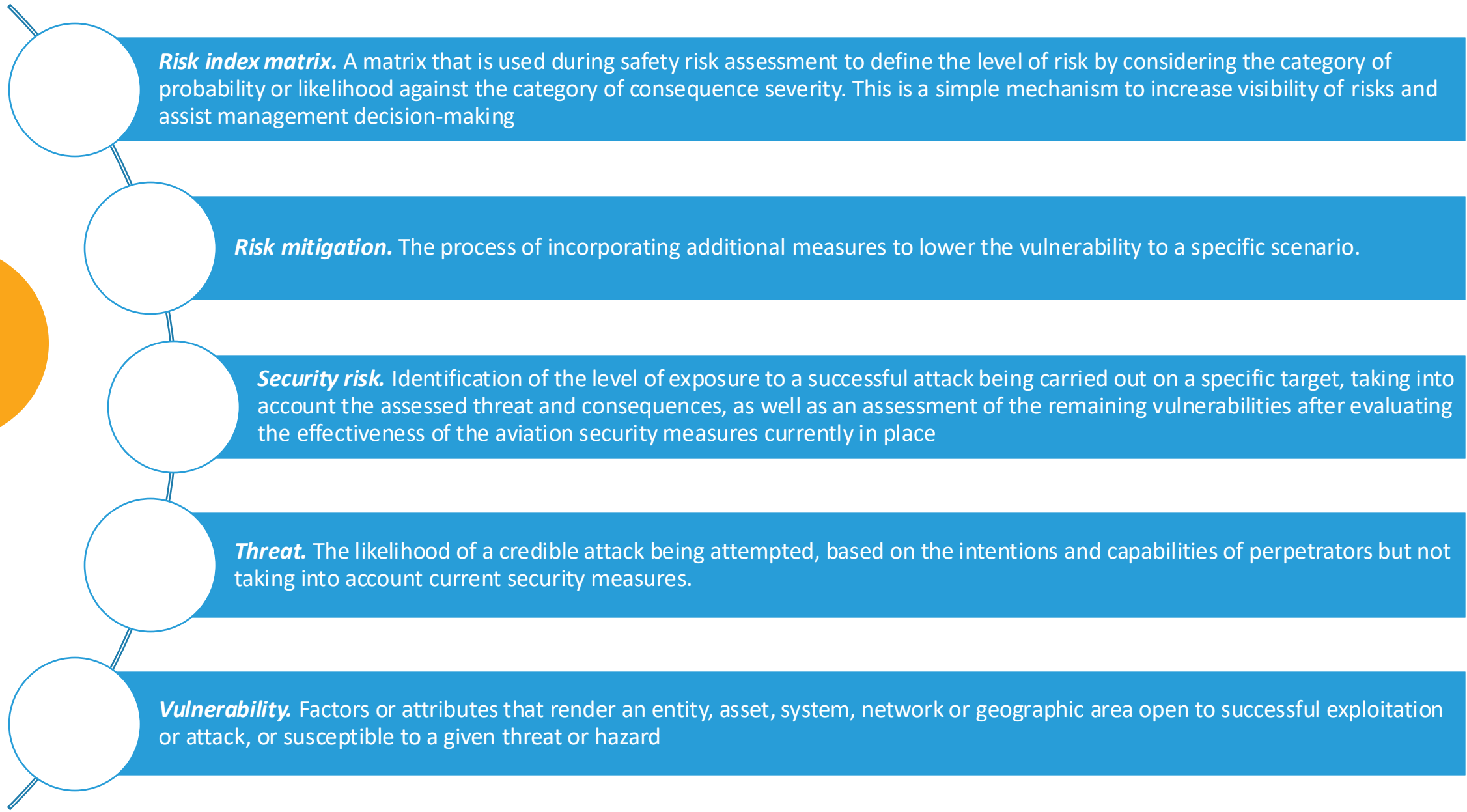


Possible additional mitigation: identified measures, not formally included in ICAO SARPs, that could be implemented to further mitigate residual risks where necessary

ICAO definitions*

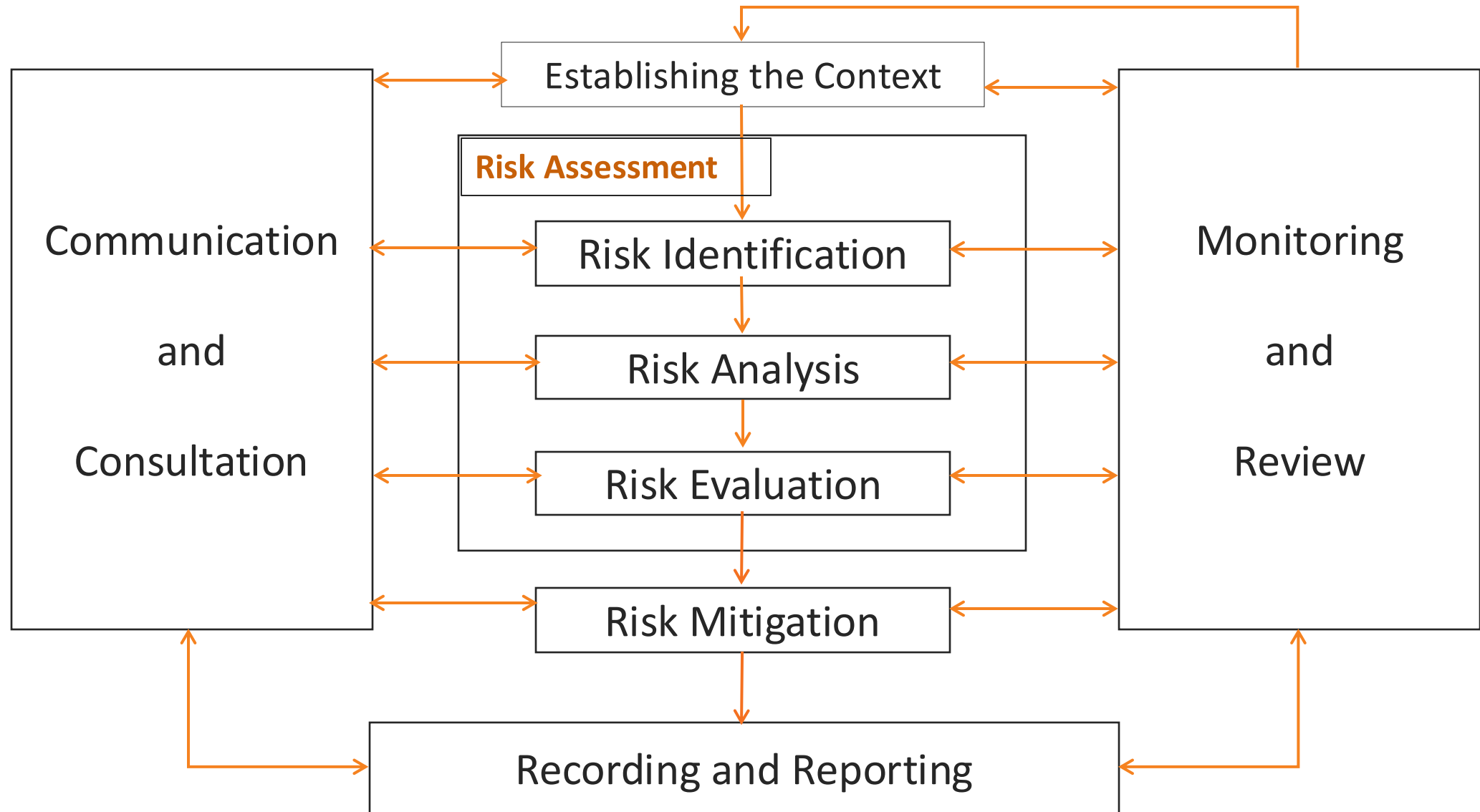
220

Doc
10084



Risk management*

221



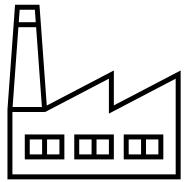
Threat Assessment

222

Assessment of the
threat to target

Preventive
security measures

Crisis
management



Identified
target

**Focuses on
attacks
known or
currently
happening
or attacks
being
threatened
by**



Primarily focuses on identifying
and analyzing threats, their
likelihood

Quite often connected with
assessment of consequence and
understanding of weaknesses of
target



Applying security
measures to detect,
deter and prevent
event to happen
Applying additional
security measures
based on threat
level

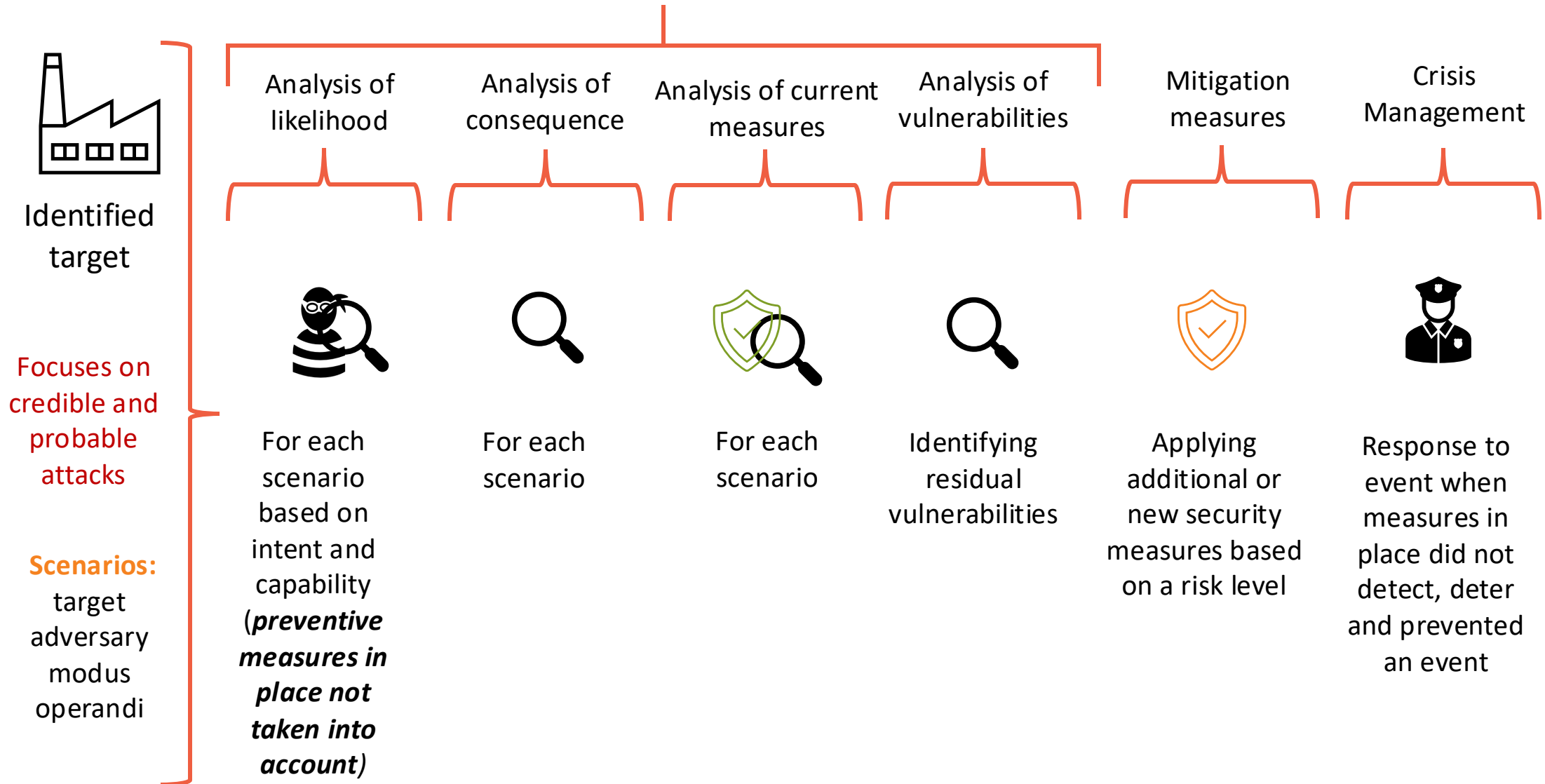


Measures to
respond to an event
when measures in
place did not detect,
deter and prevented
an event

Risk assessment based on scenario

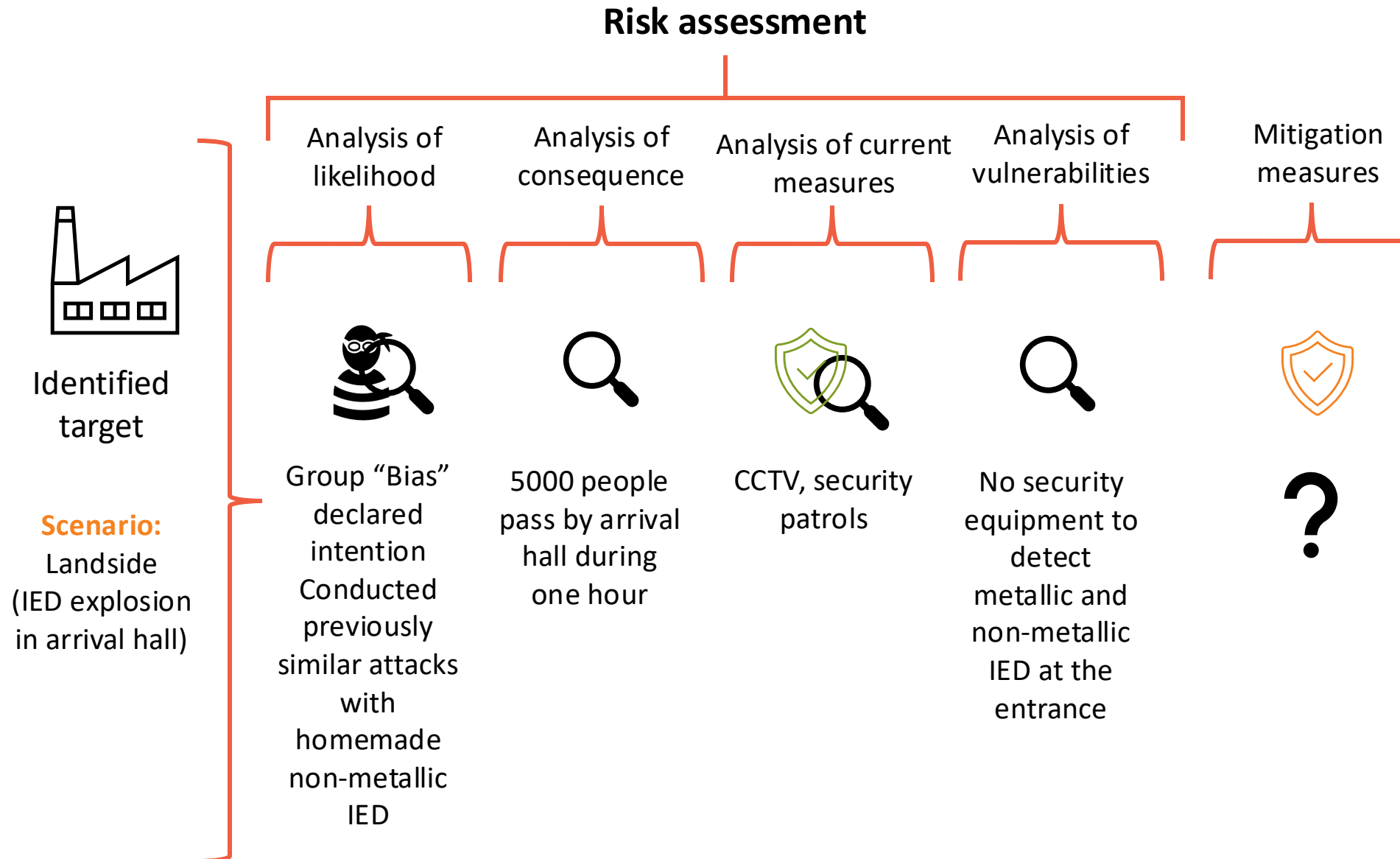
223

Risk assessment



Risk assessment based on scenario - example

224




Risk Assessment is part of the Risk Management process


225

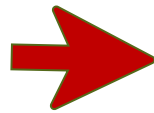
Risk assessment

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation*

 threat/likelihood







 consequence

 vulnerability



Risk Management

coordinated activities to direct and control an organization with regard to risk* which involves systematic application of policies, procedures and practices the activities of:

-  communicating and consulting
-  establishing the context
-  **assessing**
-  treating (mitigating)
-  monitoring and reviewing
-  recording and reporting

*SOURCE: ISO 31000:2018

Benefits of a common interagency risk management methodology

226



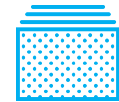
Provides a systematic approach to examine the key components of risk and produce a risk assessment



Assesses your security environment focusing on keeping vulnerabilities at an acceptable level



Informs the effective allocation of limited resources



Establishes a common frame of reference for examining a system, communicating issues, and determining priorities



Provides basis for prioritizing mitigation strategy alternatives

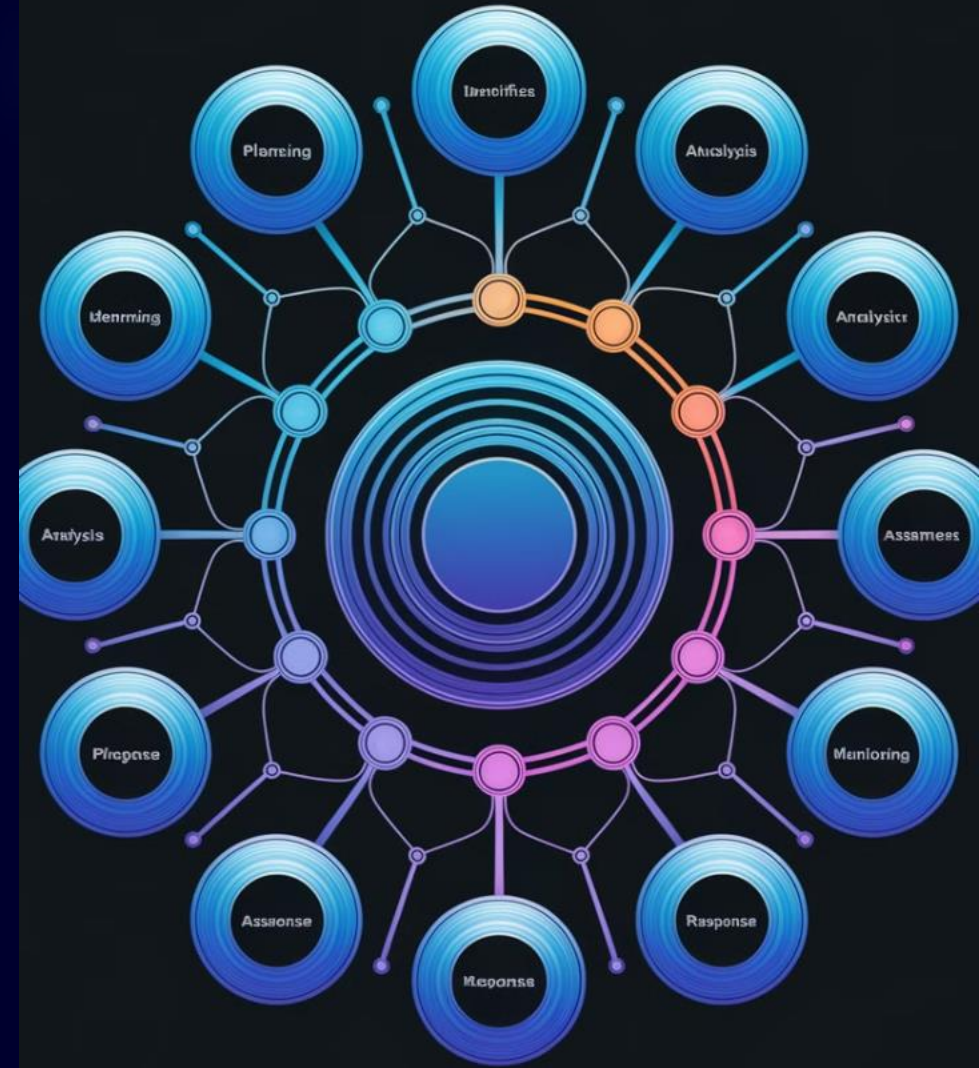


Provides the basis for compliance with applicable regulations

Cybersecurity risk assessment

The Risk Management Lifecycle in Cybersecurity

The risk management lifecycle is a structured process for identifying, assessing, and mitigating cybersecurity risks. It's an ongoing process that requires regular updates to address evolving threats and changes in the organizational environment



Identification Phase

1

Discover Assets

Organizations catalog their systems, assets, and people who influence network security

2

Evaluate Attack Pathways

Identify potential routes that attackers could use to breach the system

3

Recognize Attack Surface

Determine all possible points where an unauthorized user can try to enter or extract data from the environment





Key Aspects of Cybersecurity Risk



Confidentiality

The risk of unauthorized access to sensitive information



Integrity

The risk of data being altered or damaged without authorization



Availability

The risk of information or systems becoming inaccessible when needed

Risk Treatment Strategies



Modify

Applying security controls to mitigate the risk



Retain

Accepting the risk if it falls within acceptable criteria



Avoid

Changing circumstances to eliminate the risk



Share

Distributing the risk with partners or insurers

AVOIDANCE



REPRESENTS



TRANSENTS



ACCEPTANCE



Risk Treatment Options in Cybersecurity

Risk treatment options are essential components of cybersecurity risk management. The four main options for addressing identified risks are

Four Main Risk Treatment Options

1

Accept

Organizations choose to accept the risk without further action. Typically used for low-impact or low-likelihood risks. The cost of mitigation may outweigh the potential impact

3

Transfer

Involves shifting the risk to another entity, often through insurance or outsourcing. Does not eliminate the risk but reduces the organization's direct exposure. Commonly used for financial risks or specialized technical areas

2

Avoid

Involves eliminating the risk entirely by removing the source of the threat. May include discontinuing certain activities or changing processes. Often used for high-impact risks that cannot be effectively mitigated

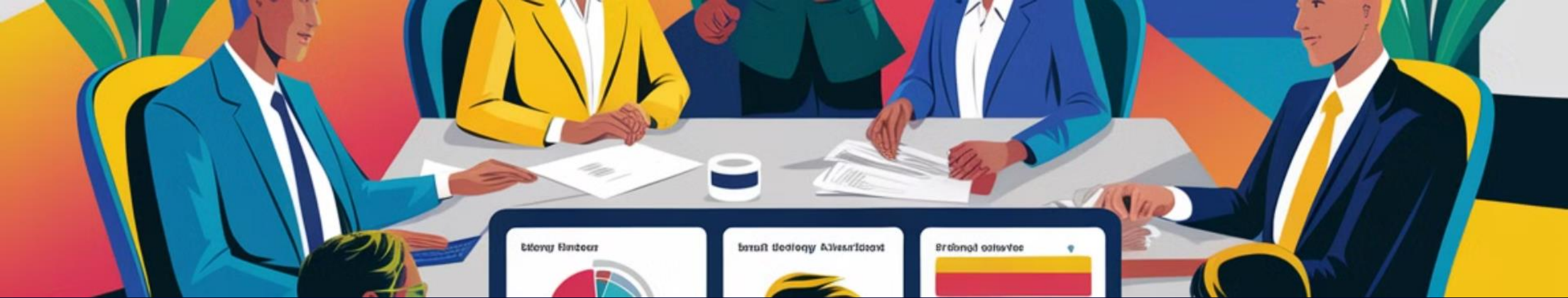
4

Mitigate

Focuses on reducing the likelihood or impact of the risk. Involves implementing controls, such as:

- Technological measures: encryption, firewalls, threat-hunting software
- Best practices: cybersecurity training, software updates, multi-factor authentication

Aims to bring the risk to an acceptable level



Selecting Risk Treatment Options

When selecting a risk treatment option, organizations should consider:

Impact and Likelihood

The potential impact and likelihood of the risk

Cost-effectiveness

The cost-effectiveness of the treatment option

Alignment

Alignment with overall business objectives and risk tolerance

It's important to note that risk management is an ongoing process. Organizations should regularly reassess their risks and the effectiveness of their chosen treatment options to ensure continued protection against evolving threats

Security Controls: Preventive, Detective, and Corrective Measures

Security controls are essential measures implemented to protect information systems and data from various threats. These controls can be categorized into three main types: preventive, detective, and corrective. Each type plays a crucial role in maintaining a robust security posture for organizations



Preventive and Detective Controls

Preventive Controls

Preventive controls aim to stop security incidents before they occur. They act as proactive barriers against potential threats. Examples include:

- Firewalls
- Access control lists
- Strong password policies
- Employee security awareness training
- Encryption
- Physical barriers

Detective Controls

Detective controls are designed to identify and alert on security incidents after they have occurred. They act as surveillance systems, monitoring for suspicious activity. Examples include:

- Intrusion detection systems (IDS)
- Security audits
- Log monitoring
- CCTV cameras
- Vulnerability scanning

Corrective Controls



Incident Response Plans

Detailed procedures for responding to and managing security incidents effectively



Data Recovery Processes

Methods to restore lost or compromised data to its original state



System Patching and Updates

Regular application of security patches and software updates to address vulnerabilities



Post-incident Analysis and Training

Reviewing incidents to improve future responses and educate staff on prevention

Corrective controls focus on mitigating the impact of security incidents and restoring normal operations after an event has occurred. They also aim to prevent similar incidents in the future





Implementing a Defense-in-Depth Strategy

Implementing a defense-in-depth strategy involves creating multiple layers of security to protect an organization's assets. Here's a simple approach to implementing this strategy

Steps to Implement Defense-in-Depth

1

Assess and Plan

Conduct a thorough assessment of your organization's current security posture, identifying critical assets, potential threats, and vulnerabilities

2

Implement Layered Security

- Physical Controls: Secure physical access to IT systems with measures like keycards and locked doors
- Network Security: Deploy firewalls, VPNs, and intrusion detection/prevention systems
- Endpoint Protection: Install anti-spam and antivirus software on workstations
- Access Management: Implement multi-factor authentication and role-based access control
- Data Protection: Use encryption for sensitive data and secure transfer protocols

3

Educate Users

Provide security awareness training to employees on best practices and policies

4

Regular Updates and Patching

Keep all systems and software up-to-date with the latest security patches

5

Continuous Monitoring

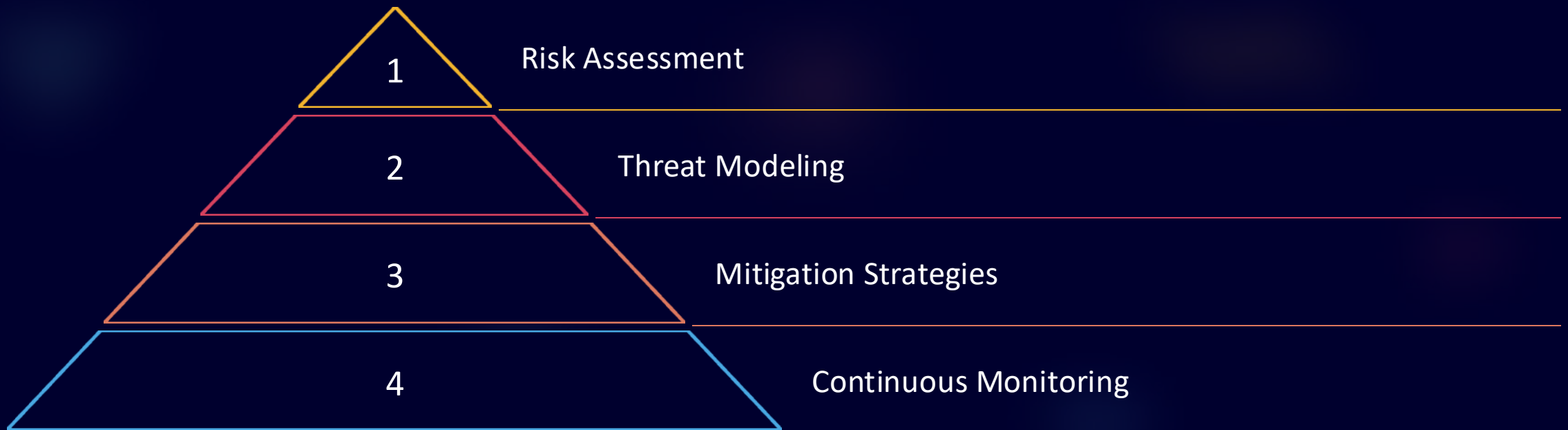
Implement logging and vulnerability scanning to detect and respond to security events promptly

6

Review and Improve

Regularly assess the effectiveness of your security measures and update your strategy as threats evolve

Conclusion: Comprehensive Cybersecurity Risk Management

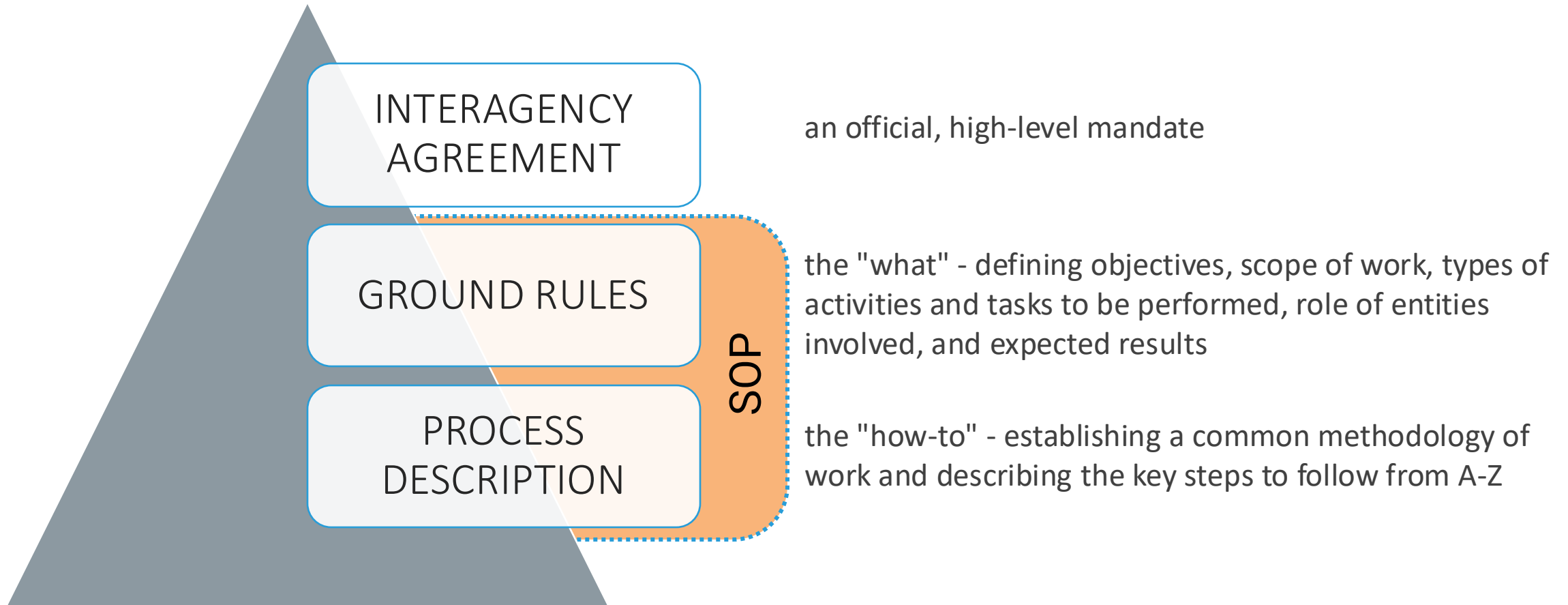


A comprehensive approach to cybersecurity risk management involves thorough risk assessment, effective threat modeling, implementation of robust mitigation strategies, and ongoing monitoring and reassessment

Inter-agencies cooperation

Key elements structuring interagency cooperation

242



Common language and scoring

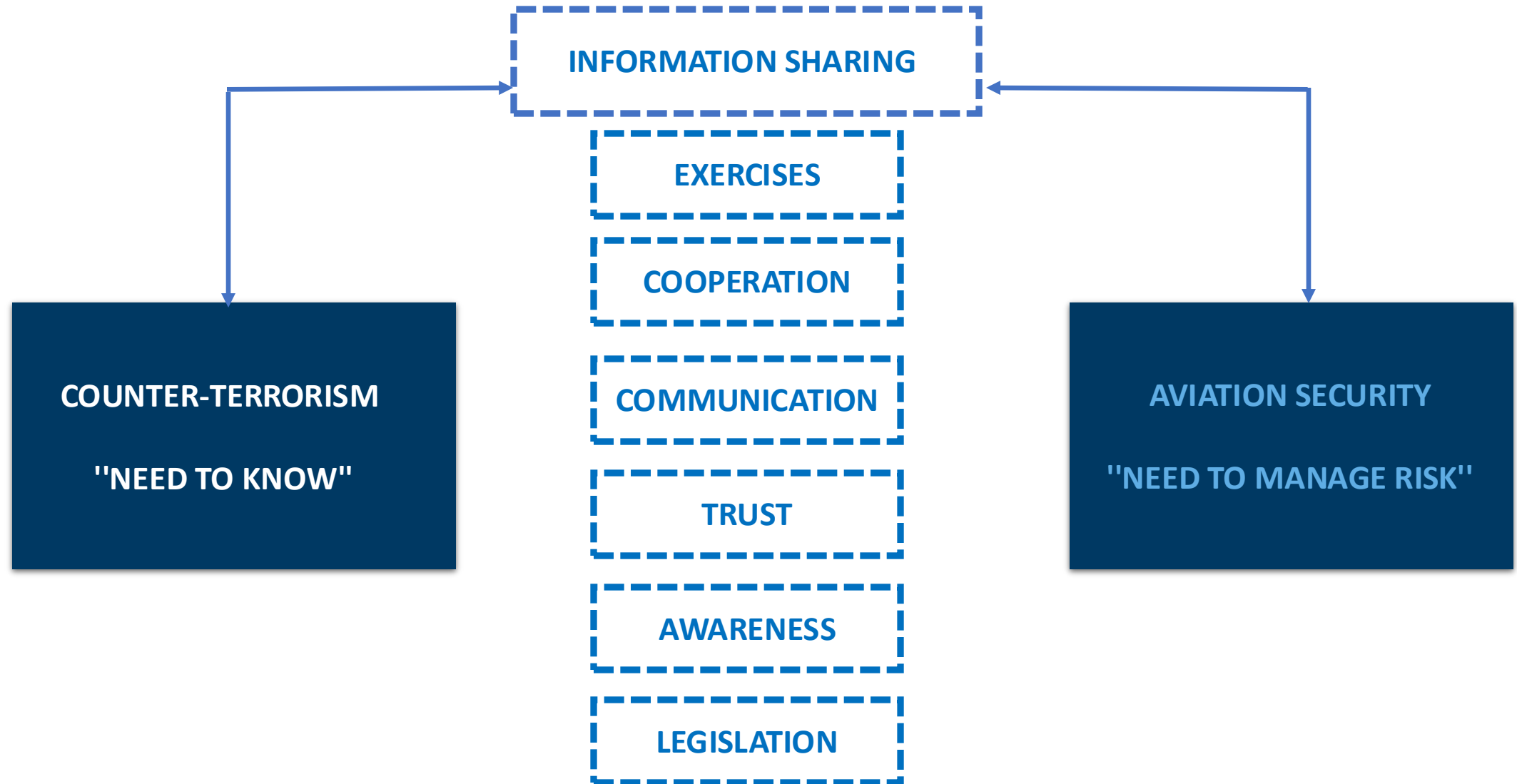
243

- Threat
- Intent
- Capability
- Opportunity
- Risk
- Vulnerability
- Consequence
- Scenario
- Assessment
- Methodology
- Score levels*
- AVSEC
- AVSEC operators
- Mitigation measures
- Classification
- Sanitization

* consider table of equivalencies

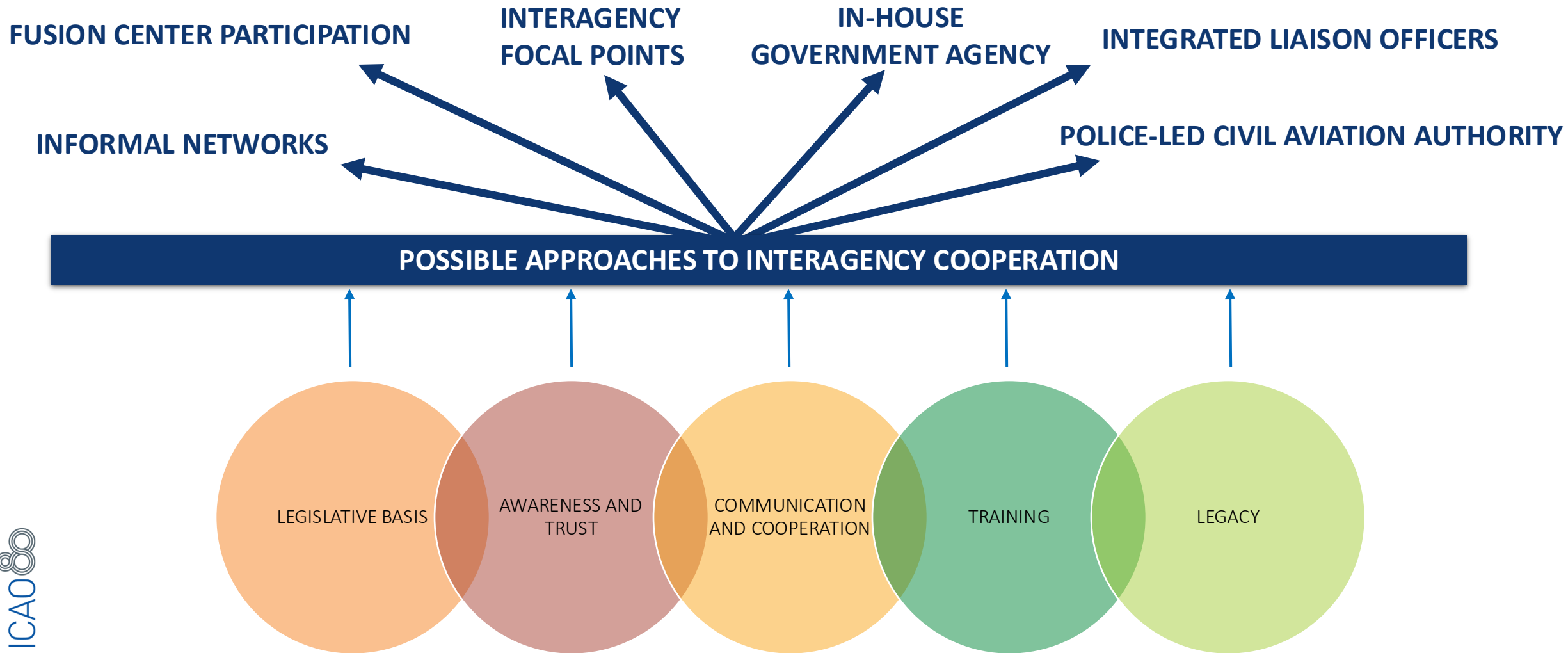
Transparent and interconnected elements

244



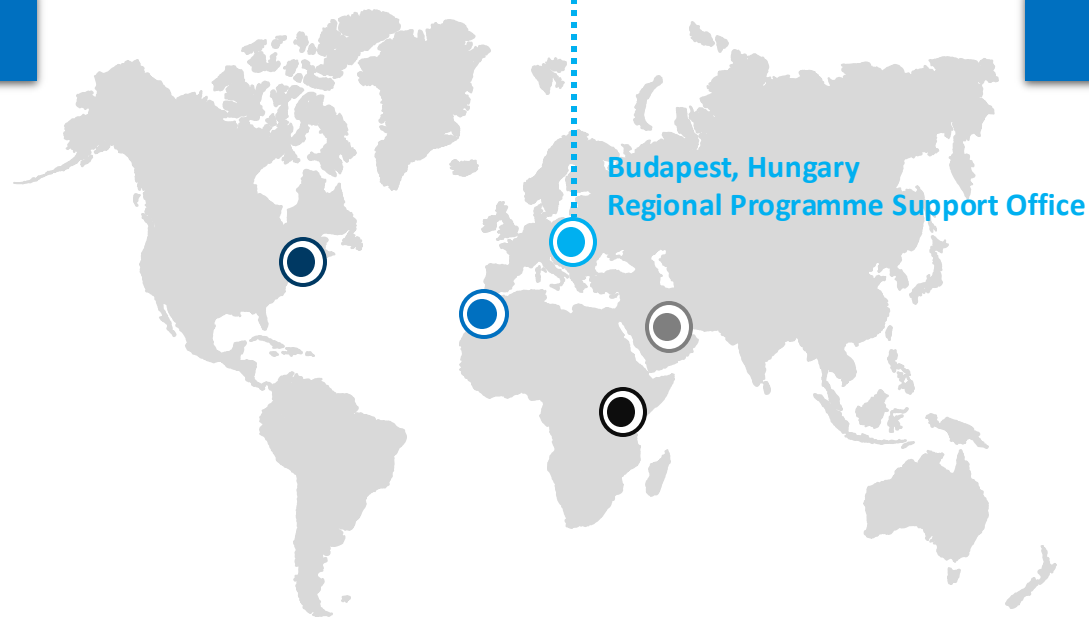
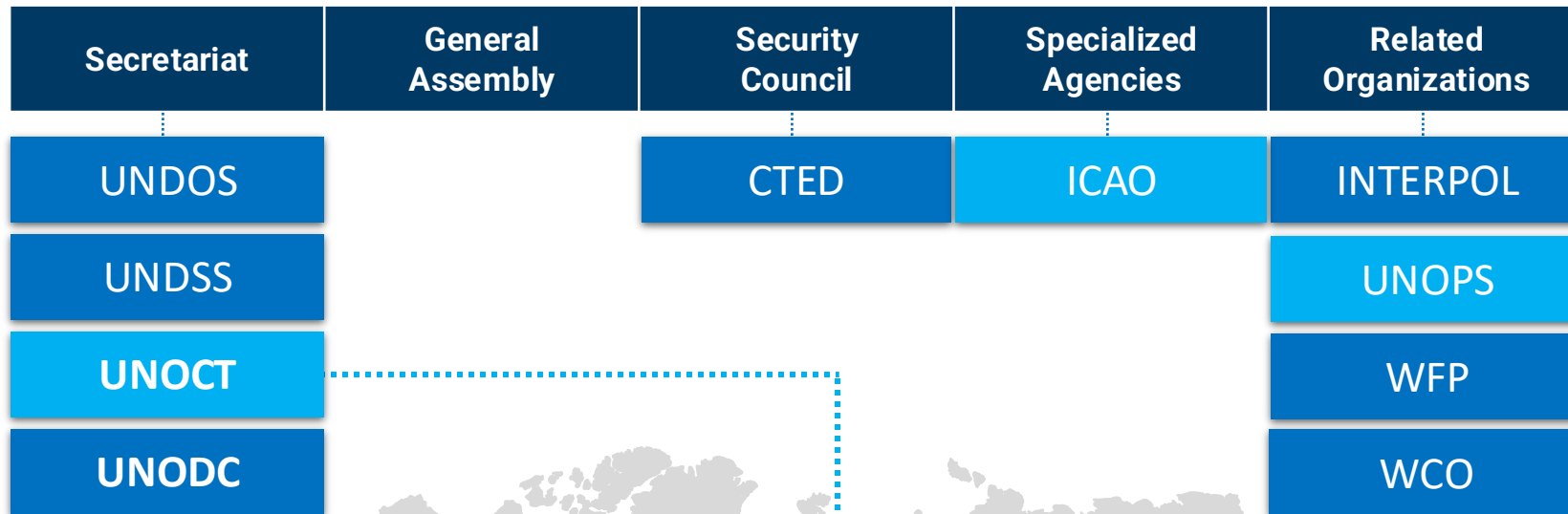
Results of TAM Programme global scan

245



UNOCT-ICAO TAM Programme orientation

24



Solution: harmonizing points of mutual interest

247

