The CYRENE Risk and Conformity Assessment (RCA) Methodology

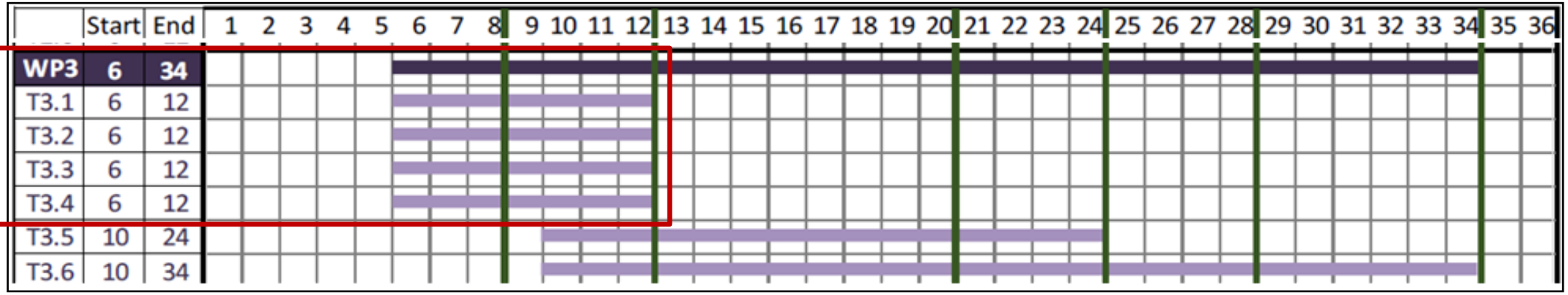
[FP-MAG-HYPER]

1st Review Meeting, Remote
5/04/2022

European Commission

Related WP and Tasks

CYRENE RCA Methodology Development



Outcome of Tasks:

T3.1 Models for Infrastructure Dependencies and Events [M6-M12]

T3.2 Multi-Layer Algorithms for Quantitative and Qualitative Analysis of Cascading Effects [M6-M12]

T3.3 Analysis and Documentation of Risks and Measures for Reducing their Effects [M6-M12]

T3.4 Conformity Evaluation Process and Multi-Level Evidence-Driven Supply Chain Risk Assessment Specifications [M6-M12]

D3.1 Conformity Evaluation Process & Multi-Level Evidence-Driven Supply Chain Risk Assessment
[PU] Due: M12

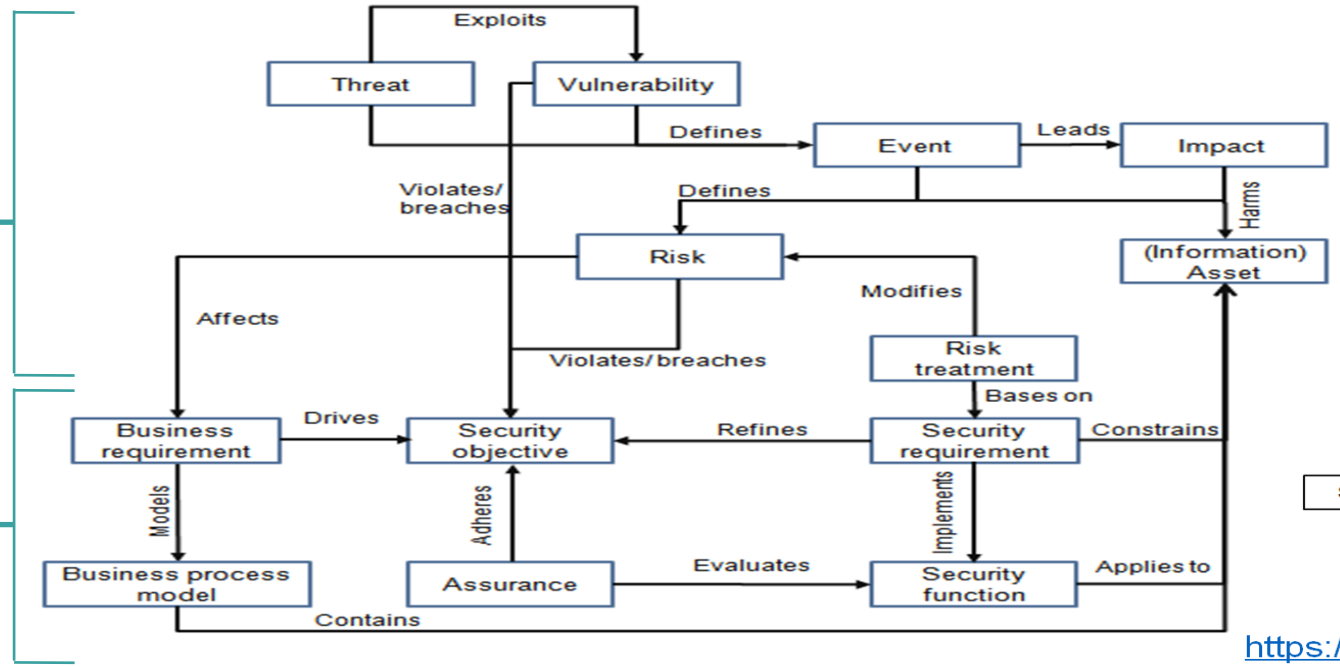
CYRENE RCA Methodology
Vision

An Extended Security Model

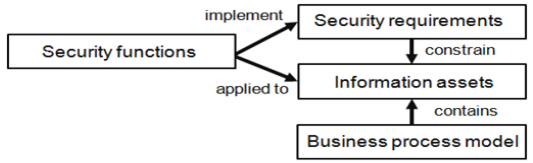
INTERPLAY BETWEEN RISK AND CONFORMITY ASSESSMENT (RCA)

Information Security Concepts (ISO/IEC 27k)

Conformity Assessment Concepts (ISO/IEC 15408, ISO/IEC 18045)



A dual use evaluation process for SCS*
- ❑ Risk Assessment (SCS-RA)
- ❑ Conformity Assessment Processs (SCS-CAP)



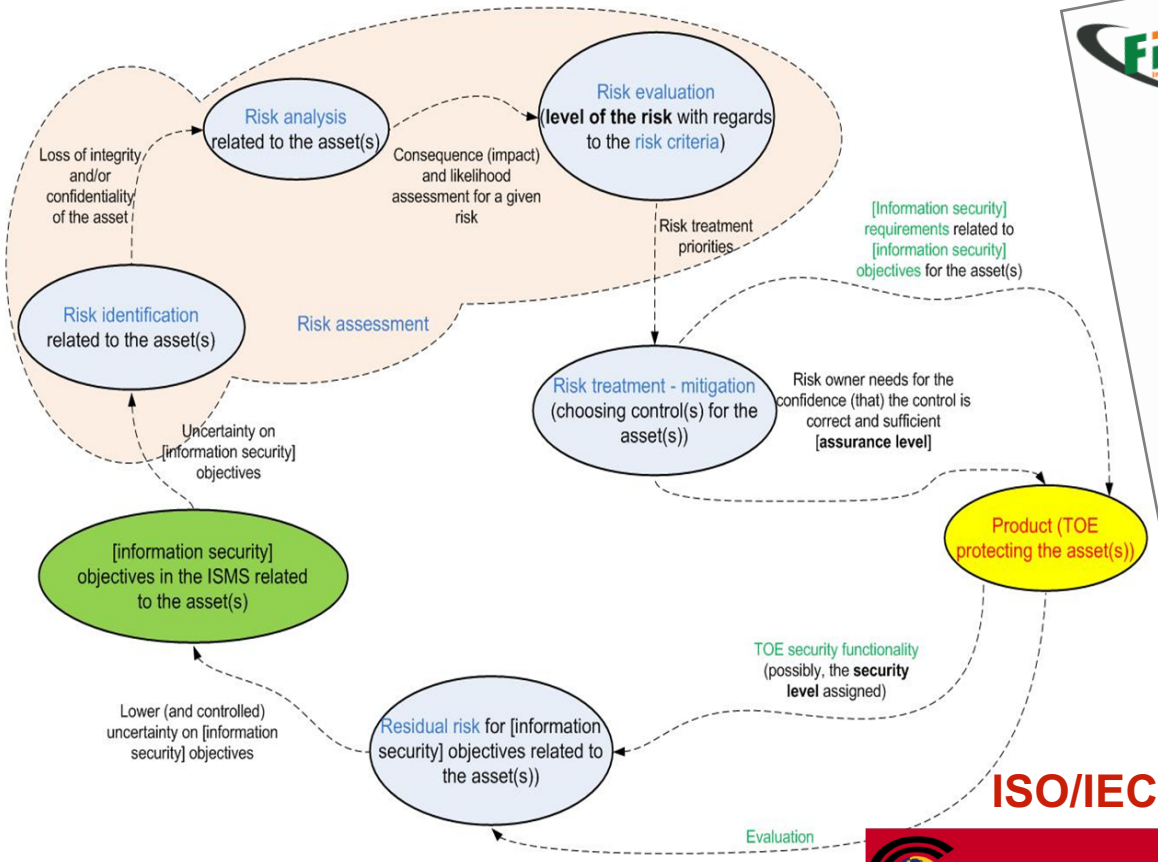
https://www.cyrene.eu/glossary/

(Source: Taubenberger, Stefan (2014) "Vulnerability Identification Errors in Security Risk Assessments". PhD thesis The Open University).

*SCS: Supply Chain Service

Legal Background and Standards

CYRENE



ISO/IEC 15408

Common Criteria

ISO 28k

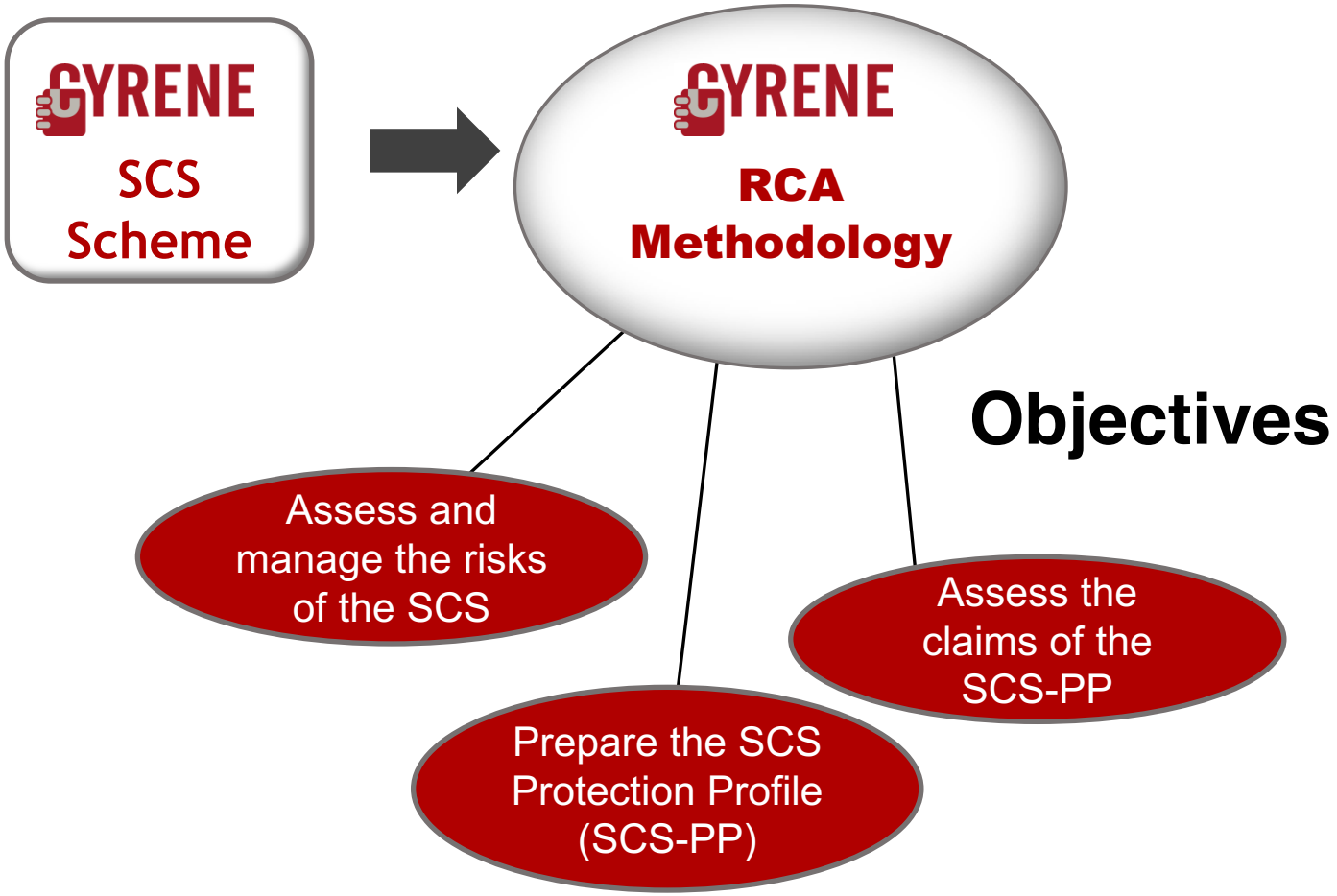
ISO

IEC

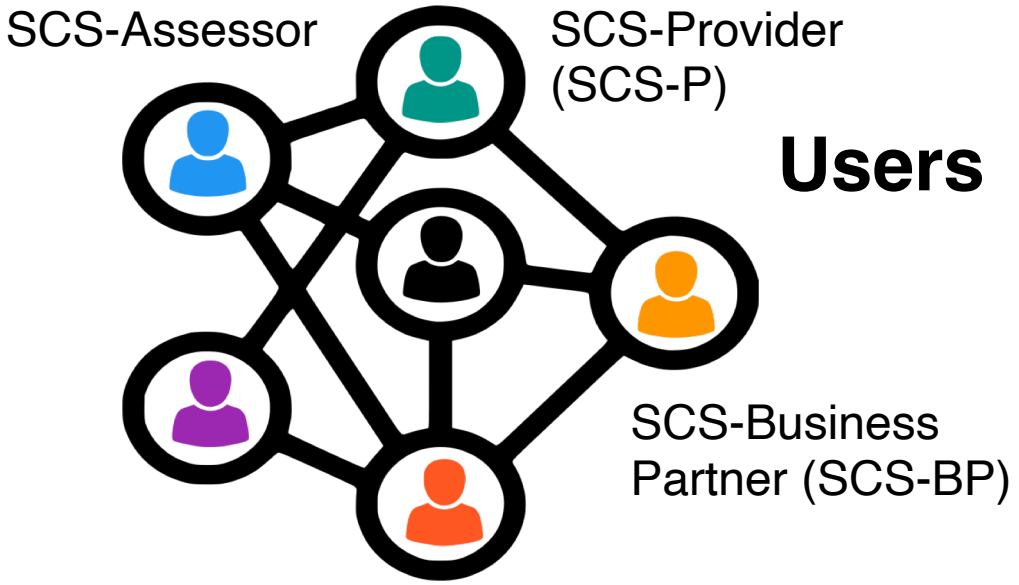
ISO/IEC 18045

ISO/IEC 27k

CYRENE RCA Methodology
Objectives – Users – Outcomes



Objectives



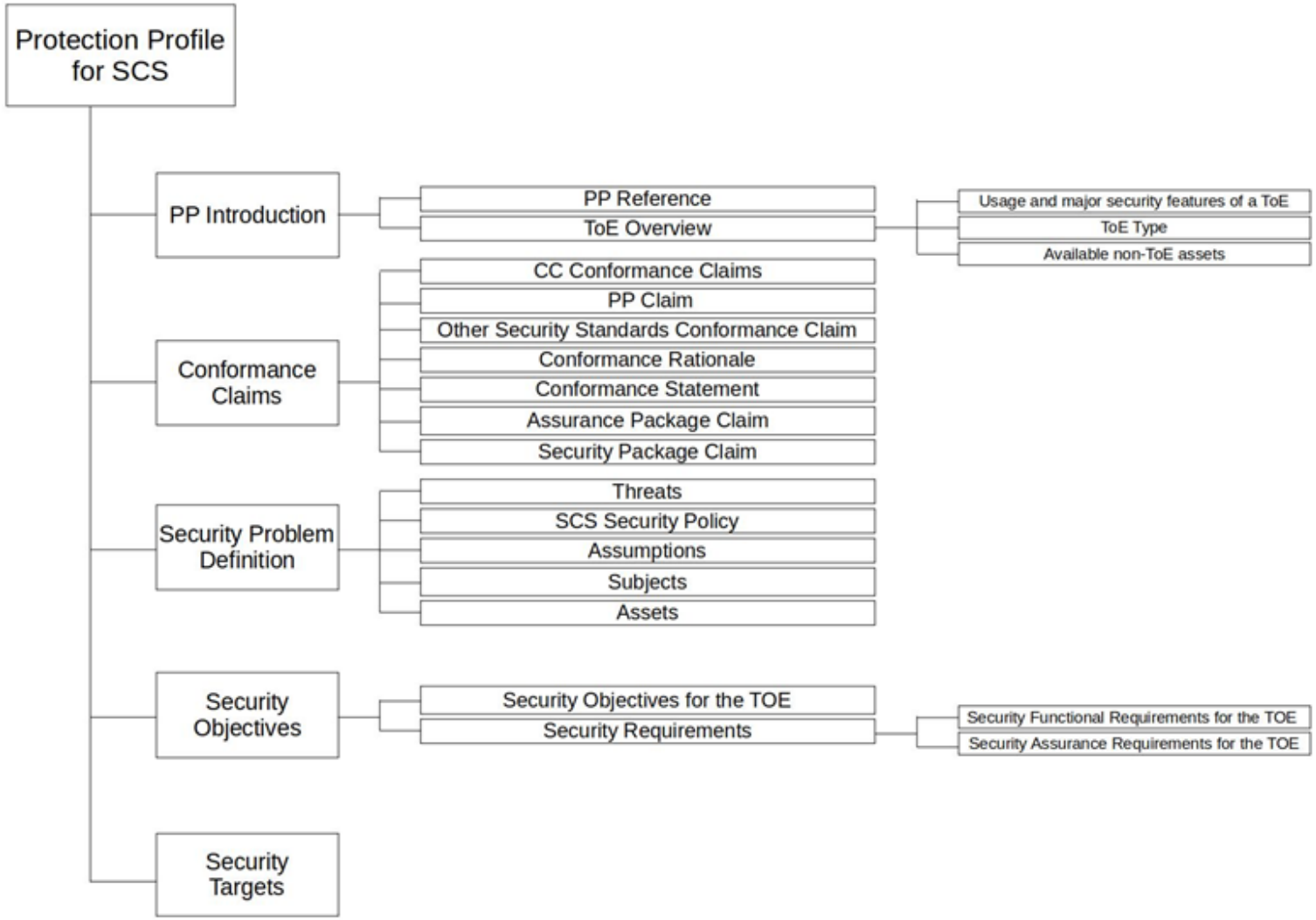
Users

Outcomes

- ❑ Risk Assessment Report
- ❑ Risk Treatment Report
- ❑ SCS-Protection Profile

*SCS: Supply Chain Service

CYRENE Supply Chain Service Protection Profile (SCS-PP)



CYRENE RCA Methodology
Assumptions / Benefits

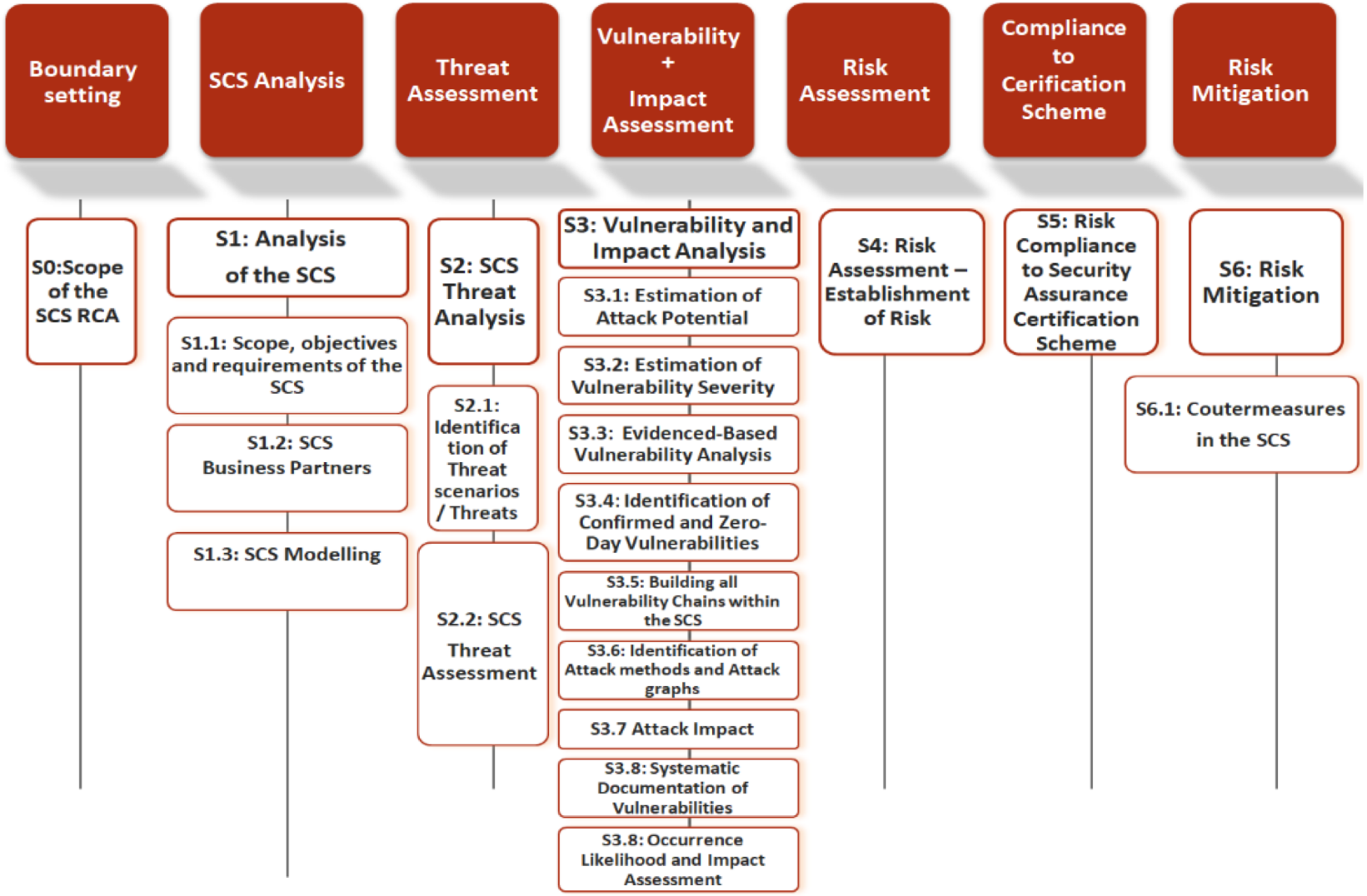
Assumptions

- ❑ The perimeter of the CYRENE RCA includes only assets in the provision of the SCS. SCS-assets hosted by the different SCS-BPs are isolated from their organization network.
- ❑ SCS-BPs submit their security policies, SCS assets and implemented controls docs under signing mutual agreement(s):
  - ❖ Security Declaration and statement of Application (SDA)
  - ❖ Mutual Recognition Agreement (MRA)

Benefits

- ❑ Double use; Risk - Conformity interplay
- ❑ Up-to-date threat and vulnerability information
- ❑ Addresses highly interconnected SCS assets
- ❑ Compliant with EU regulations & international standards
- ❑ Applicable to all SCS sectors with different Assurance Levels
- ❑ Enhances security, privacy, resilience, accountability and trustworthiness of SCS:
  - ❖ Increases SCS level of competence in the internal market
  - ❖ Strengthens the EU economy

CYRENE RCA Methodology **Overview**



CYRENE RCA Methodology

Step 0: Scope of the SCS RCA

Scope

- SCS as Target of Evaluation (SCS-TOE)
- Assessment scope
- SCS evaluation view
- Assessment boundaries
- Assurance level, Attack Potential and AVA_VAN according to SCS criticality

Input

- SCS SDA signed from SCS-BPs and SCS MRA signed whether required

Outcome

- Specification of the boundaries of the SCS RCA

CYRENE RCA Methodology

Step 0: Scope of the SCS RCA

SCS Assurance Scales

CYRENE SCS Criticality (based on NIS 2 DIRECTIVE)	**CYRENE Assurance Level (AL)** (EUSCS)	**Vulnerability Analysis (AVA Class)** (ISO/IEC 15408-CC)	**Attack Potential (AP)** (ISO/IEC 18045)
The SCS-Provider is **neither an operator of essential service nor an operator of important service.**	Basic	AVA_VAN.1 Vulnerability survey	Basic
The SCS-Provider is an **operator of important service.**	Substantial	AVA_VAN.2 Vulnerability analysis	Basic
The SCS-Provider is an **operator of essential service.**	Substantial	AVA_VAN.3 Focused vulnerability analysis	Enhanced Basic
The SCS-Provider is an operator of **essential and international service** of global supply chains (including business partners from non EU Member States).	High	AVA_VAN.4 Methodical vulnerability analysis	Moderate
The SCS-Provider is an **operator of a military/defense service** (national security, law enforcement).	High	AVA_VAN.5 Advanced Methodical/ Advanced Technical/vulnerability analysis	High

- **Assessment scope:** RA, develop SCS-PP, assess the claims of SCS-PP
- **SCS evaluation view** : overall business/ holistic-technical/ sector-specific technical views
- **SCS criticality** (based on NIS 2 Directive) determines:
  - The Assurance Level followed (CYRENE EUSCS)
  - The level of Vulnerability Analysis (AVA_VAN) adopted (Assurance Class AVA, ISO/IEC 15408-CC)
  - The SCS is resistant to attacks performed by an attacker possessing a specified level of Attack Potential

CYRENE RCA Methodology

Step 1: Analysis of the SCS

Scope

- Analysis of SCS components: processes / Business Partners / assets
- Identification of SCS security objectives & requirements

Input

- SCS-ISMS of each SCS Business Partner (SCS-BP): SCS assets, implemented controls (SDA)

Outcome

- Security objectives/requirements/SCS processes (textual description)
- SCS business models/asset models
- Lists of security controls implemented on assets
- SCS processes criticality (calculation upon process criticality rules)
- SCS-BPs importance in the SCS (declared by SCS-BPs)
- SCS assets criticality (calculation upon asset criticality rules)
- SCS-ISMS inventory : hosting all above

CYRENE RCA Methodology

Step 1: Analysis of the SCS

❑ **Determine the SCS Scope-Objectives**
- ❖ RCA Target of Evaluation (TOE): the SCS (SCS-TOE)
- ❖ Identification of SCS main components: SCS processes, SCS Business Partners (SCS-BPs), SCS assets

❑ **Identify Business, Security and Assurance Requirements**
- ❖ Define the requirements to estimate the criticality of SCS components
- ❖ Define security objectives
- ❖ Check whether security controls meets the security objectives (review SDA)
- ❖ Specify SCS-PP requirements (to meet the prerequisites of the proposed EUSCS)

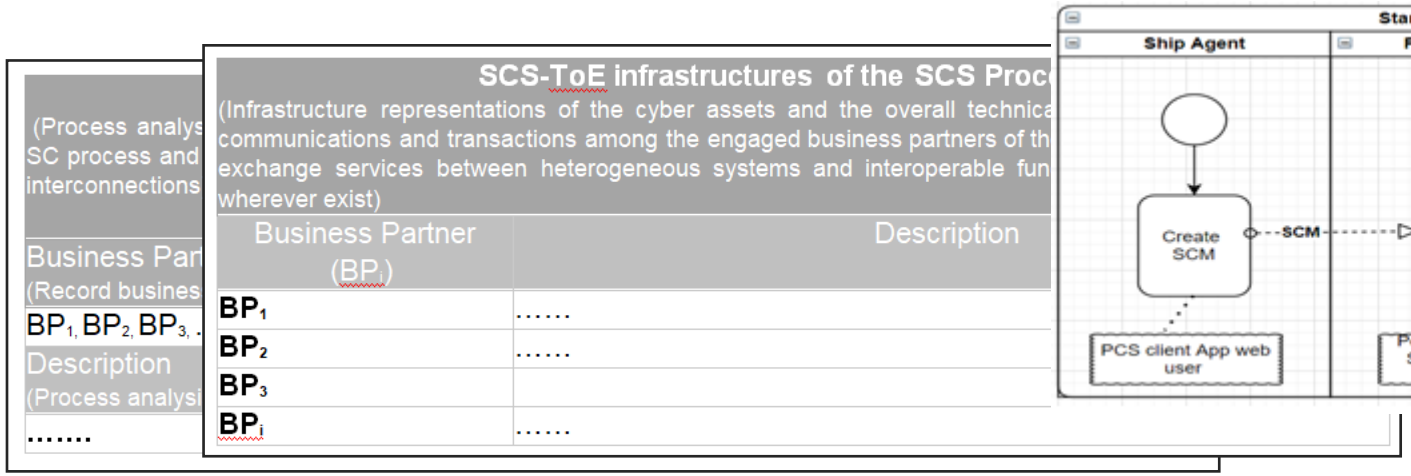
❑ **Categorize SCS-BPs**
- ❖ SCS Provider (SCS-P)
- ❖ SCS SCS-BP (e.g. Commercial, Governmental)
- ❖ SCS Self-Assessor

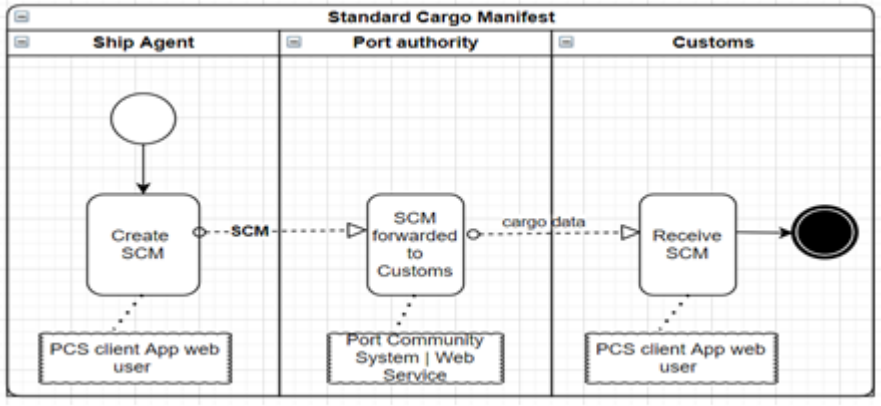
CYRENE RCA Methodology

Step 1: Analysis of the SCS

- **SCS Modelling**
  - Analysis of SCS processes and SCS-BPs (e.g. roles, interactions)
  - SCS infrastructure description (if applicable)
  - Generate business process models
  - Generate SCS asset models (e.g. define technical characteristics, interdependencies)
  - Estimate SCS components criticality

SCS components analysis templates





SCS Process Model (BPMN 2.0 Diagram)

CYRENE RCA Methodology

Step 1: Analysis of the SCS

SCS Process Criticality Rules

SCS process Criticality Rule		SCS-BP response (Yes/No)	SCS process criticality scale Very Low (VL), Low (L), Medium (M), High (H), Very High (VH)
Rule #1	The loss of, Integrity, or Availability (CIA) of the SCS process affects the provision of the SCS	Yes	VL, L
		No	M, H, VH
Rule #2	The SCS process has a backup/business continuity/disaster plan or alternative SCS process	Yes	Decreases criticality at one level (-1)
		No	Increases criticality at one level (+1)

SCS Asset Criticality Rules

SCS Asset Criticality Rule		SCS Asset criticality scale Very Low)/ Low (L)/Medium (M)/ High (H)/ Very High (VH)
Rule #1	The SCS asset inherits the SCS process criticality level it operates of the worst-case scenario.	VL / L / M / H / VH
Rule #2	The SCS asset operates to >= 50% of the total number of the SCS processes.	Increases criticality at one level (+1)
Rule #3	There is sufficient backup plan or an alternative procedure for the SCS asset operation.	Decreases criticality at one level (-1) (it cannot turn to a lower level than the SCS process criticality it operates)
	There is no sufficient backup plan/ alternative procedure for the use of the SCS asset	Increases criticality at one level (+1)
Rule #4	Asset model complexity: -Asset entries points the targeted SCS asset can be reached - Asset Length between an SCS asset entry point and the SCS asset target point	Asset model complexity: Increases criticality at one level (+1) No asset model complexity: decreases criticality at one level (+1)

CYRENE RCA Methodology

Step 2: SCS Threat Analysis

Scope

- Identification of all individual cyber threats against the SCS cyber assets
- Threat Assessment

Input

- Cyber threats frequency of appearance
  (business partners expertise, existing cyber threat repositories, crowdsourcing, social media, history of previous incidents, log files)
- List of SCS cyber assets, services, business workflows, systems & infrastructure

Outcome

- List of individual cyber threats applicable to the SCS-assets
- Set of correspondences of individual cyber threats to the SCS assets
- List of Threat Levels per asset/service/system prioritized for every identified threat

CYRENE RCA Methodology

Step 2: SCS Threat Analysis

- Identification of threats
  - threats characteristics: description, target, attack techniques, countermeasures (MITRE ATT&CK, Deep and Dark Web Mining, anomaly detection and classification algorithms)
  - individual cyber threats applicable to the SCS-assets (threat scenarios)
- Threat Assessment
  (Estimation of threat level based on expected frequency of appearance)

Estimation of Threat Level

Threat scale			Probability of Occurrence	
Threat class (Low (L), Medium (M), High (H), Very High (VH))	**Value Range (%)**	**Default Value (%)**	**History of incidents**	**Intuition & knowledge / Social Information**
VH	(80-100]	100	1 in the last year (12-month period)	VH (> 80%)
H	(60-80]	80	1 in the last year (12-month period)	H (61-80%)
M	(40-60]	60	> 1 in the last 2 years	M (41-60%)
L	(20-40]	40	<= 1 in the last 2 years	L (21-40%)
VL	[1 –20]	20	<= 1 in the last 3 years	VL (<= 20%)

CYRENE RCA Methodology

Step 3: Vulnerability & Impact Analysis

Scope

- Severity estimation of all identified vulnerabilities (CVSS v3.1)
- Calculation of vulnerability exploitability
- Propagation consideration

Input

- Implemented controls towards the existing patches (SCS-BPs collaborative assessment)
- Consideration of SCS-asset interdependency graphs & SCS assets criticality (Step 1)

Outcome

- Attack Potential score, Vulnerability Levels + Impact Levels to each SCS-cyber assets (based on CVSS v3.1 total score)
- Calculation of Vulnerability Exploitability and Attack Path Exploitability score

CYRENE RCA Methodology

Step 3: Vulnerability & Impact Analysis

- ❑ Estimation of Attack Potential (AP) (score)
- ❑ Identification of Confirmed Vulnerabilities (CVSS 3.1 specification of FIRST)
- ❑ Identification of Zero-Day Vulnerabilities (signature-based detection, SNORT framework)
- ❑ Evidence-based Vulnerability Analysis (from historical data, network data logs, host-based scans, etc.)
- ❑ Estimation of the Vulnerability Severity Level (Vulnerability
- ❑ Building Vulnerability Chains
- ❑ Attack graph generation and attack path score

Mapping Attack Portential (ISO/IEC 15408) onto CYRENE Probability Scale (Qualitative/Quantitative values)

CYRENE Probability scale						
CYRENE Qualitative value	Quantitative value		SCS-TOE is resistant to attackers with AP (ISO/IEC 15408 –CC)	SCS-TOE can be intruded with attacker's possessing AP (ISO/IEC 15408 –CC)	Vulnerability Analysis Level (AVA Class of ISO/IEC 15408 –CC)	EUSCS AL
	Range	Numeric Value				
Very Low	0.00-0.19	0,09	Basic	Enhanced-Basic, Moderate, High, Beyond High	AVA_VAN.1	Basic
Low	0.20-0.39	0,29	Basic	Enhanced-Basic, Moderate, High, Beyond High	AVA_VAN.2	Substantial
Medium	0.40-0.59	0,39	Enhanced-Basic	Moderate, High, Beyond High	AVA_VAN.3	Substantial
High	0.60-0.79	0,69	Moderate	High, Beyond High	AVA_VAN.4	High
Very High	0.80-1.00	0,90	High	Beyond High	AVA_VAN.5	High

CYRENE RCA Methodology

Step 3: Vulnerability & Impact Analysis

CVSS 3.1 Vulnerability Severity Metrics

Base Metric Group

Attack Vector (AV)

Network (N) | Adjacent (A) | Local (L) | Physical (P)

Attack Complexity (AC)

Low (L) | High (H)

Privileges Required (PR)

None (N) | Low (L) | High (H)

User Interaction (UI)

None (N) | Required (R)

Scope (S)

Unchanged (U) | Changed (C)

Confidentiality (C)

None (N) | Low (L) | High (H)

Integrity (I)

None (N) | Low (L) | High (H)

Availability (A)

None (N) | Low (L) | High (H)

Temporal Metric Group

Exploit Code Maturity (E)

Not Defined (X) | Unproven (U) | Proof-of-Concept (P) | Functional (F) | High (H)

Remediation Level (RL)

Not Defined (X) | Official Fix (O) | Temporary Fix (T) | Workaround (W) | Unavailable (U)

Report Confidence (RC)

Not Defined (X) | Unknown (U) | Reasonable (R) | Confirmed (C)

Environmental Metric Group

Confidentiality Requirement (CR)

Not Defined (X) | Low (L) | Medium (M) | High (H)

Integrity Requirement (IR)

Not Defined (X) | Low (L) | Medium (M) | High (H)

Availability Requirement (AR)

Not Defined (X) | Low (L) | Medium (M) | High (H)

Modified Attack Vector (MAV)

Not Defined (X) | Network | Adjacent Network | Local | Physical

Modified Attack Complexity (MAC)

Not Defined (X) | Low | High

Modified Privileges Required (MPR)

Not Defined (X) | None | Low | High

Modified User Interaction (MUI)

Not Defined (X) | None | Required

Modified Scope (MS)

Not Defined (X) | Unchanged | Changed

Modified Confidentiality (MC)

Not Defined (X) | None | Low | High

Modified Integrity (MI)

Not Defined (X) | None | Low | High

Modified Availability (MA)

Not Defined (X) | None | Low | High

CYRENE RCA Methodology

Step 3: Vulnerability & Impact Analysis

Vulnerability Severity Level (VSL) Estimation

CVSS 3.1 total score with CYRENE considerations

Base Metric Group

Attack Vector (AV)

Network (N) | Adjacent (A) | Local (L) | Physical (P)

Attack Complexity (AC)

Low (L) | High (H)

Privileges Required (PR)

None (N) | Low (L) | High (H)

User Interaction (UI)

None (N) | Required (R)

Scope (S)

Unchanged (U) | Changed (C)

Confidentiality (C)

None (N) | Low (L) | High (H)

Integrity (I)

None (N) | Low (L) | High (H)

Availability (A)

None (N) | Low (L) | High (H)

Constant vulnerability characteristics over time and across the SCS environment (CVE MITRE)

Temporal Metric Group

Exploit Code Maturity (E)

Not Defined (X) | Unproven (U) | Proof-of-Concept (P) | Functional (F) | High (H)

Remediation Level (RL)

Not Defined (X) | Official Fix (O) | Temporary Fix (T) | Workaround (W) | Unavailable (U)

Report Confidence (RC)

Not Defined (X) | Unknown (U) | Reasonable (R) | Confirmed (C)

Vulnerability characteristics changing over time (filled by SCS-BPs consulting the implemented controls from the SCS-ISMS

Environmental Metric Group

CVSS 3.1 Metric Name	CVSS 3.1 Possible Values of vulnerabilities (on assets of a SCS network)	Remarks
Modified Attack Vector (AV)	Filled by SCS-BP	Security control strength, asset model complexity
Modified Attack Complexity (MAC)	Filled by SCS-BP	Security control strength, asset model complexity
Modified Privileges Required (MPR)	Not Defined	Based on Attack Potential
Modified User Interaction (MUI)	Not Defined	Based on Attack Potential
Modified Scope (MS)	Changed	An attack on SCS asset affects its interconnected SCS assets

Vulnerability characteristics impacted by the SCS environment

CVSS 3.1 Metric Name	CVSS 3.1 Possible values of vulnerabilities (on assets of a SCS network) **CR/IR/AR:** Not Defined, Low, Medium, High **MC/MI/MA:** Not Defined, None, Low, High	Possible values of SCS Asset Criticalilty [Very Low, Low Medium, High, Very High]
Confidentiality Requirement (CR)	Low	Very Low
	Low	Low
	Medium	Medium
	High	High
	High	Very High
Integrity Requirement (IR)	Low	Very Low
	Low	Low
	Medium	Medium
	High	High
	High	Very High
Availability Requirement (AR)	Low	Very Low
	Low	Low
	Medium	Medium
	High	High
	High	Very High
Modified Confidentiality (MC)	None	Very Low
	None	Low
	Low	Medium
	High	High
	High	Very High
Modified Integrity (MI)	None	Very Low
	None	Low
	Low	Medium
	High	High
	High	Very High
Modified Availability (MA)	None	Very Low
	None	Low
	Low	Medium
	High	High
	High	Very High

CYRENE RCA Methodology

Step 3: Vulnerability & Impact Analysis

Vulnerability Exploitability Estimation, Asset graphs and Vulnerability Chains

CYRENE Vulnerability Exploitability Calculation

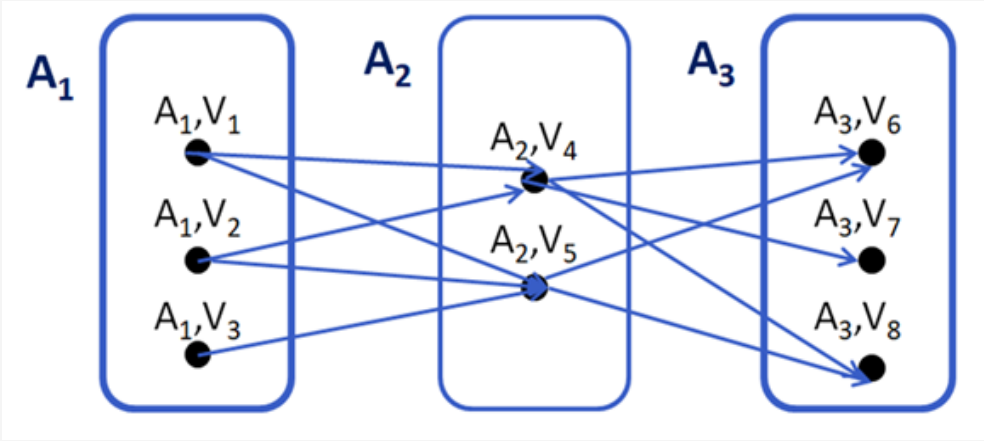
Individual Vulnerability Modified Exploitability (IVME):
The *vulnerability exploitability upon a specific SCS asset*

IVME = MESS x AP

IVME = (8.22 x ModifiedAttackVector x ModifiedAttackComplexity x ModifiedPrivilegesRequired x ModifiedUserInteraction**) x AP**

- **MESS:** Modified Exploitability sub score (MESS) of CVSS 3.1 https://www.first.org/cvss/specification-document
- **AP:** Attack Potential

Asset/Vulnerability Combinations



Vulnerability Chains

$V_1 \rightarrow V_4 \rightarrow V_6$ $V_2 \rightarrow V_5 \rightarrow V_6$ $V_3 \rightarrow V_4 \rightarrow V_6$
$V_1 \rightarrow V_4 \rightarrow V_7$ $V_2 \rightarrow V_5 \rightarrow V_7$ $V_3 \rightarrow V_5 \rightarrow V_7$
$V_1 \rightarrow V_4 \rightarrow V_8$ $V_2 \rightarrow V_5 \rightarrow V_8$ $V_3 \rightarrow V_4 \rightarrow V_8$

CYRENE RCA Methodology

Step 3: Vulnerability & Impact Analysis

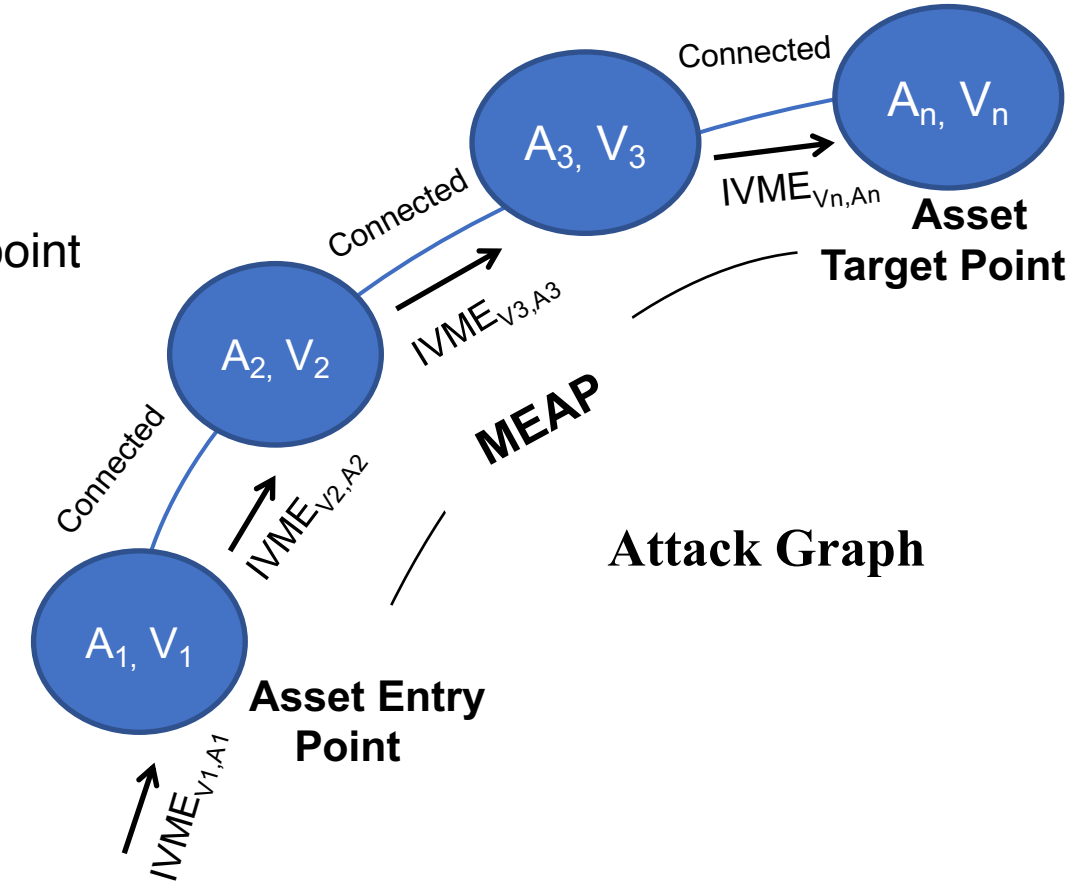
Attack Paths Exploitability estimation and Attack Graphs

CYRENE Attack Path Exploitability

Modified Exploitability Attack Path (MEAP):
The Attack Path Exploitability of specific asset/vulnerability combinations between an asset entry point and an asset target point

$$\mathbf{MEAP = IVME_{V1,A1} \times IVME_{V2,A2} \times IVME_{V3,A3} \times \ldots \times IVME_{Vn,An}}$$

- **IVME:** Individual Vulnerability Modified Exploitability



CYRENE RCA Methodology

Step 4: Risk Assessment

Scope

- Risk estimation of each SCS asset
- Risk estimation of the attack path

Input

- Threat Level (Step 2)
- Vulnerability Severity Level (VSL) (Step 3)
- Attack Potential (AP) (Step 3)

Outcome

- SCS asset Risk Level for a specific threat on specific SCS asset
- Risk Level of attack path (considering the propagation rates & attack paths)

CYRENE RCA Methodology

Step 4: Risk Assessment

Risk Level estimation

❑ **CYRENE Individual Risk Level $R_{sj,Ai,j}$** : how dangerous a threat, s_j, is to the specific asset $A_{i,j}$ within the SCS

$$R_{sj,Ai,j} = TL_{sj,Ai,j} \times VL_{v,Ai,j} \times I_{v,Ai,j} \text{ x AP} = TL_{s,Ai,j} \times VSL_{v,Ai,j} \text{ x AP}$$

❖ **Threat Level ($TL_{sj,Ai,j}$):** derived from the Threat Assessment

❖ **Vulnerability Severity Level ($VSL_{v,Ai,j}$) = Vulnerability Level ($VL_{v,Ai,j}$)+ Impact Level ($I_{v,Ai,j}$):** estimated during Vulnerability and Impact Analysis (based on CVSS 3.1)

❖ **Attack Potential (AP):** defined during the Vulnerability and Impact Analysis according to the SCS criticality and the adopted EUSCS Assurance Level (AL) (CYRENE probability scale).

❖ Risk Levels, Threat Levels and Vulnerability Levels **qualitative values can be converted into quantitative values** and opposingly according to the CYRENE probability scale

CYRENE Probability scale

CYRENE Qualitative value	Quantitative value		SCS-TOE is resistant to attackers with AP (ISO/IEC 15408 –CC)	SCS-TOE can be intruded with attacker's possessing AP (ISO/IEC 15408 –CC)	Vulnerability Analysis Level (AVA Class of ISO/IEC 15408 –CC)	EUSCS AL
	Range	Numeric Value				
Very Low	0.00-0.19	0,09	Basic	Enhanced-Basic, Moderate, High, Beyond High	AVA_VAN.1	Basic
Low	0.20-0.39	0,29	Basic	Enhanced-Basic, Moderate, High, Beyond High	AVA_VAN.2	Substantial
Medium	0.40-0.59	0,39	Enhanced-Basic	Moderate, High, Beyond High	AVA_VAN.3	Substantial
High	0.60-0.79	0,69	Moderate	High, Beyond High	AVA_VAN.4	High
Very High	0.80-1.00	0,90	High	Beyond High	AVA_VAN.5	High

CYRENE RCA Methodology

Step 4: Risk Assessment

Risk of Attack Path

- For **EUSCS AL = "High", risk propagation** should be estimated
- The risk of **implementing an Attack Path $R_{Attack\ Path}$ is calculated from the multiplication of the individual Risks $R_{sj,Ai,j}$ of all asset nodes Ai,j** from an **Asset Entry point** to an **Asset Target Point**

$$R_{AttackPath} = R_{node1} \times R_{node2} \times R_{node3} \times \ldots \times R_{nodeN}$$

- **R_{nodeN}:** Individual risk **$R_{sj,Ai,j}$**
- **$R_{Attack\ Path}$: multiplication of the individual Risks $R_{sj,Ai,j}$ of all asset nodes Ai,j** from an **Asset Entry point** to an **Asset Target Point**
- Risk Levels, **qualitative values can be converted into quantitative values** and inversely by utilizing the CYRENE probability scale

CYRENE RCA Methodology

Step 5: Risk Compliance to Security Assurance Certification Scheme

Scope

- Alignment of mitigation measures: explore various options for mitigation actions that can be selected. Provide a cost-benefit analysis to decide what is the best choice based on their agreement (performed by the SCS-P & SCS-BPs)
- Assess the risk levels estimates of Step 4 against security requirements of the SCS-PP submitted (performed by the auditor in case of conformity assessment)

Input

- SCS SDA
- List of risk estimates
- SCS-ISMS
- SCS-PP

Outcome

- Cost-Benefit Analysis towards the entire Supply Chain Service
- List of all the CYRENE measures focusing on risk compliance aligned with the security requirements

CYRENE RCA Methodology

Step 6: Risk Mitigation: Security Countermeasures Identification

Scope

- In case risk levels are **above** a required threshold, additional security controls are determined by the SCS-BPs for the SCS to meet thresholds
  (consult cost-Benefit Analysis + implement/ test selected mitigation actions to identify the optimal set of security controls)
- Develop security reports for the SCS (performed by the SCS-P & SCS-BPs)
- Assess the implemented mitigation actions against their strength in treating the risks to meet the security requirements of the SCS-PP (performed by the auditor)

Input

- Potential attack strategies (attack paths scores)
- Available security measures
- Cost-Benefit Analysis towards the entire SCS

Outcome

- Optimal security strategy (set of security controls) to be applied by all SCS-BPs
- SCS security reports (e.g. security policy, Disaster Recovery Plan, Business Continuity Plan)
- Auditor's report on the assessment

Thank you!

Eleni-Maria Kalogeraki

elma.kalogeraki@maggioli.gr