SESAR Security Risk Assessment Tutorial

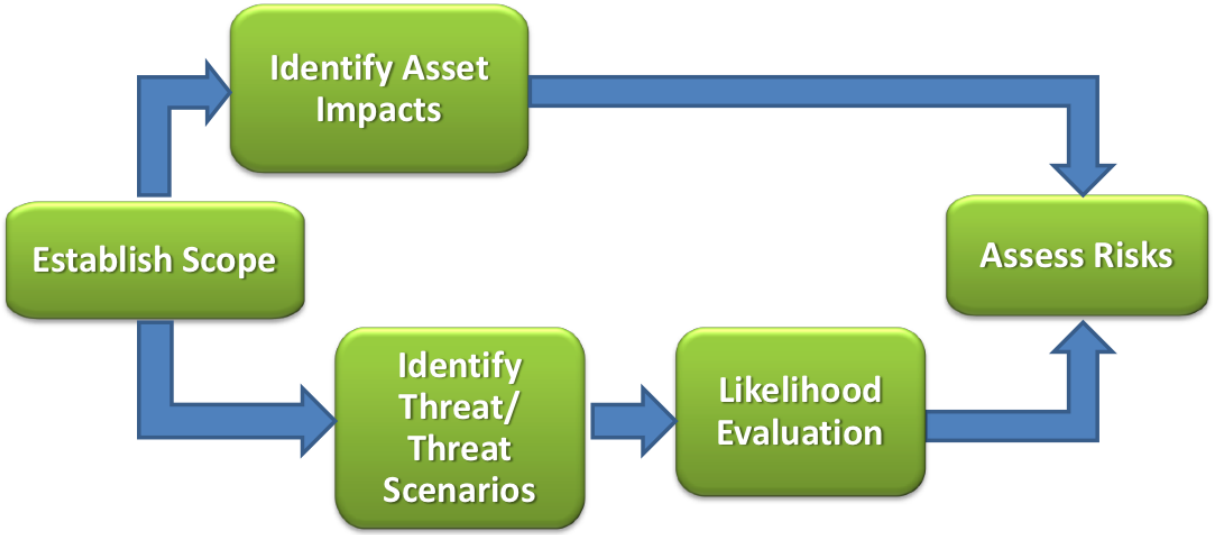
Federica Paci
University of Trento

Outline

- What is Security Risk Assessment?
- SESAR SecRAM
  - Definitions
  - Primary Assets Identification and Impact Assessment
  - Supporting Assets Identification and Valuation
  - Threat Scenarios
  - Risk Evaluation
  - Risk Treatment

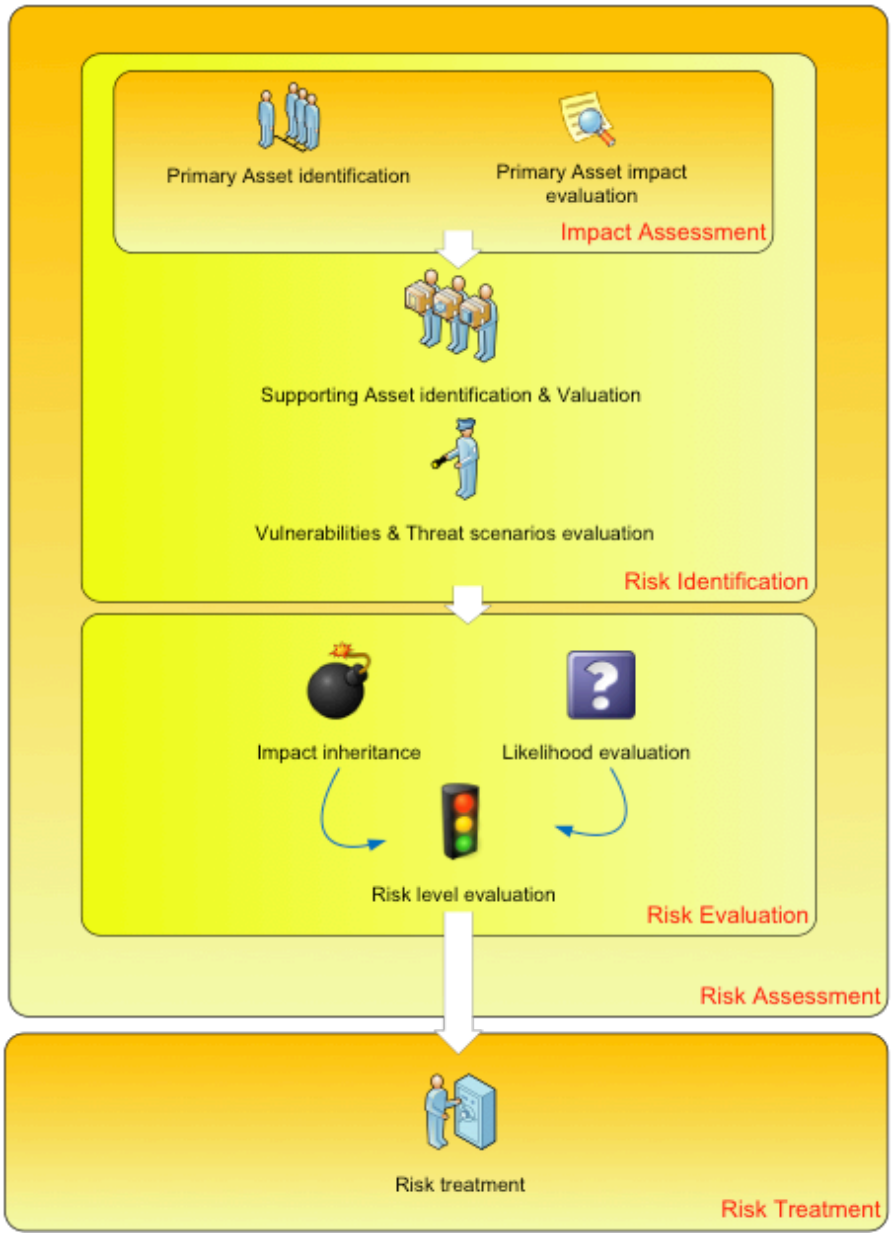
What is Security Risk Assessment?

- Systematic process for the identification and quantification of the severity of risks of a system



SESAR SecRAM

- Build security into system development lifecycle
- Easy to use for no security experts
- Compliant with ISO 27005
- Focuses on two types of assets
  - Primary Assets
  - Supporting Assets



Definitions

- **Primary Asset**
  - Intangible entities like information or service that is part of the system under analysis and has value to the system
- **Supporting Asset**
  - Tangible entities which enable the primary assets
  - They possess the vulnerabilities that are exploitable by threats aiming to impair primary assets

Definitions

- **Threat Source**
  - The potential cause of an unwanted incident which may result in an impact on the operations
- **Threat**
  - Potentially harmful event initiated by a threat source exploiting vulnerabilities of a supporting asset

Definitions

- **CIA**
  - **Confidentiality.** The property that information is not made available or disclosed to unauthorized individuals, entities or processes
  - **Integrity.** The property of safeguarding the accuracy and completeness of assets
  - **Availability.** The property of being accessible and usable upon demand by unauthorized entity

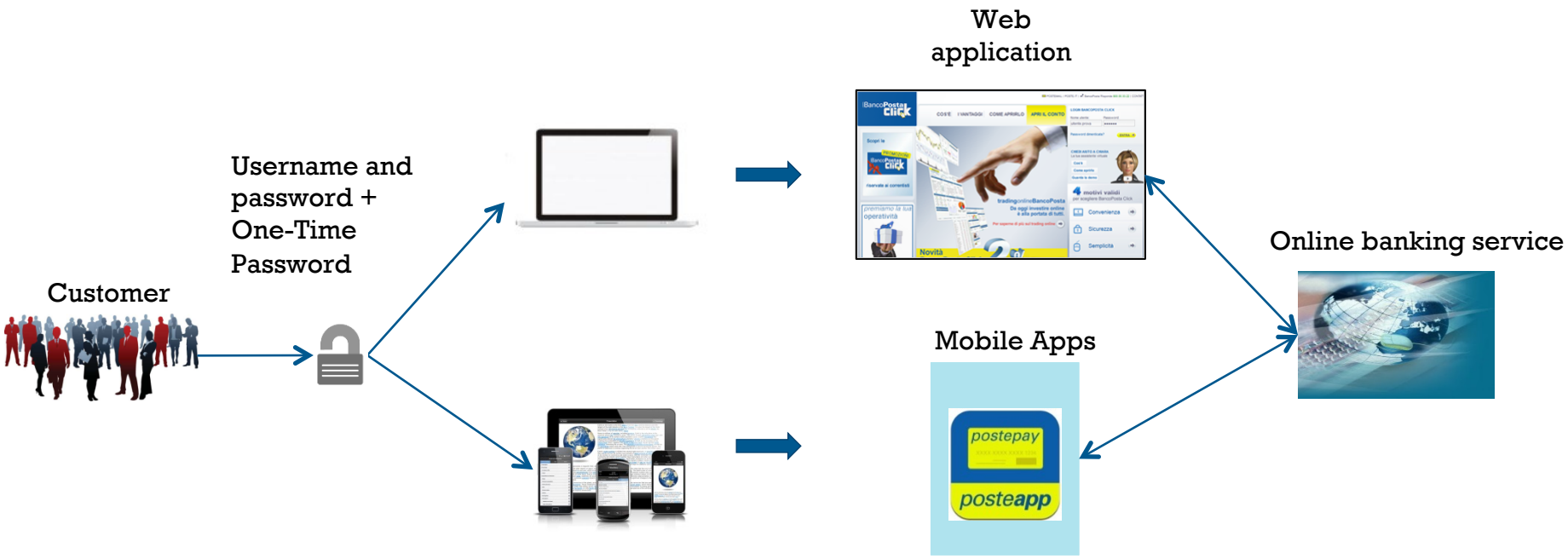
Definitions

- **Impact**
  - The effect of compromising confidentiality, availability or integrity of a primary asset
- **Likelihood**
  - Evaluation of the chance of a threat scenario successfully occurring
- **Risk**
  - The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby have an impact on the identified asset**s**

Definitions

- **Risk Treatment**
  - The process of selecting and implementing measures to modify risk
- **Control**
  - Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be administrative, technical, management or legal in nature

Application Scenario



Primary Assets and Impacts

Primary Asset Identification

- Services
- Information

Primary Asset ID	**Primary Asset**	**Type**
PA_1	Credit Card Number	Information
PA_2	Customer Address	Information
PA_3	One-Time Password	Information

Impact

	5	4	3	2	1
Impacted Areas	Catastrophic	Critical	Severe	Minor	No Impact
IA1: PERSONNEL	Fatalities	Multiple Severe injuries	Severe injuries	Minor injuries	No injuries
IA2: CAPACITY	Loss of 60%-100% capacity	Loss of 60%-30% capacity	Loss of 30%-10% capacity	Loss of up to 10% capacity	No capacity loss
IA3: PERFORMANCE	Major quality abuse that makes multiple major systems inoperable	Major quality abuse that makes major system inoperable	Severe quality abuse that makes systems partially inoperable	Minor system quality abuse	No quality abuse
IA4: ECONOMIC	Bankruptcy or loss of all income	Serious loss of income	Large loss of income	Minor loss of income	No effect
IA5: BRANDING	Government & international attention	National attention	Complaints and local attention	Minor complaints	No impact
IA6:REGULATORY	Multiple major regulatory infractions	Major regulatory infraction	Multiple minor regulatory infractions	Minor regulatory infraction	No impact
IA7: ENVIRONMENT	Widespread or catastrophic impact on environment	Severe pollution with long term impact on environment	Severe pollution with noticeable impact on environment	Short Term impact on environment	Insignificant

Impact Assessment

Maximum impact of all impacted areas

Primary Asset	CIA	Personnel	Capacity	Performance	Economic	Branding	Regulatory	Environment	Overall Impact
One-Time Password	C				5	3	4		5
	I						4		4
	A								

Supporting Assets Identification and Valuation

Supporting Assets

- They possess the vulnerabilities that are exploitable by threats
- Examples
  - Hardware
  - Software
  - Operating Systems
  - Storage Media
  - Personnel….
- Supporting assets must be linked to primary assets

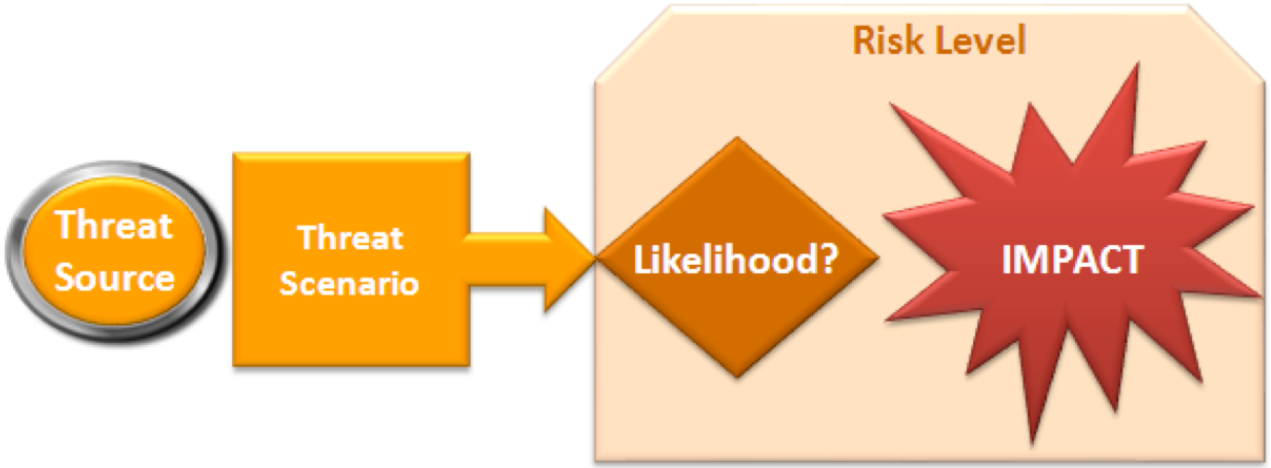
Supporting Assets Table

Supporting Asset	One-Time Password	……	…….
Mobile Device			
One-Time Password Device			

Threat Scenarios

Threat scenarios

- Threat × Supporting Asset → Impact on Primary Asset



Threat scenario steps

- For each supporting asset
  1. Identify relevant threats (threat catalogue)
  2. Identify which criteria are targeted by the threat (confidentiality, integrity, availability)
  3. Build a table
     a) Linking threats to supporting assets
     b) Impacts on primary asset CIA

The threat scenario table

Supporting Assets	**Threats**	**Primary Assets**		
		One-Time Password		
		C	I	A
Mobile Device	Theft	5		
	Malicious Code	5	4	

Same as Overall Impact

Risk Evaluation

Impact Evaluation

- **Inherited Impact**
  - Maximum impact of all CIA criteria among all the primary assets (via supporting assets) targeted by the threat

- **Reviewed Impact**
  - Usually equal or lower than Inherited Impact

The impact Evaluation table

Maximum impact of all CIA

Supporting Assets	**Threats**	**Primary Assets**			**Inherited Impact**	**Reviewed Impact**
		One-Time Password				
		C	I	A		
Mobile Device	Theft	5			5	5
	Malicious Code	5	4		5	5

Likelihood Evaluation

Likelihood	Qualitative Interpretation
5. Certain	There is a high chance that the scenario successfully occurs in a short time
4. Very likely	There is a high chance that the scenario successfully occurs in the medium term
3. Likely	There is a high chance that the scenario successfully occurs during the life time of the project
2. Unlikely	There is a low chance that the scenario successfully occurs during the life time of the project
1. Very Unlikely	There is little or no chance that the scenario successfully occurs in a short time

Risk Assessment

	Mitigated Impact				
Likelihood	1	2	3	4	5
5. Certain	Low	High	High	High	High
4. Very likely	Low	Medium	High	High	High
3. Likely	Low	Low	Medium	High	High
2. Unlikely	Low	Low	Low	Medium	High
1. Very Unlikely	Low	Low	Low	Medium	Medium

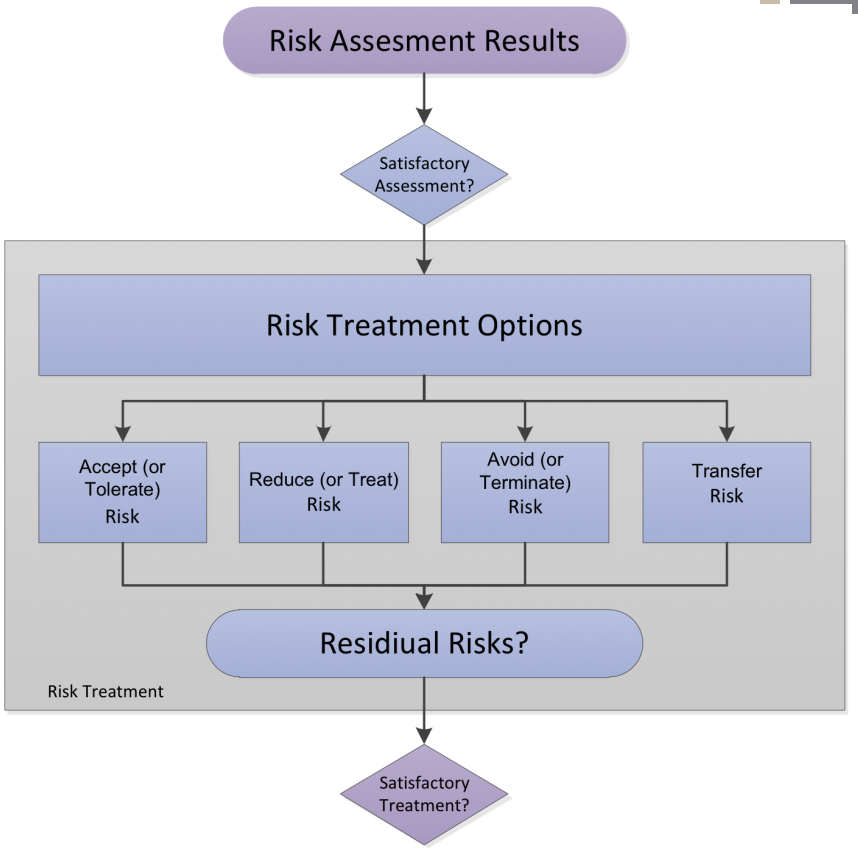
The risk assessment table

Supporting Assets	**Threats**	**Reviewed Impact**	**Likelihood**	**Risk Level**
Mobile Device	Theft	5	Likely	High
	Malicious Code	5	Very Likely	High

Risk Treatment

Risk Treatment

- Four options for risk treatment
  - **Accept or Tolerate** (no action needed)
  - **Reduce or Treat** (through controls)
  - **Avoid or Terminate** (change or stop the activity)
  - **Transfer** (to another party)



Controls

- For each threat scenario select controls from the catalogue
- Two types of controls
  - Pre Event Controls
    - They avoid that threats occur
  - Post Event Controls
    - They correct or remediate threats that have already occurred

The risk treatment table

Supporting Assets	Threats	Reviewed Impact	Likelihood	Risk Level	Controls
Mobile Device	Theft	5	Likely	High	Security Training
	Malicious Code	5	Very Likely	High	Virus Protection

Registration

- Choose a partner to work with for the assignments
- Go to https://docs.google.com/forms/d/1n4OZiOziiABww-XXvmOP2_wSsTtbZloARvDzZ50XuSQ/viewform
  - Your name, last name, email and student ID
  - The name, last name, email and student ID of your partner