

The slide features a large orange square on the left with a white plus sign in the top-left corner. To its right are three smaller squares: a light blue one with the EMFASE logo (a cluster of colored squares), a green one, and a blue one. Further right is a Venn diagram with three overlapping circles labeled 'Threat', 'Asset', and 'Vulnerability'. The intersection of all three is shaded red and labeled 'Risk'. A hand is shown pointing to this intersection. Below the main content is the title 'Tutorial on Modeling Security Risk with Tables' in bold brown text. At the bottom center, it says 'Thanks to  for the provision of the Scenario'. The SESAR logo is in the bottom right corner.

**Tutorial on Modeling Security Risk with Tables**

Thanks to  for the provision of the Scenario

EMFASE

Threat Asset Vulnerability Risk

SESAR  
JOINT UNDERTAKING

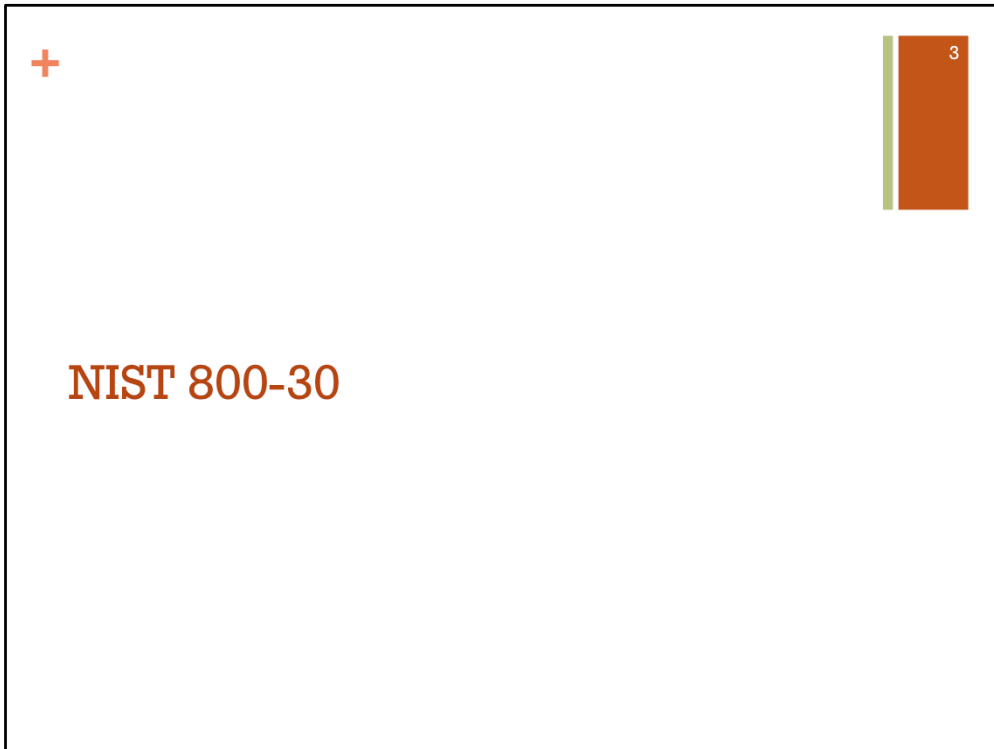
This tutorial is on modeling security risks using tables. It is targeted to security professionals as well as anyone is interested in knowing more about security risk modeling.

## + About This Tutorial

2

- In this tutorial you will
  - learn about tabular notation for modeling security risks
  - get familiar with the Poste Italiane home banking scenario
- We will introduce you to
  - NIST 800-30 Tabular Risk Modeling Notation
  - Scales to quantify security risks
  - The scenario under analysis

This tutorial will give you the basics to model security risks using tables. We will first introduce you to the NIST 800-30 tabular risk modeling 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 see how security risks can be represented using the tabular approach supported by the NIST 800-30 standard for security risk assessment.

## + NIST 800-30 Terms

4

<b>Term</b>	<b>Definition</b>
Threat source	The adversarial, accidental, structural or environmental exploitation of a vulnerability
Threat event	An event (or scenario) or situation that has the potential for causing undesirable consequences or impact
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source
Impact	A harmful event that may occur given the potential for threats exploiting vulnerabilities
Asset	Operations, individuals, physical or non-physical entities that can be harmed due to a threat event and its impact

The NIST standard uses 8 main concepts to denote security risk. Here you can see the first five concepts. The other three are in the next slide.

## + NIST 800-30 Terms

5

<b>Term</b>	<b>Definition</b>
Security control	Safeguards or countermeasures to protect the confidentiality, integrity and availability of a system and its information
Overall likelihood	The likelihood that a threat event results in adverse impact
Level of impact	The degree of impact in terms of harm to assets

These are the other three main concepts that NIST standard uses to denote security risk.

## + NIST Example

6

Threat event	Threat source	Vulnerability	Impact	Asset	Overall likelihood	Level of impact	Security control
Customer share credentials with next-of-kin	Customer	Lack of compliance with terms of use	Unauthorized Account Login	Integrity of account da	Unlikely	Critical	Regularly Inform customers of terms of use
Customer share credentials with next-of-kin	Customer	Lack of compliance with terms of use	Unauthorized Account Login	User Authenticity	Unlikely	Critical	Regularly Inform customers of terms of use
Customer keeps credentials on post-it notes which leads to credential being revealed to third party	Customer	Negligent Customer	Unauthorized Account Login	Integrity of account data	Unlikely	Severe	Inform customer of security best practices
Customer keeps credentials on post-it notes which leads to credential being revealed to third party	Customer	Negligent Customer	Unauthorized Account Login	User Authenticity	Unlikely	Critical	Inform customer of security best practices

Now let's give a look at a NIST risk model.

The table in this slide provides an example of application of the NIST risk model. Each row in the table represent a threat event. If a threat event has an impact on more than one asset, there will be a separate row for each asset attacked by the threat.

For example, in this table we have two threat events initiated by the threat source "Customer".

In the first scenario represented by the first two rows the customer exploits vulnerability "Lack of compliance with terms of use" to initiate the threat event "Customer shares credentials with next-of-kin". The threat event results in the impact "Unauthorized Account Login" which affects the assets Integrity of Account Data and User Authenticity.

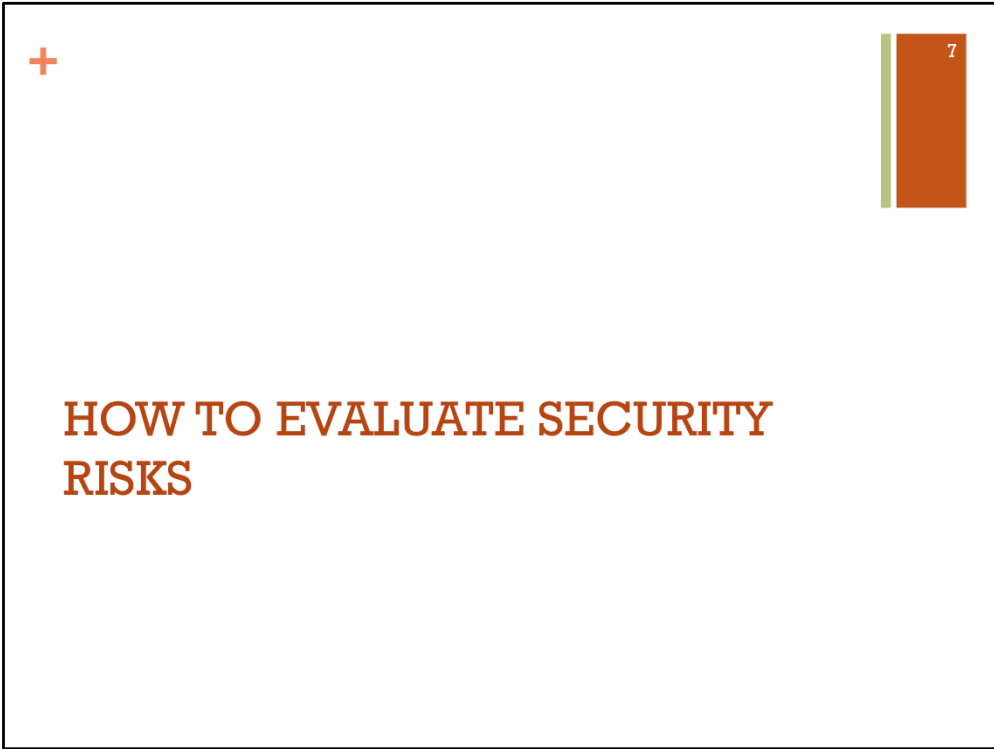
In the second scenario represented by the last two rows The customer exploits vulnerability "Negligent customer" to initiate the threat event "Customer keeps credentials on post-it note" which leads to "Credential being revealed to third party". Also this scenario results in the impact "Unauthorized Account Login" which affects the assets "Integrity of Account Data" and "User Authenticity".

The risk of the threat event is given by the likelihood that it occurs and the impact that it has on the assets Integrity of account data and User authenticity.

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

The first attack 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

8

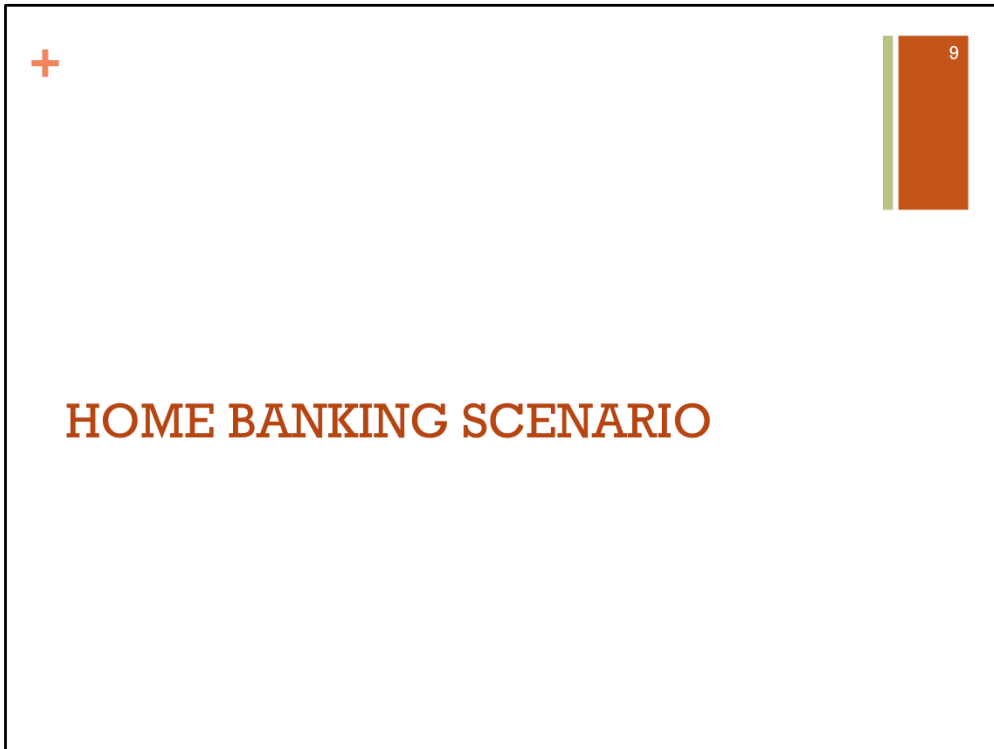
		Consequence/Impact				
		Insignificant	Minor	Severe	Critical	Catastrophic
Likelihood	Certain	Yellow	Orange	Red	Red	Red
	Very likely	Green	Yellow	Orange	Red	Red
	Likely	Green	Green	Yellow	Orange	Red
	Unlikely	Green	Green	Green	Yellow	Orange
	Very unlikely	Green	Green	Green	Green	Yellow

Risk value of an impact of a threat event is computed 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.

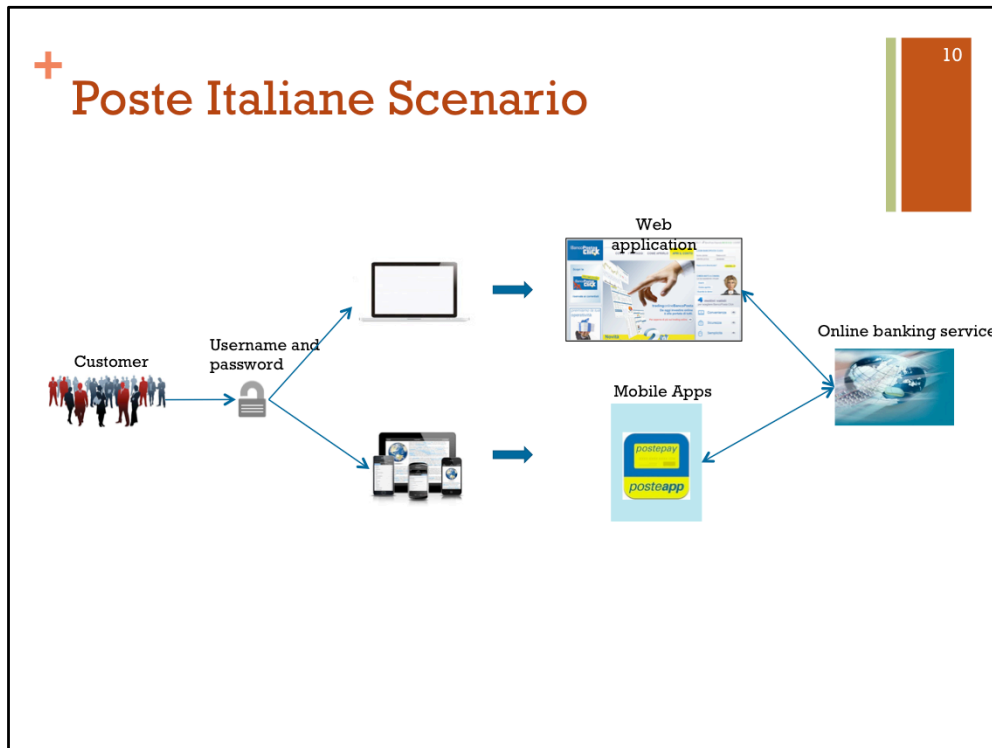
The entries of the map represent risk values:

- 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

11

- 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