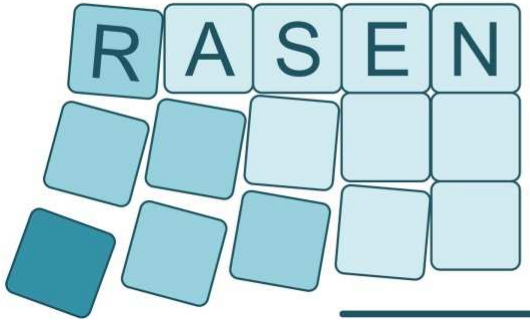


Compositional Risk Assessment and Security Testing of Networked Systems

Jürgen Großmann
(FhG Fokus)
Fredrik Seehusen
(SINTEF ICT)

Combining Security Risk Assessment and Security Testing based on Standards

3rd RISK Workshop

at OMG TC in Berlin, 2015-06-16

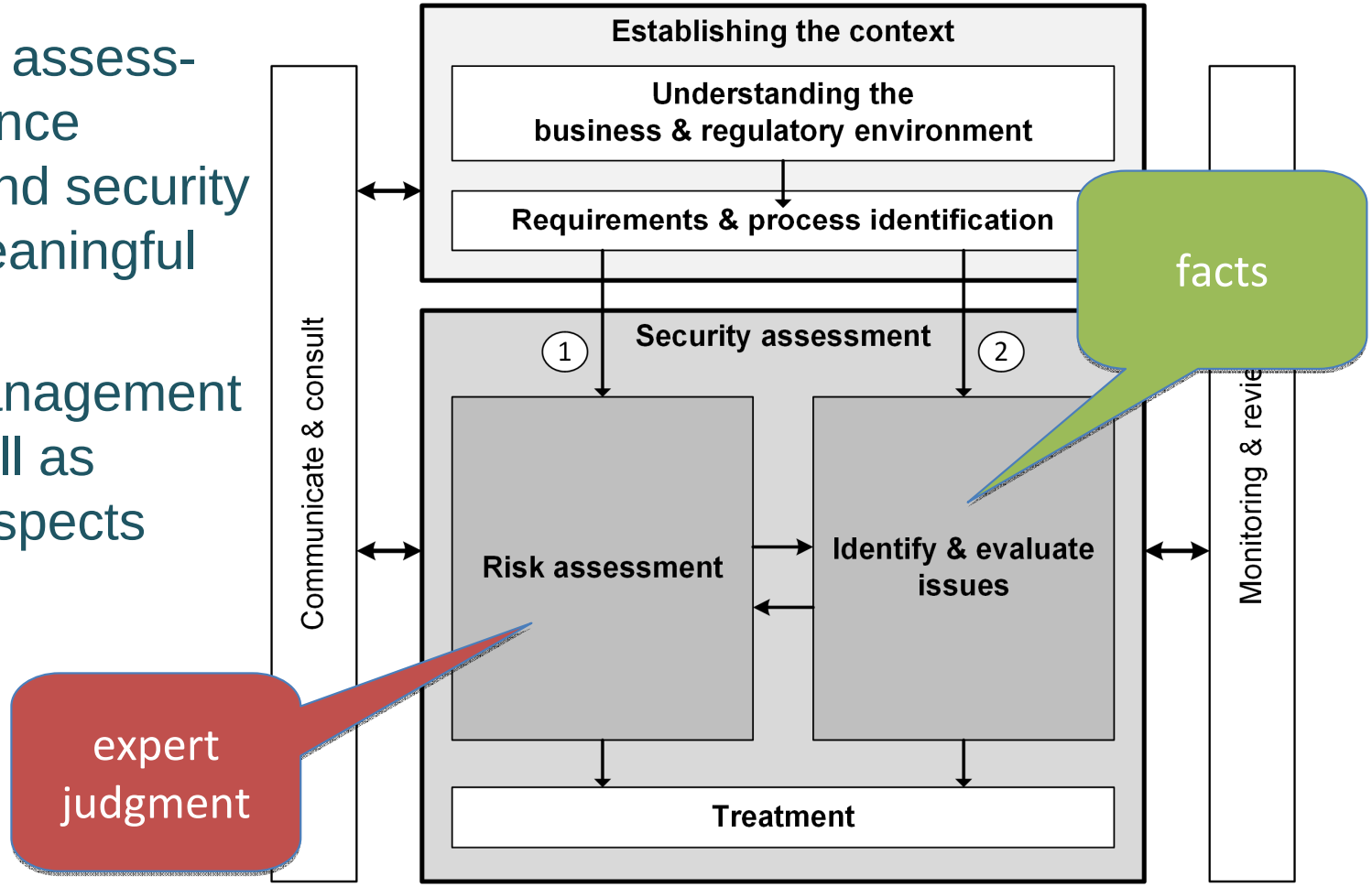
FP7 project **RASEN** (RASEN - 316853)

Developing methods and tools to support **security assessments** for **large-scale networked infrastructures** by considering:

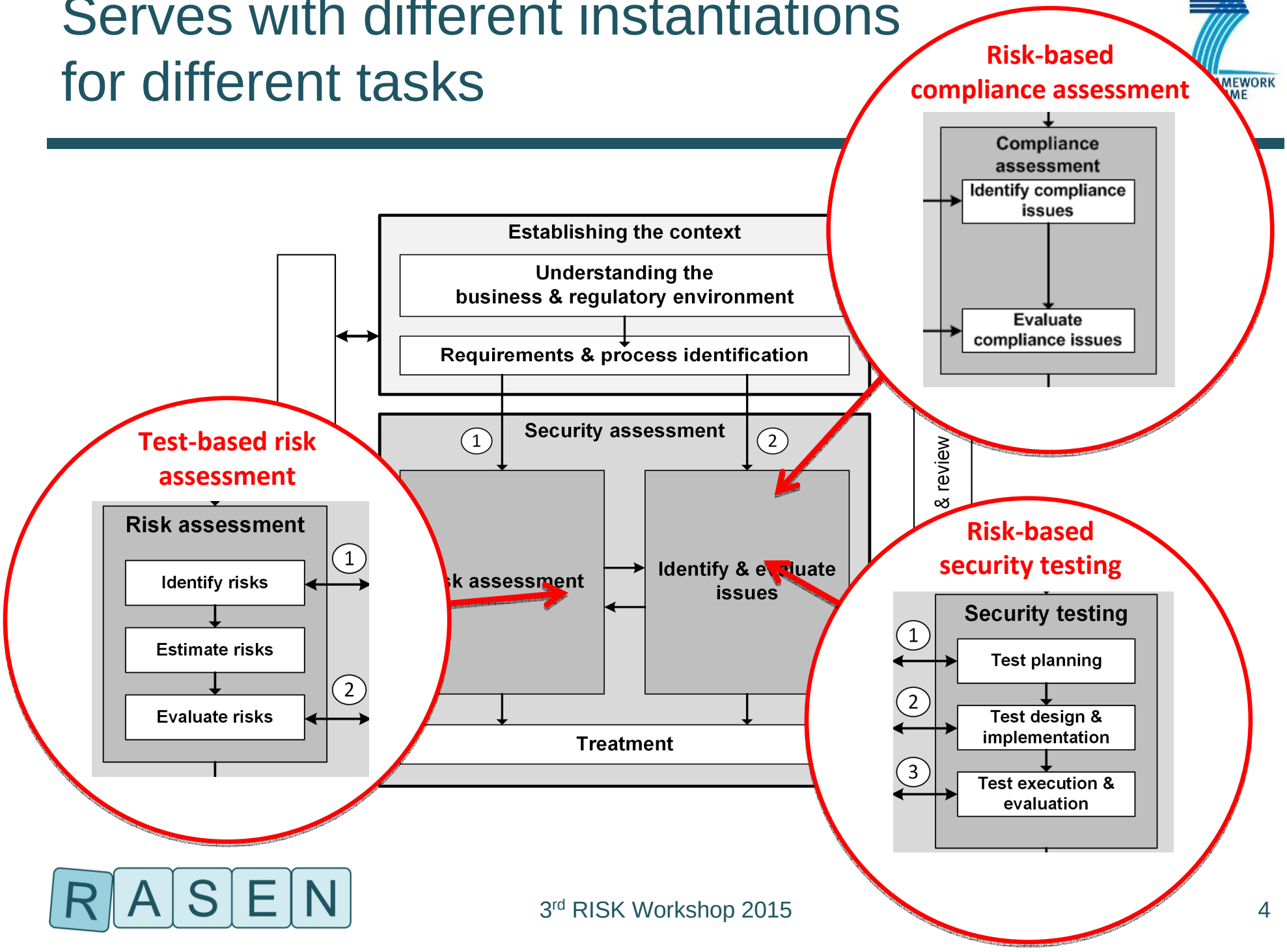
1. technical aspects
2. legal and regulatory aspects
3. uncertainty and risk

The RASEN method for security testing, risk & compliance assessment

- Conforms to ISO/IEC 31000
- Integrates risk assess-ment, compliance assessment and security testing in a meaningful manner
- Addresses management aspects as well as assessment aspects



Serves with different instantiations for different tasks



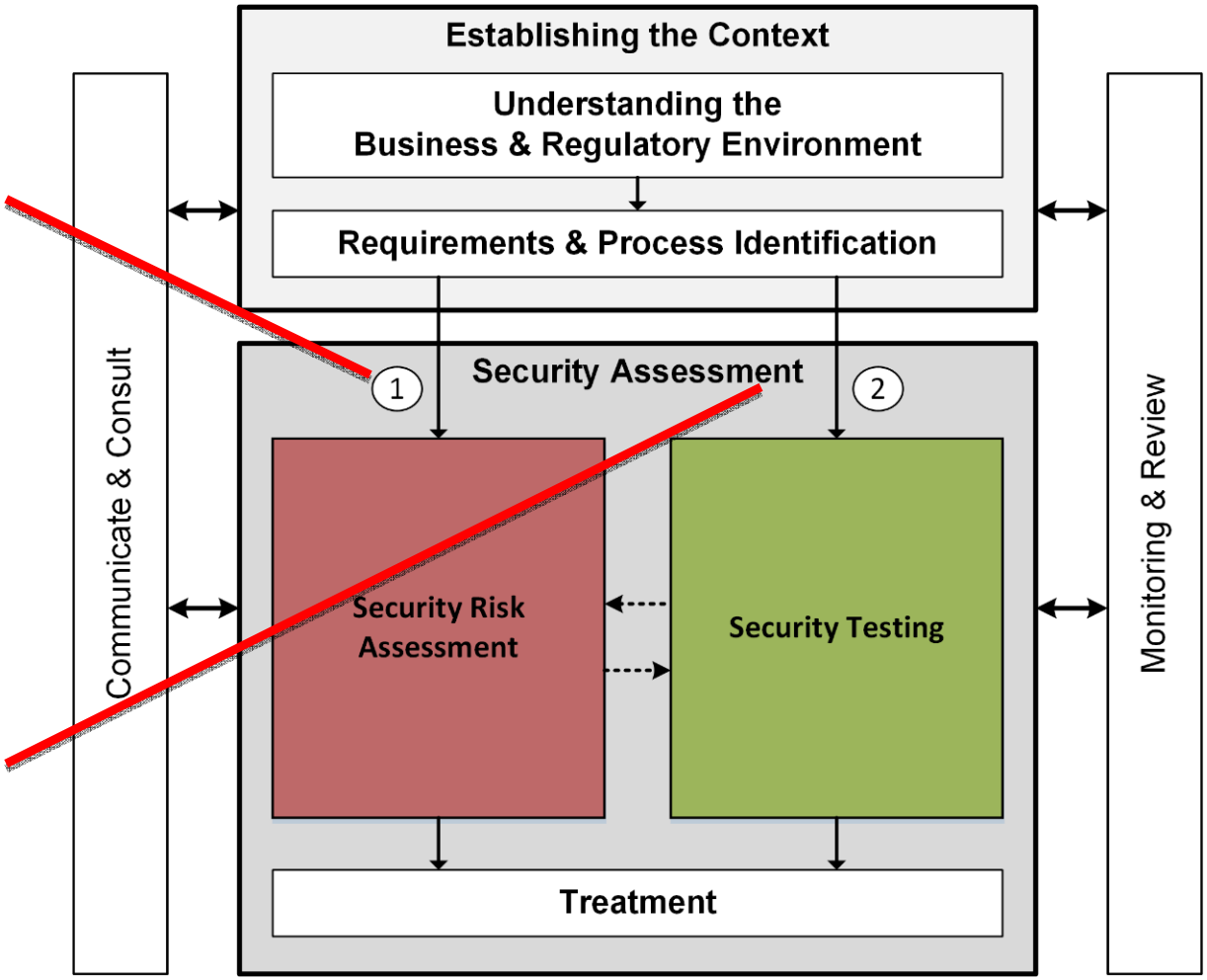
Two main workstreams: Risk assessment and security testing

A test-based security risk assessment process (1)

- starts with the risk assessment
- is used to optimize security risk assessment with empirical data coming from test results or compliance issues.

A risk-based method for compliance and security testing (2)

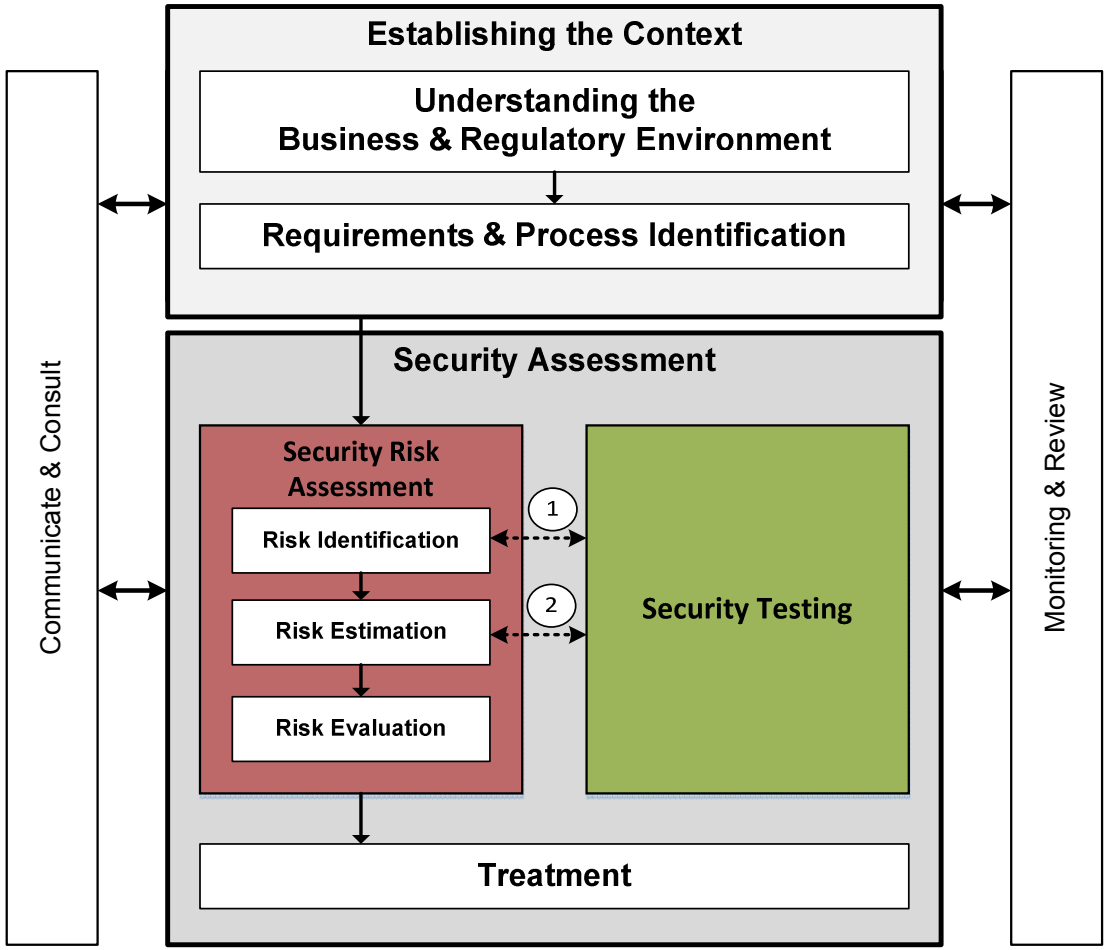
- starts with the identification of issues by security testing or compliance assessment
- focus the compliance and security testing resources on the areas that are most likely to cause concern
- building and prioritizing the compliance measures or testing program around these risks.



Workstream 1: Test-based security risk assessment

1. Test-based risk identification
2. Test-based risk estimation

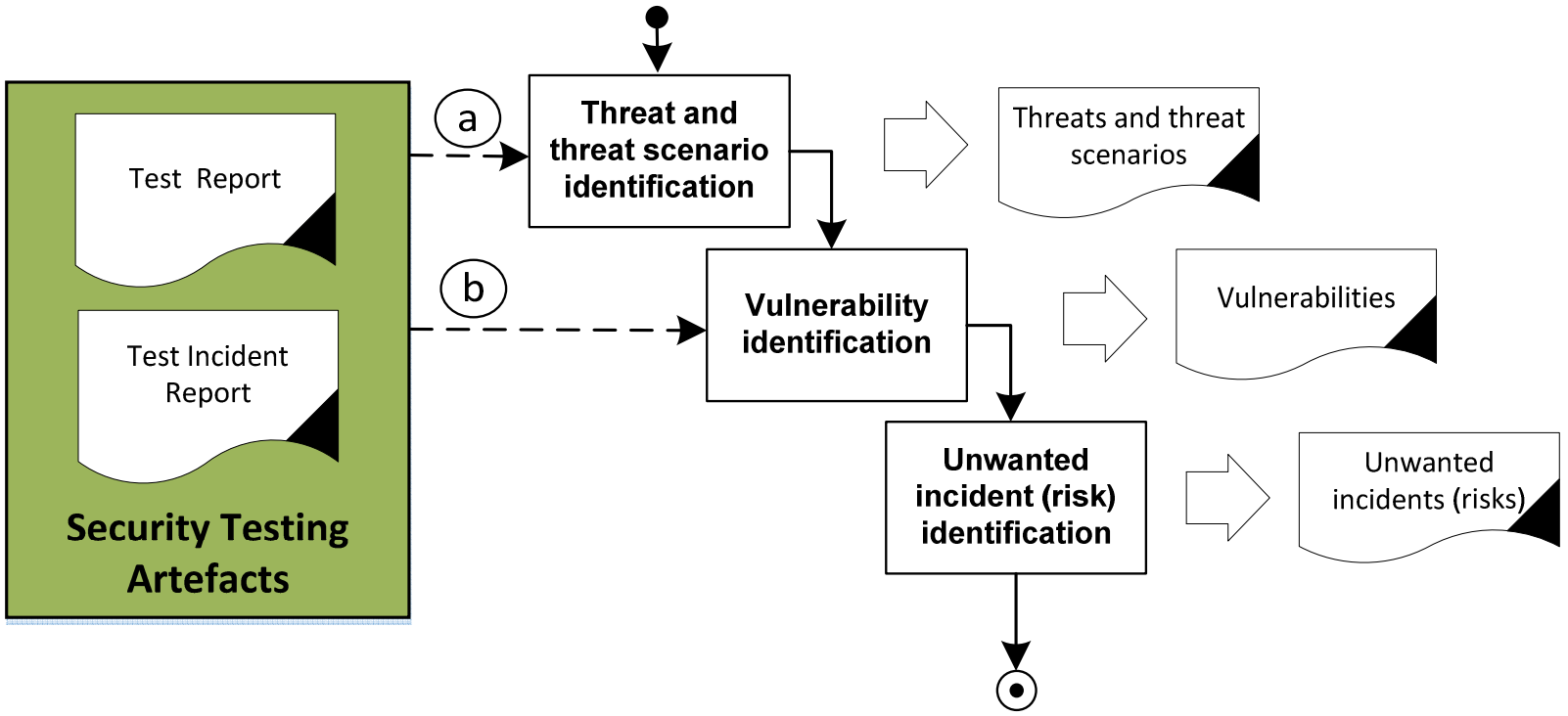
- **Basic idea:** improve risk assessment activities through facts from testing



Test-based risk identification

a) Test-based threat and threat scenario identification

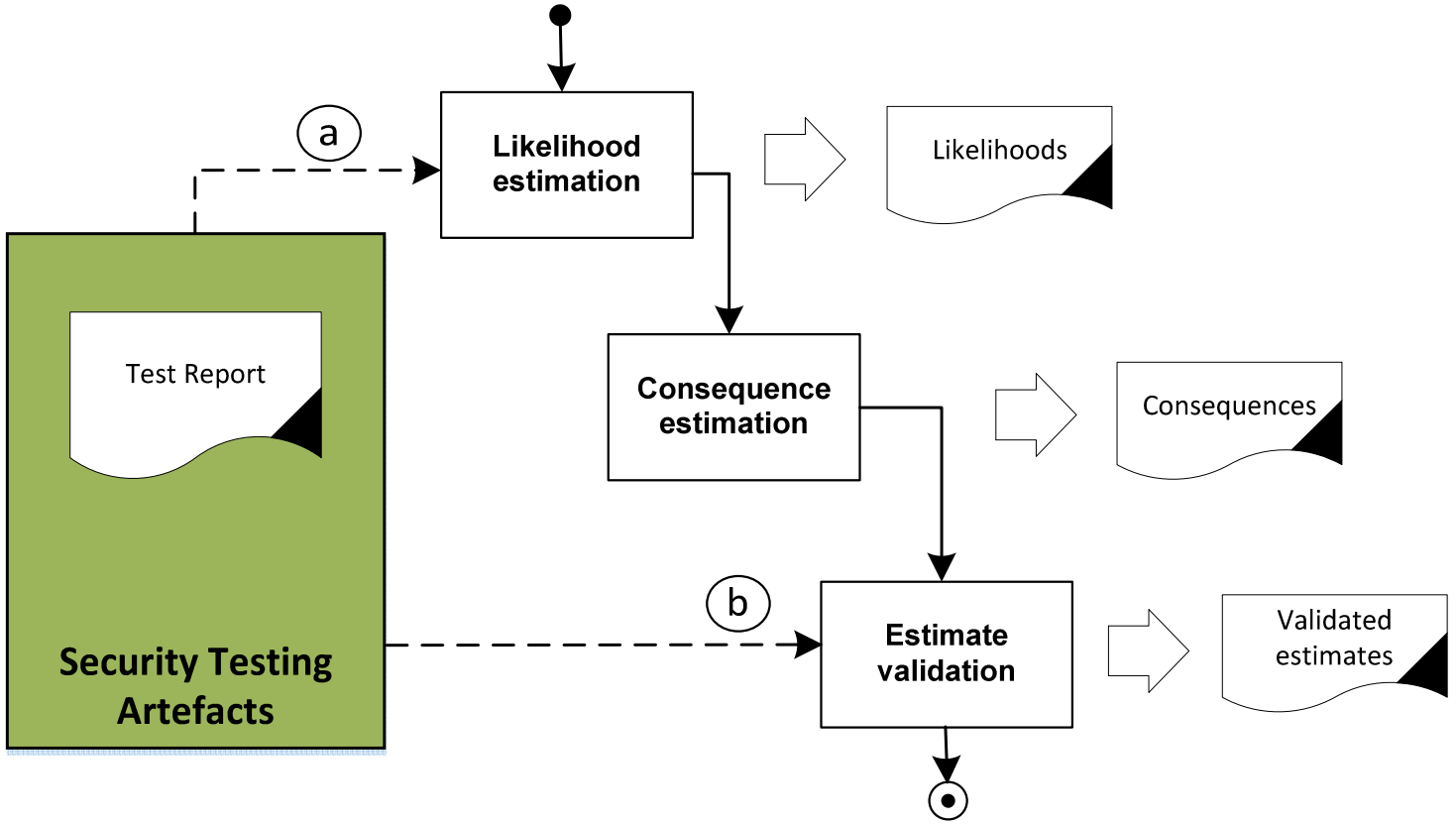
b) Test-based vulnerability identification



Test-based risk estimation

a) Test-based likelihood estimation

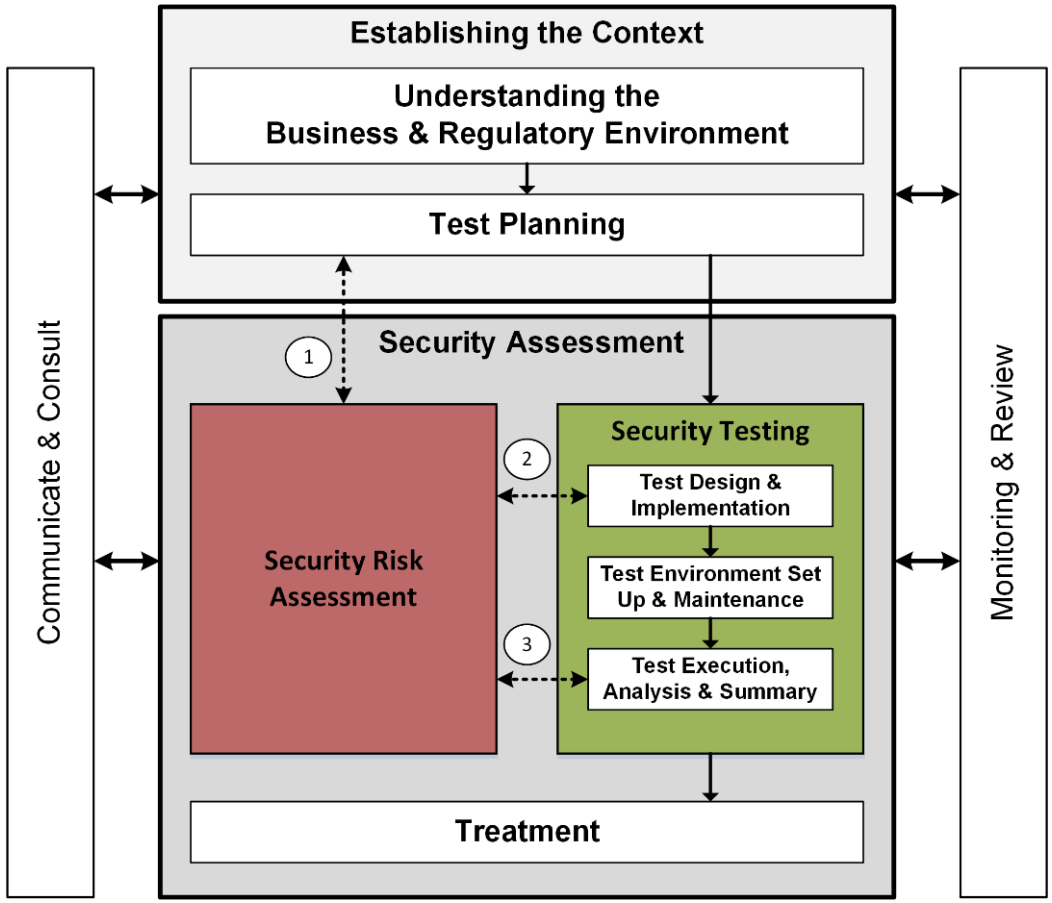
b) Test-based estimate validation



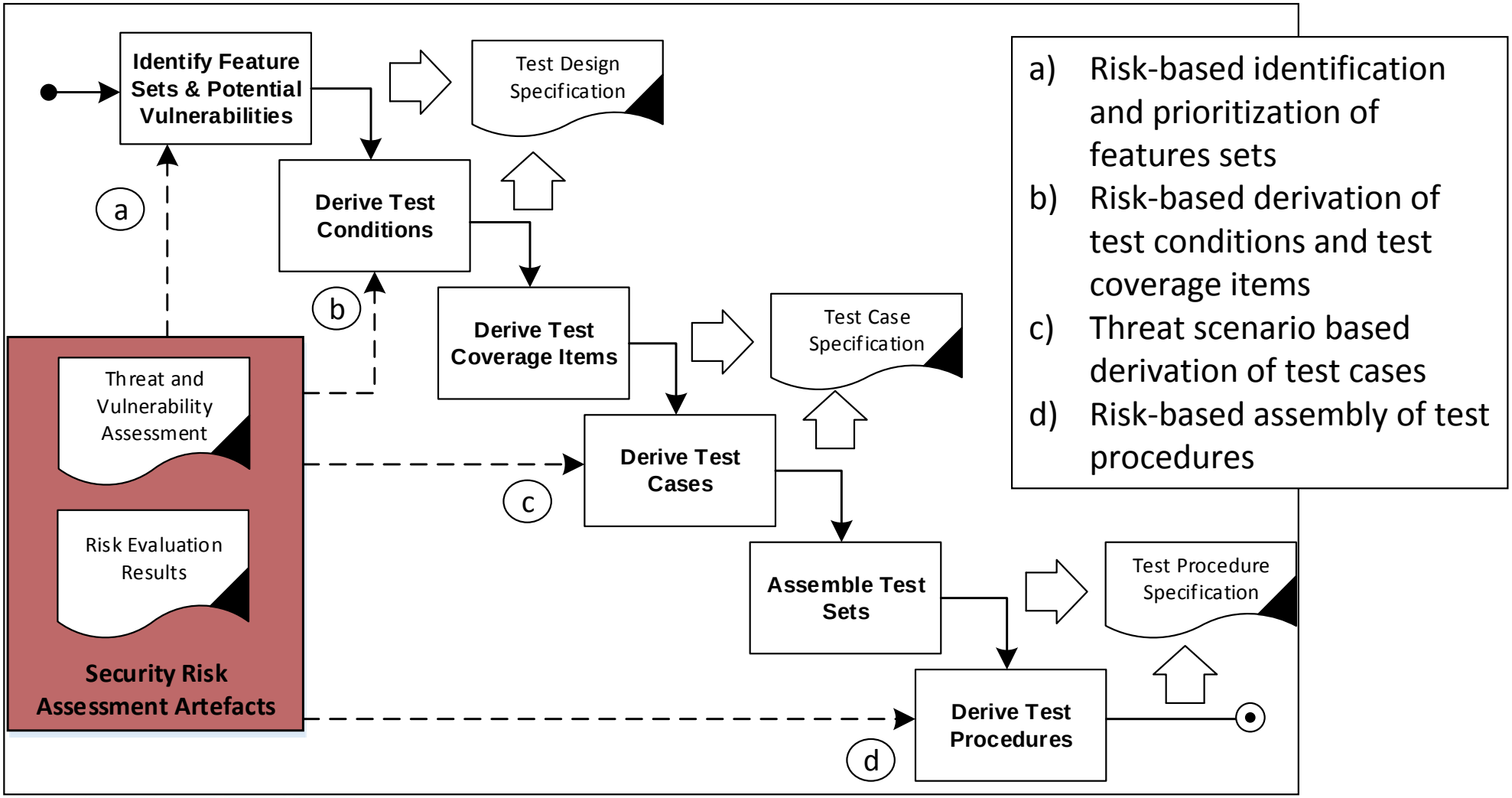
Workstream 2: Risk-based security testing compliant to ISO 29119

1. Risk-based security test planning
2. Risk-based security test design & implementation
3. Risk-based test execution, analysis & summary

- **Basic idea:** focus testing activities on high risk areas



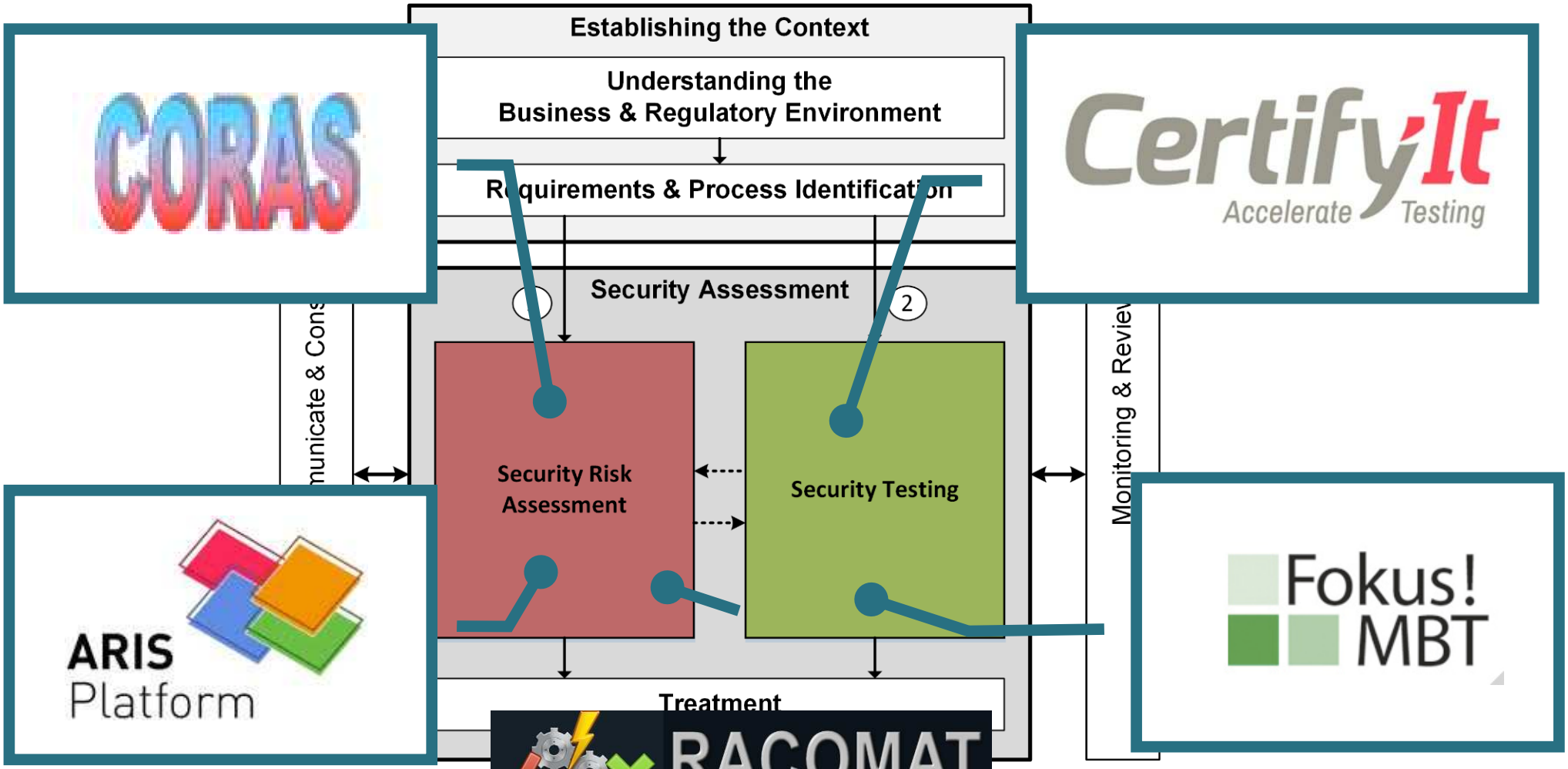
Risk-based security test design and implementation



Activities are specified in detail to provide guidance

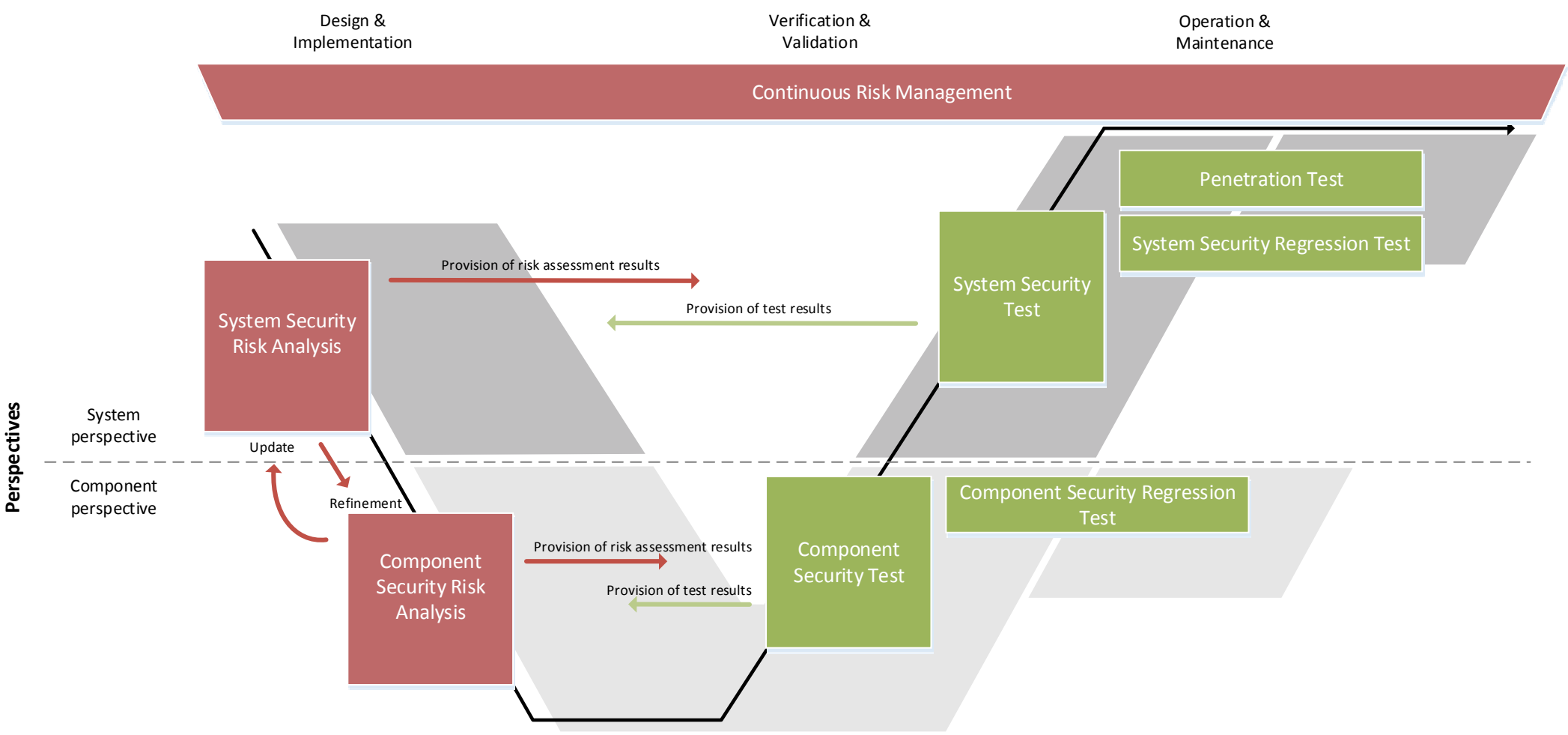
Name	**Risk-based identification and prioritization of features sets (a)**
Actors	Security Tester (ST), Security Risk Analyst (SRA)
Tools	Test Specification Tool (STST), Security Risk Assessment Tool (SRAT)
Precondition	Security relevant features are documented and the security risk assessment is available
Postcondition	Security relevant features to be tested are grouped with respect to potential vulnerabilities and threat scenarios.
Scenario	1. The Security Tester should identify testable security relevant features that need to be covered by security testing. The security tester classifies the security relevant features by grouping them to form feature sets that each addresses exactly one threat scenario and/or one vulnerability. 2. The Security Tester should prioritize the security relevant feature sets using the risk levels that are associated with the threat scenario and/or vulnerabilities. 3. The Security Tester should document the relations between security relevant feature sets and their associated threat scenarios and/or vulnerabilities (maintain traceability).
Data exchanged/ processed	**In:** *Vulnerabilities*, *threat scenarios*, *unwanted incident*, *likelihoods, consequences, risk level* **Out:** *Prioritized list of testable security relevant features (security feature sets).*

Supported by the **RASEN toolbox** and the **RASEN exchange** format



RASEN

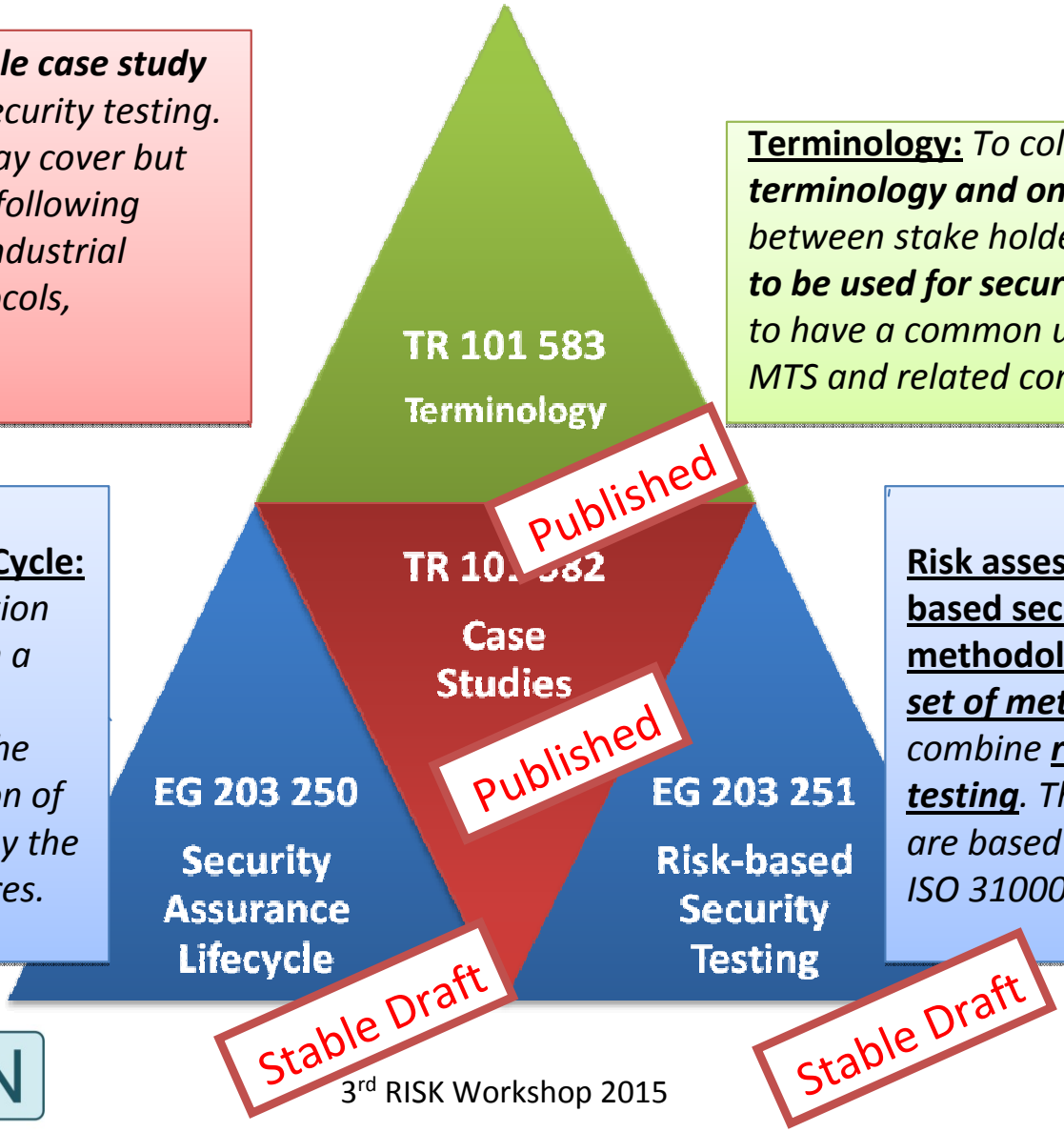
Mapping to System Lifecycle Phases



The RASEN method is itself in **standardization**

Case Studies: *To **assemble case study experiences** related to security testing. Industrial experiences may cover but are not restricted to the following domains: Smart Cards, Industrial Automation, Radio Protocols, Transport/Automotive, Telecommunication*

Terminology: *To collect the **basic terminology and ontology** (relationship between stake holder and application) **to be used for security testing** in order to have a common understanding in MTS and related committees.*



Security Assurance Life Cycle: ***Guidance to** the application **system designers** in such a way to maximise both security assurance and the verification and validation of the capabilities offered by the system's security measures.*

Risk assessment and risk-based security testing methodologies: *Describes a **set of methodologies** that combine **risk assessment and testing**. The methododologies are based on standards like ISO 31000 and IEEE 29119*

RASEN

RASEN method summary

- Covers the integration of security testing, risk & compliance assessment
- Is concisely specified and supported by tools
- Is mature and powerful
  - applied to all RASEN case studies
  - integrates with recent risk assessment and testing standards
  - constitutes standardization work item at ETSI

THANK YOU!

Questions and Comments?