
The slide features a large orange square on the left with a white plus sign in the top-left corner. To its right is the EMFASE logo, which consists of three overlapping squares (blue, red, green) and the text 'EMFASE'. Further right is a solid green square. Below the EMFASE logo is a blue square. To the right of the blue square is a Venn diagram with three overlapping circles labeled 'Threat', 'Asset', and 'Vulnerability'. The intersection of all three circles is shaded red and labeled 'Risk'. A hand is shown pointing to the 'Risk' label. Below the Venn diagram is the SESAR logo, which includes the text 'SESAR' and 'JOINT UNDERTAKING' with several yellow stars. At the bottom center, there is a small yellow circle with 'PT' inside, and the text 'Thanks to' and 'for the provision of the Scenario' on either side.

**Tutorial on Modeling Security Risk  
with Graphs**

Thanks to  for the provision of the Scenario

This tutorial is on modeling security risks using graphs. It is targeted to security professionals as well as anyone is interested in knowing more about security risk modeling.

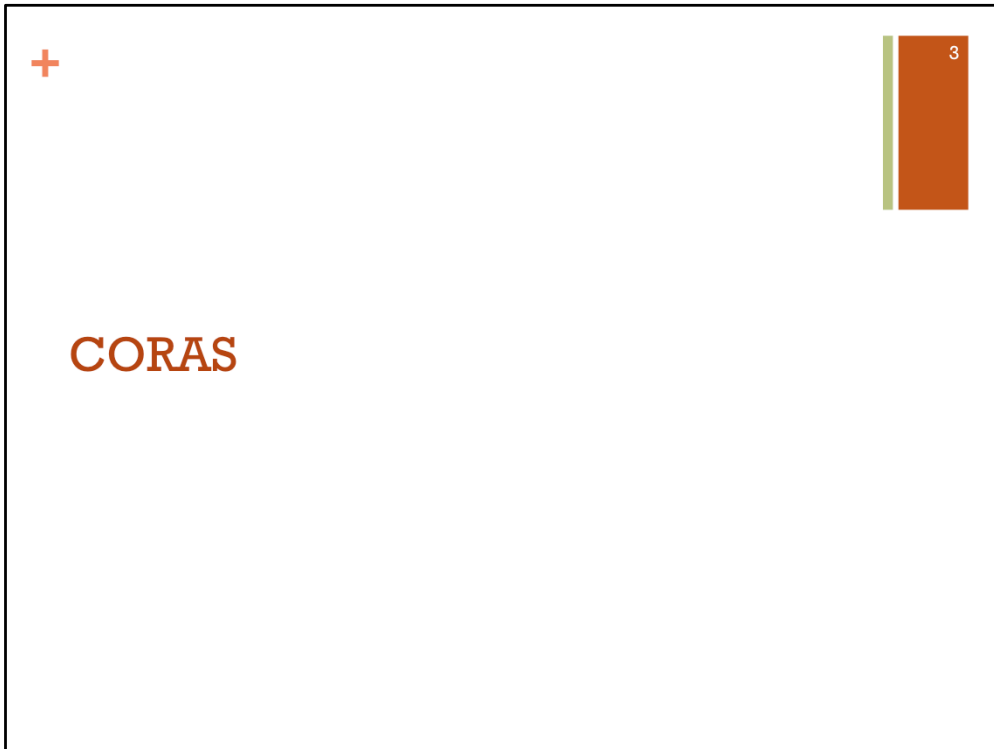
## + About This Tutorial

2

- In this tutorial you will
  - learn about graphical notations for modeling security risks
  - get familiar with the Poste Italiane home banking scenario
- We will introduce you to
  - CORAS Graphical Risk Modeling Notation
  - Scales to quantify security risks
  - The scenario under analysis

This tutorial will give you the basics to model security risks using graphs. We will first introduce you to the CORAS graphical approach to identify, communicate and document security risks.

We will also explain you how to evaluate security risks. And at the end we will present an home banking scenario that you will analyze during the experiment.



Now let's introduce the CORAS' main concepts

## + CORAS Elements





4



CORAS is a method for conducting security risk analysis developed by SINTEF. CORAS provides a graphical language for threats and risk modeling. The language provides a graphical symbol for all the standard concepts.

## + CORAS terms

5

Term	Definition	Icon
Threat	A potential cause of an unwanted incident	
Vulnerability	A weakness, flaw or deficiency that opens for, or may be exploited by a threat to cause harm to or reduce the value of an asset	
Threat scenario	A chain or series of events that is initiated by a threat and that may lead to an unwanted incident	
Unwanted incident	An event that harms or reduces the value of an asset	



These are first four main concepts of the CORAS risk modeling language.

On the left of the table there is the term used for the concept, at the center you can read its definition and finally on the right you can find its representation.

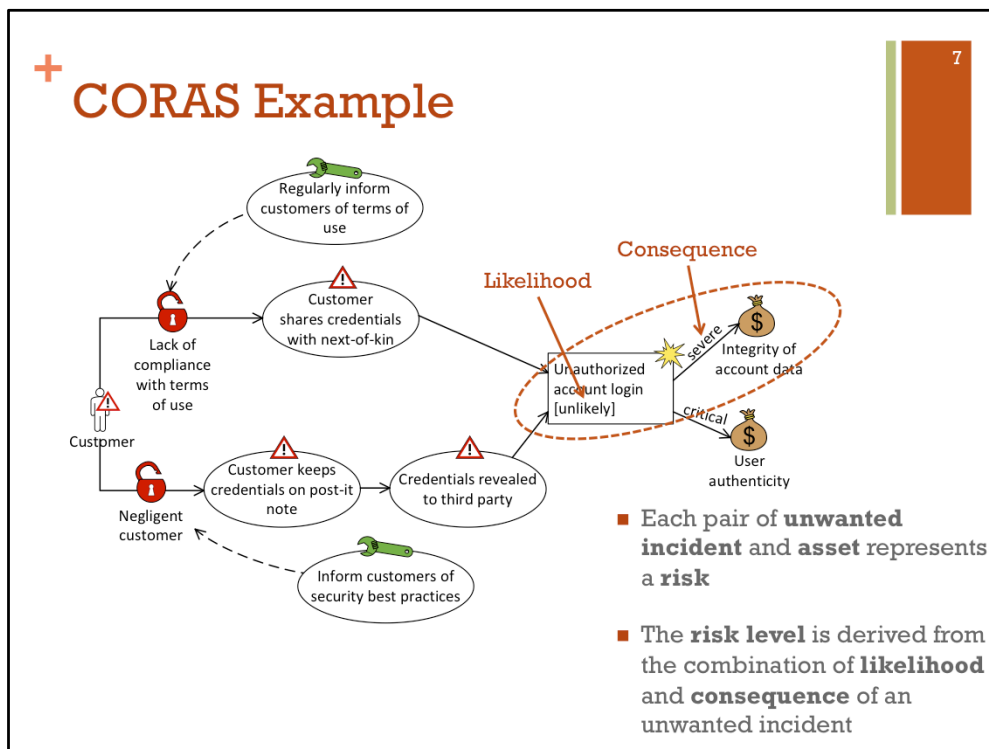
Special attention in this notes is given to Threats as they have multiple representations in the CORAS model. A threat is an initiator of events that may harm the system we are analyzing. A threat can be a human with a malicious intent (devil's icon of threat) or human that accidentally harms the systems (centered icon) under analysis. But a threat can also be an event outside control like a natural disaster or a failure (white flag icon).

## + CORAS terms

6

Term	Definition	Icon
Asset	Something to which a party assigns value and hence for which the party requires protection	
Treatment	An appropriate measure to reduce risk level	
Likelihood	The frequency or probability for something to occur	
Consequence	The impact of an unwanted incident on an asset in terms of harm to or reduced asset value	

These are other four main concepts of the CORAS risk modelling language.



Now let's give a look to a CORAS risk model.

The threat customer initiates two different attack scenarios:

Scenario 1. The customer exploits vulnerability "Lack of compliance with terms of use" to initiate the threat scenario "Customer shares credentials with next-of-kin"

Scenario 2. The customer exploits vulnerability "Negligent customer" to initiate the threat scenario "Customer keeps credentials on post-it note" which leads to the threat scenario "Credential revealed to third party".

Both scenarios lead to the unwanted incident "Unauthorized account login" which impacts the assets "Integrity of account data" and "User authenticity".

The risk of the unwanted incident "Unauthorized account login" is given by the likelihood that it occurs and the impact that it has on the assets Integrity of account data and User authenticity.

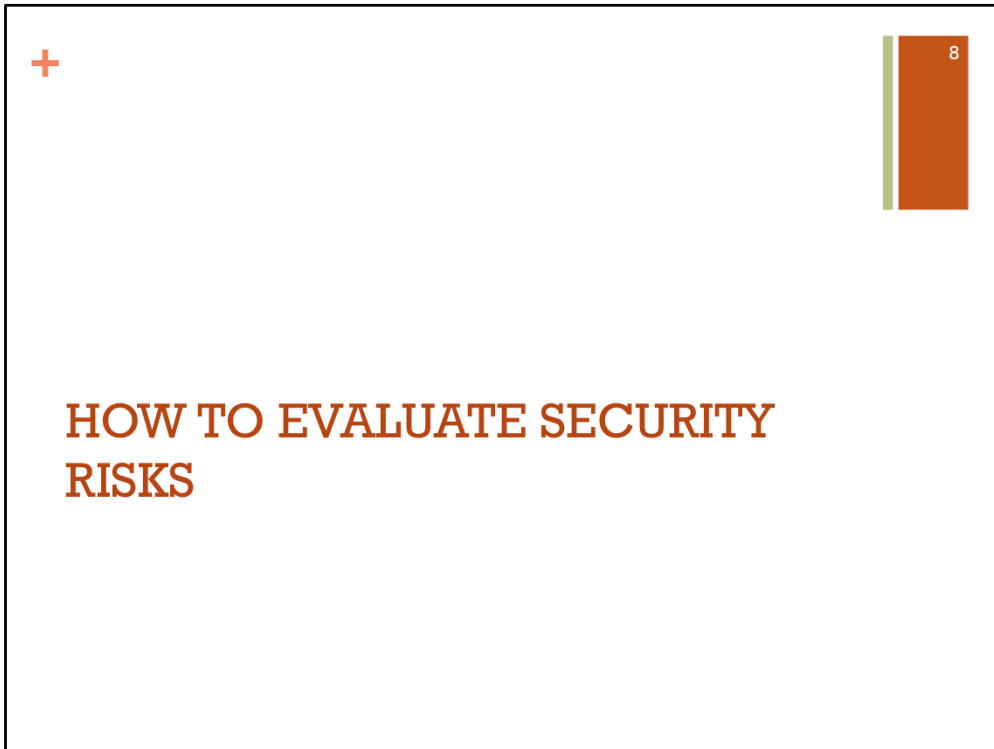
The likelihood of the unwanted incident "Unauthorized account login" is a label on the unwanted incident.

The consequence is specified on the arrow that links the unwanted incident to the assets.

To reduce this risk we need to mitigate the two threat scenarios.

The first threat scenario "Customer shares credentials with the next-of-kin" is mitigated by the treatment "Regularly inform customers of terms of use"

The second threat scenario is mitigated by the treatment "Inform customers of security best practices".



The next section is dedicated to the evaluation of the security risks.



## + Risk Evaluation

9

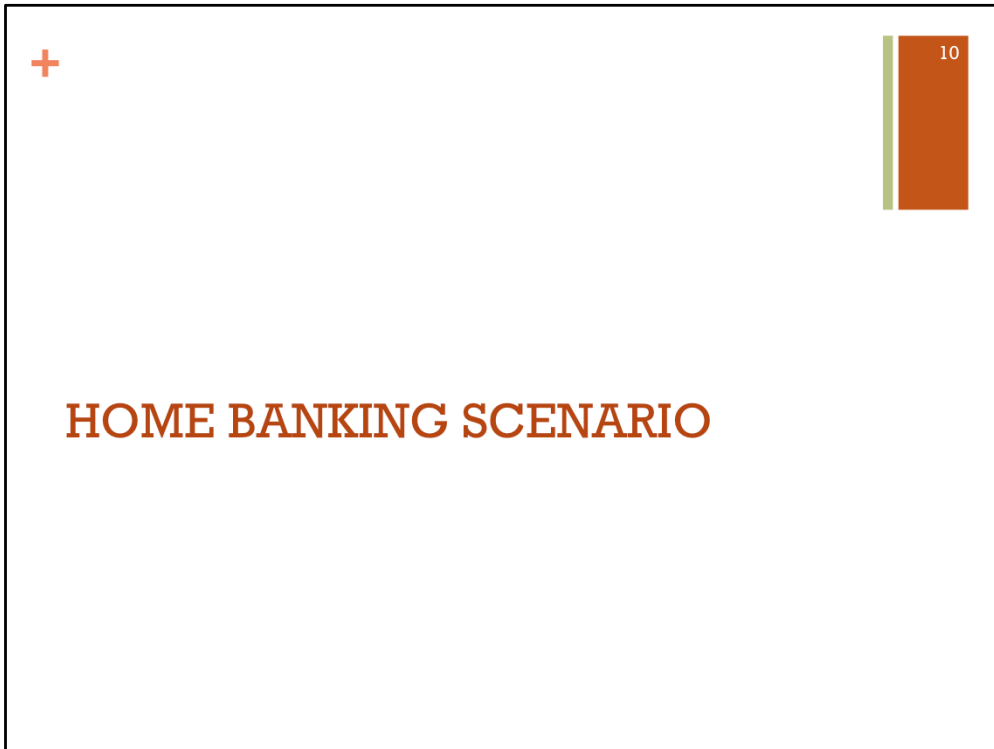
		Consequence/Impact				
		Insignificant	Minor	Severe	Critical	Catastrophic
Likelihood	Certain	Yellow	Red	Red	Red	Red
	Very likely	Green	Yellow	Red	Red	Red
	Likely	Green	Green	Yellow	Red	Red
	Unlikely	Green	Green	Green	Yellow	Red
	Very unlikely	Green	Green	Green	Green	Yellow

Risk value of an unwanted incident of a threat scenario is computed based on a risk evaluation matrix.

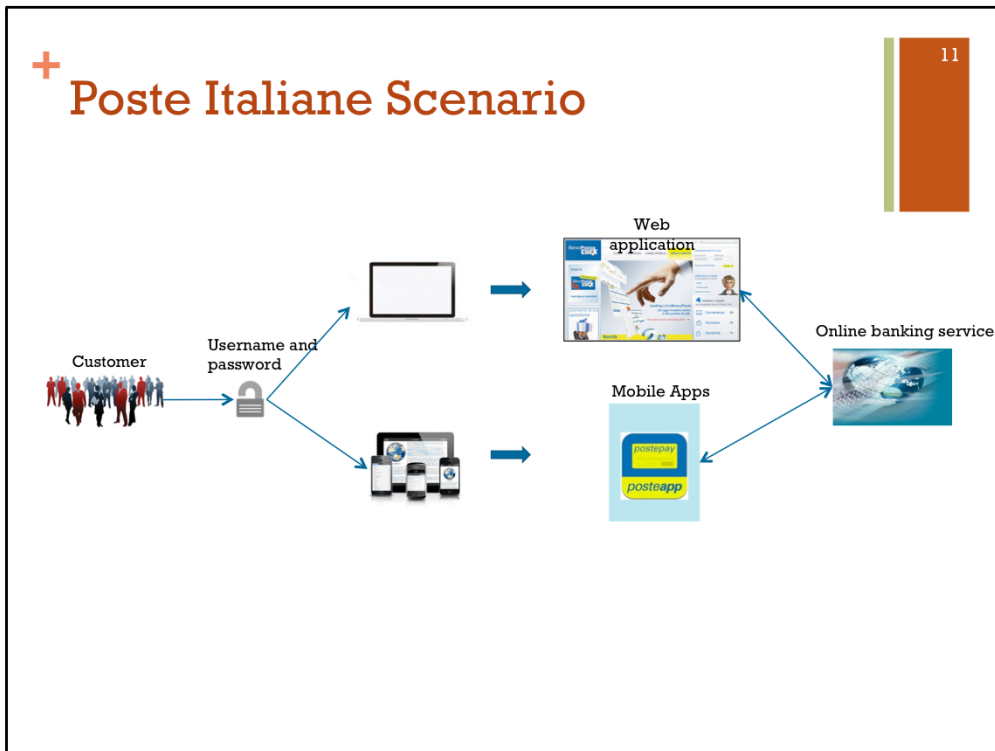
The matrix has on the rows the possible values that the likelihood can assume, and as columns the possible values that the consequence of impact can assume.

The entries of the map represent risk values:

- Risk values represented in green are risks that can be accepted
- Entries denoted in orange are risks that need to be monitored
- Red entries are risks that need to be treated. So a possible counter measure or treatment needs to be identified and implemented



The next section is dedicated to the presentation of the home banking scenario. This is the scenario that will be used in the experiment.



The home banking scenario focuses on the online banking services provided by Poste Italiane to their customers.

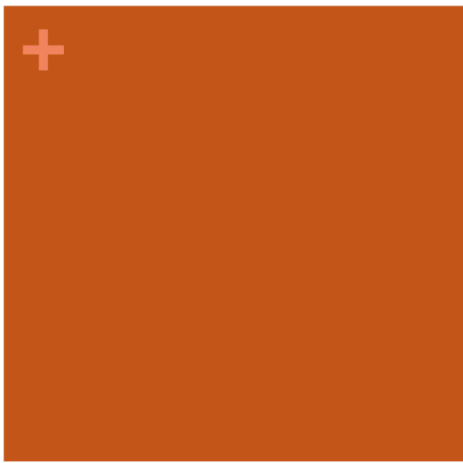
Customers can access their bank account information through the Poste Italiane application or through the Poste Italiane mobile application. Customers can perform operations like checking their mobile balance, checking their credit cards or topping up their mobile phone.

## + Poste Italiane Assets

12

- The Poste Italiane risk assessment is done with respect to the following assets
  - **Integrity of account data**  
Includes personal information, as well as the bank account balance
  - **User authenticity**  
This means that the person that is logged in as a user is identical to the user
  - **Confidentiality of customer data**  
Includes personal information, as well as information about savings, loans, account balance, etc.
  - **Availability of service**  
The online banking services shall be available to the customers 24/7

These are the Poste Italiane assets that are used for the risk assessment.



**Thank you for your attention**

Thanks to  for the provision of the Scenario