
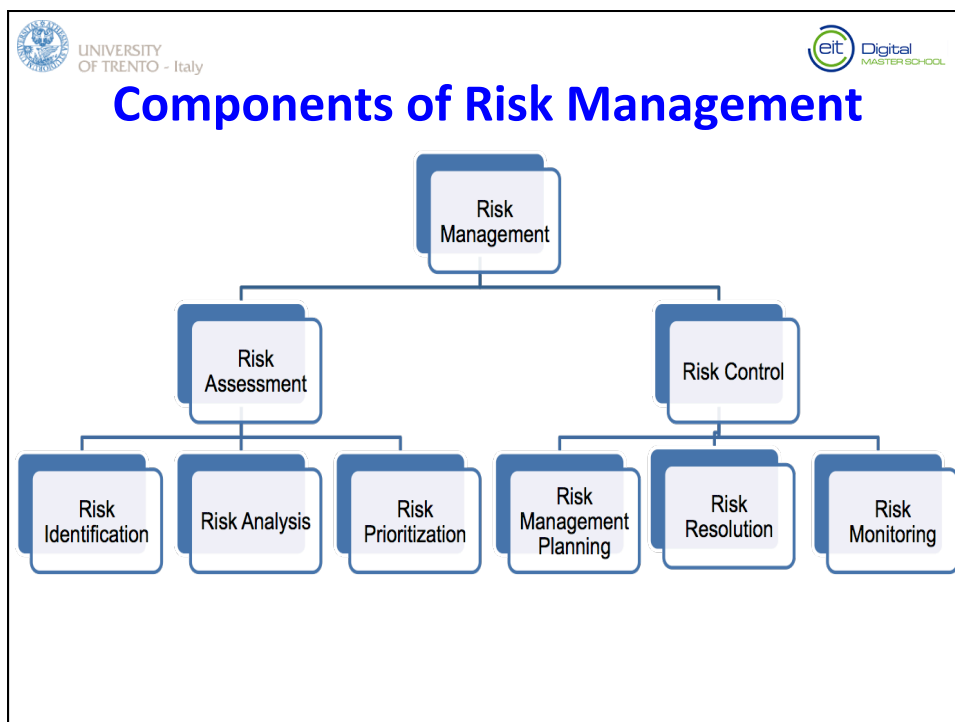
 UNIVERSITY OF TRENTO - Italy 

Cyber Security Risk Assessment Fall 2016

Lecture 04 – Security Risk Management – NIST - SecRAM
Fabio Massacci

Fall 2015 Fabio Massacci - EIT Security Engineering



UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Typical Division

- **Risk Assessment**
 - “Triggered”
 - New project
 - Estimate status, plan protection, roll new protections
- **Risk Control**
 - “On-going”
 - Existing activities
 - Monitor status, check metrics, react to events
- **Fuzzier in modern systems → things evolve quickly**
 - E.g. Poste Italiane IT System: 100+ change requests a month

Fall 2015 Fabio Massacci - EIT Security Engineering

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

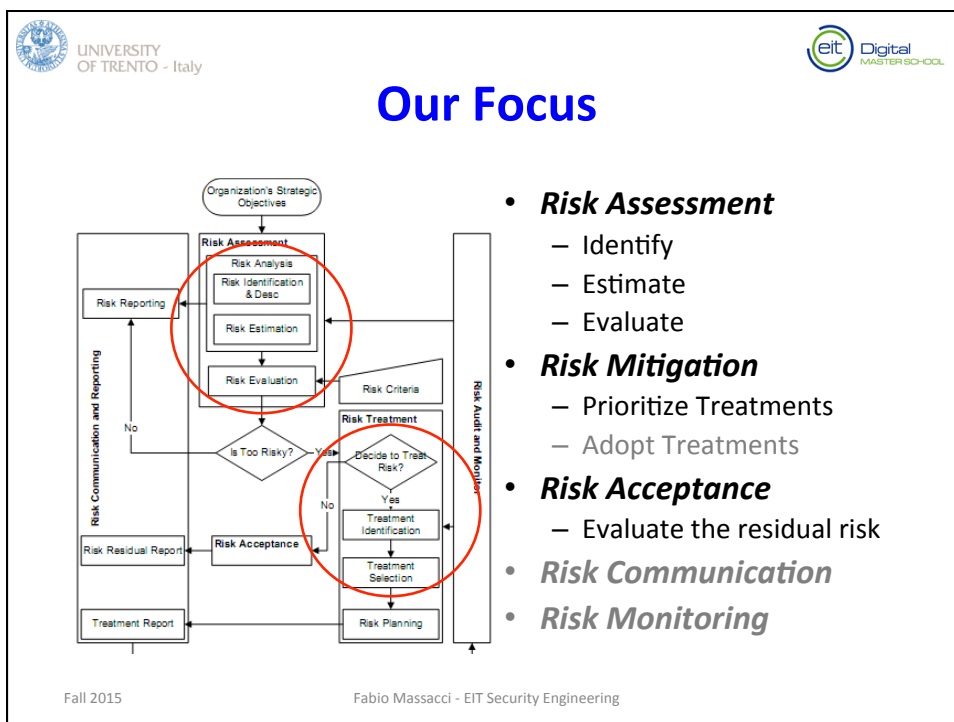
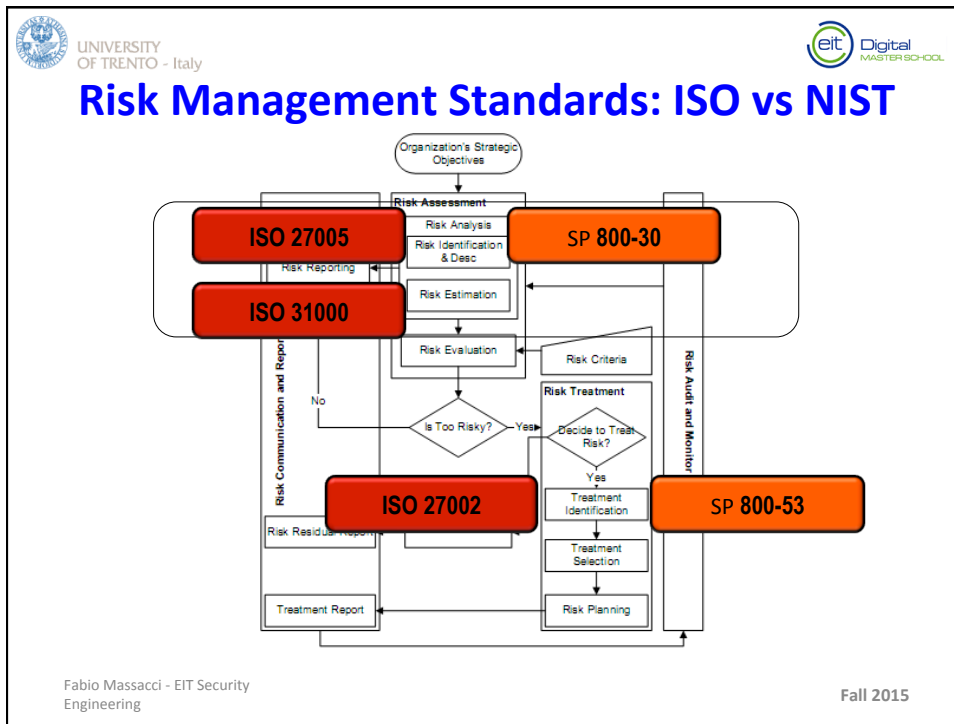
Temporal View of Risk Management


```

graph TD
    SO([Organization's Strategic Objectives]) --> RA[Risk Assessment]
    subgraph RA_Box [Risk Assessment]
        RA_Analysis[Risk Analysis]
        RA_ID[Risk Identification & Desc]
        RA_Est[Risk Estimation]
        RA_Eval[Risk Evaluation]
    end
    RA_Box --> ITR{Is Too Risky?}
    ITR -- No --> RA_Accept[Risk Acceptance]
    ITR -- Yes --> RT[Risk Treatment]
    subgraph RT_Box [Risk Treatment]
        RT_Decide{Decide to Treat Risk?}
        RT_ID[Treatment Identification]
        RT_Select[Treatment Selection]
        RT_Plan[Risk Planning]
    end
    RT_Box --> RR[Risk Reporting]
    RA_Accept --> RR
    subgraph RR_Box [Risk Reporting]
        RR_Rep[Risk Reporting]
        RR_Res[Risk Residual Report]
        RR_Treat[Treatment Report]
    end
    RR_Box --> RCM[Risk Communication and Reporting]
    RCM --> RR_Box
    RCM --> RA_Box
    RCM --> RT_Box
    RCM --> RAM[Risk Audit and Monitor]
    RAM --> RA_Box
    RAM --> RT_Box
    RAM --> RR_Box
  
```


- **Risk Assessment**
 - Identify
 - Estimate
 - Evaluate
- **Risk Mitigation**
 - Prioritize treatments
 - Adopt treatments
- **Risk Acceptance**
 - Evaluate the residual risk
- **Risk Communication**
- **Risk Monitoring**

Fall 2015 Fabio Massacci - EIT Security Engineering






UNIVERSITY
OF TRENTO - Italy




What is Risk Assessment?

- **Process to determine risks that affect organization's operations, assets, individuals, other organizations and even the nation**
- **Can be based on different principles**
 - Threat Based → e.g. NIST, UK IAS
 - Start from what can go wrong and defend from it
 - Asset Based → e.g. CoBIT, SESAR SecRAM
 - Start from what is worth and protect it

Fabio Massacci - EIT Security Engineering Fall 2015




UNIVERSITY
OF TRENTO - Italy




How To Evaluate Risk?

- **Key step of any Risk Assessment Process**
 - If you don't evaluate risk → risk management is useless
- **Two main approaches**
 - Qualitative
 - Employ methods, principle or rules based on ordinal levels (e.g very low, low, moderate, high, very high)
 - Cannot use arithmetics or probability to estimate outcomes just comparisons
 - Quantitative
 - Employ methods, etc. based on cardinal numbers (eg attack/days, dollars lost, etc.)
 - Can use arithmetics or probability theory to estimate outcome
- **Beware of "quantization"**
 - If you quantize numbers to have levels → cannot use arithmetics afterwards, must use interval arithmetics
- **For first part of the course → qualitative**

Fabio Massacci - EIT Security Engineering Fall 2015



UNIVERSITY
OF TRENTO - Italy



Quantitative vs Qualitative Approach

Quantitative Approach

- **Impact of individual cardholder data disclosure**
 - 10.000 USD/customer
- **Likelihood of occurrence of XSS threat event:**
 - 0.08/year
- **Number Customers**
 - 1M
- **Risk x Customer = 800 US/ (year*customer)**
 - 10.000 USD/customer * 0.08/year
- **Global Risk = 800M USD/year**
 - 1M customer * 800 USD/ (year*customer)

Qualitative Approach

- **Impact of cardholder data disclosure : High**
- **Likelihood of occurrence of XSS threat event: High**
- **Risk :**

Impact/ Likelihood	Very High	High
Very High	Very High	High
High	Very High	High
Moderate	High	Moderate
Low	Moderate	Low
Very Low	Low	Low

Fall 2015
Fabio Massacci - EIT Security Engineering

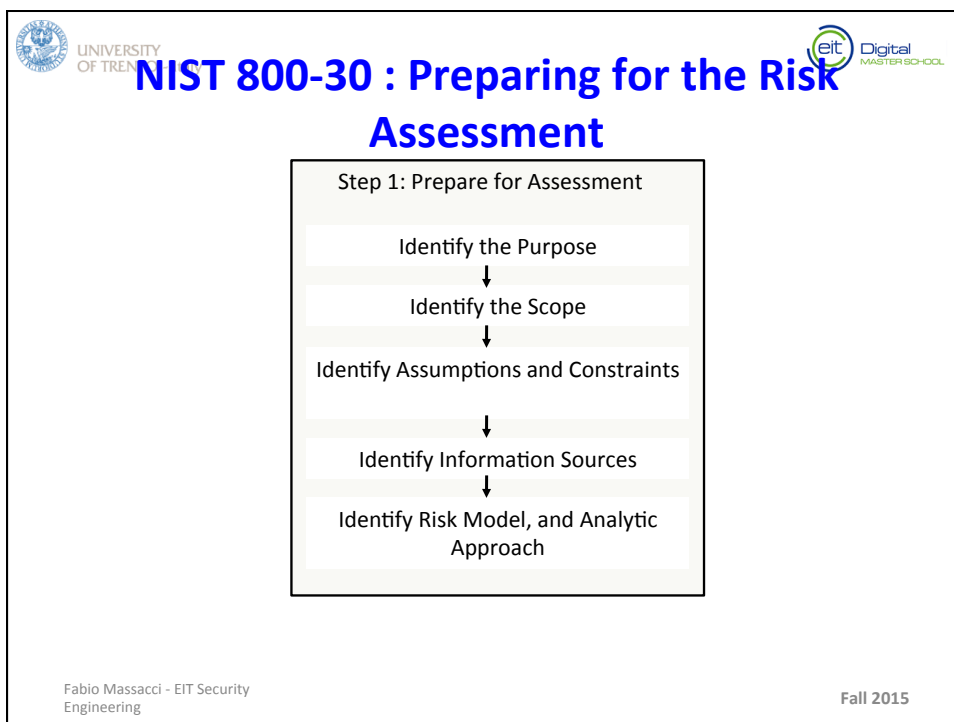
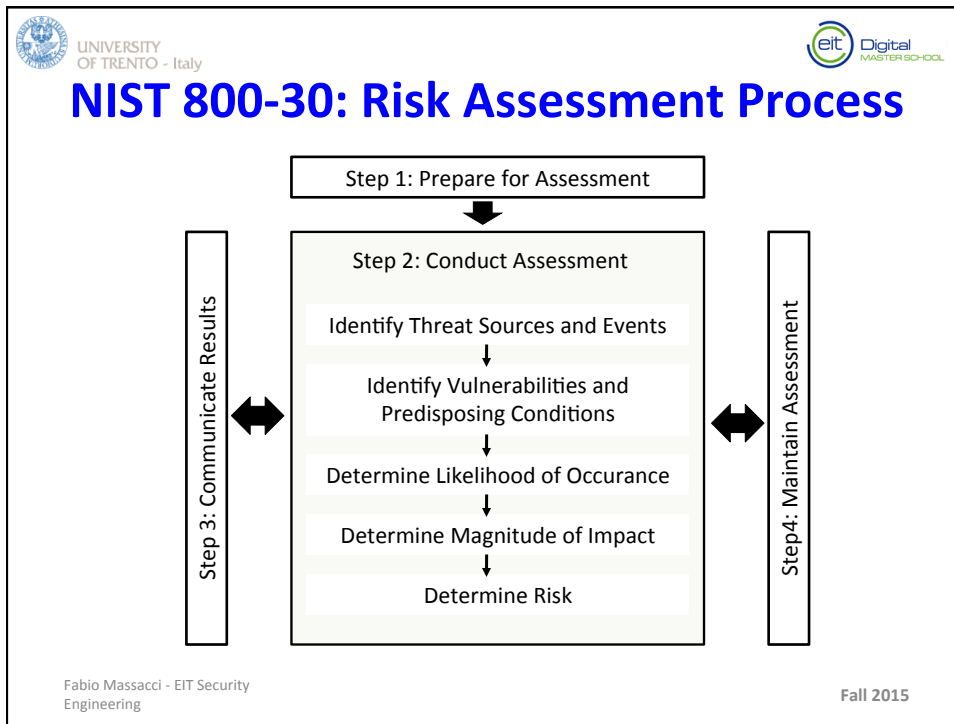




UNIVERSITY
OF TRENTO - Italy



NIST 800-30 standard for risk assessment

Fall 2015
Fabio Massacci - EIT Security Engineering





 UNIVERSITY OF TRENTO - Italy 

NIST 800-30 : Preparation

- **Risk Purpose**
 - Establishing a baseline assessment of risk
- **Decision Supported**
 - Selection of Controls
- **Assumptions and Constraints**
 - All possible threat sources and events
- **Risk Model and Analytical Approach**
 - Threat Oriented
 - Qualitative

Fabio Massacci - EIT Security Engineering Fall 2015

 UNIVERSITY OF TRENTO - Italy 

NIST 800-30 : Conduct Assessment

Step 2: Conduct Assessment

Identify Threat Sources and Events

↓

Identify Vulnerabilities and Predisposing Conditions

↓

Determine Likelihood of Occurance


↓

Determine Magnitude of Impact


↓

Determine Risk

Fabio Massacci - EIT Security Engineering Fall 2015



UNIVERSITY
OF TRENTO - Italy




NIST: Identify Threats


- **Identify threat sources**
 - Identify threat sources relevant for the organization
 - Assess their intent, capability and target
- **Identify threat events**
 - Determine source information to identify threats
 - Determine threats events relevant to conduct the assessment
 - Identify threat sources that could initiate the events

Fabio Massacci - EIT Security
Engineering

Fall 2015



UNIVERSITY
OF TRENTO - Italy




NIST: Identify Threats (Ex)


Threat Source	Threat Event
Alice	Install a malware on her laptop
Outsider	Conduct SQL Injection attack to BC portal

Fabio Massacci - EIT Security
Engineering

Fall 2015




UNIVERSITY
OF TRENTO - Italy




NIST: Identify Vulnerabilities

- **Vulnerabilities**
 - Identify using organization-defined information sources
 - Assess the severity
- **Predisposing conditions**
 - Identify
 - Assess the pervasiveness

Fabio Massacci - EIT Security Engineering Fall 2015




UNIVERSITY
OF TRENTO - Italy




NIST: Identify Vulnerabilities

Threat Source	Threat Event	Vulnerability	Predisposing Condition
Alice	Install Malware	No Anti Virus Installed	N/A
Outsider	SQL Injection Attack	No Interpreter Input Validation	N/A

Fall 2015 Fabio Massacci - EIT Security Engineering




UNIVERSITY OF TRENTO - Italy




NIST: Determine Likelihood (1)

- **Determine Likelihood of Occurrence**
 1. Determine Likelihood of Threat Event Initiation
 - Investigate Threat Source Characteristics
 2. Determine Likelihood of Threat Event Resulting In Adverse Impact
 - Investigate Vulnerabilities and Predisposing Conditions
 3. Compute Overall Likelihood as combination of the two above
 - Take Max or Min, “average”, of the two
 - Consider Likelihood of Initiation
 - Consider Likelihood of Impact

Fabio Massacci - EIT Security Engineering Fall 2015



UNIVERSITY OF TRENTO - Italy



NIST: Determine Likelihood (2)

- **Likelihood of Threat Initiation Scale**
 - Are the bad guys really going to do it?

Qualitative Values	Description
Very High	Adversary is almost certain to initiate the threat
High	Adversary is highly likely to initiate the threat
Moderate	Adversary is somewhat likely to initiate the threat
Low	Adversary is unlikely to initiate the threat
Very Low	Adversary is highly unlikely to initiate the threat

Fall 2015 Fabio Massacci - EIT Security Engineering

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

NIST: Determine Likelihood (3)

- **Likelihood of adverse impact scale**
 - IF somebody tries
 - THEN How likely are things going wrong

Qualitative Values	Description
Very High	It is almost certain to have adverse impacts
High	It is highly likely to have adverse impacts
Moderate	It is somewhat likely to have adverse impacts
Low	It is unlikely to have adverse impacts
Very Low	It is highly unlikely to have adverse impacts

Fall 2015 Fabio Massacci - EIT Security Engineering


UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

NIST: Determine Likelihood (4)


Threat Source	Threat Event	Likely Initiation	Likely Impact
Alice	Install Malware	Moderate	High
Outsider	SQL Inj. Attack	Very High	Very High

Likely Impact	Very Low	Low	Moderate	High	Very High
Likely Initiation					
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

Fabio Massacci - EIT Security Engineering Fall 2015




UNIVERSITY
OF TRENTO - Italy




NIST: Determine Impact (1)

- **Identify possible adverse impacts and affected assets**
 - Characteristics of threat sources
 - Vulnerabilities and predisposing conditions
 - Susceptibility given implemented security controls
- **Possible adverse impacts**
 - Harm to operations
 - Harm to assets
 - Harm to individuals
 - Harm to other organization
 - Harm to the nation

Fabio Massacci - EIT Security Engineering Fall 2015



UNIVERSITY
OF TRENTO - Italy




NIST: Determine Impact (2)


- **Impact Assessment Scale**

Qualitative Values	Description
Very High	The threat event could be expected to have multiple severe or catastrophic adverse effects
High	The threat event could be expected to have severe or catastrophic adverse effects
Moderate	The threat event could be expected to have serious adverse effects
Low	The threat event could be expected to have limited adverse effects
Very Low	The threat event could be expected to have negligible adverse effects

Fabio Massacci - EIT Security Engineering Fall 2015




UNIVERSITY
OF TRENTO - Italy




NIST: Determine Impact (3)

Threat Source	Threat Event	Impact
Alice	Install Malware	Moderate
Outsider	SQL Injection	High

Fabio Massacci - EIT Security Engineering Fall 2015



UNIVERSITY
OF TRENTO - Italy



NIST: Determine Risk (1)

- ***Identify Risks as Combination of***
 - Likelihood of Occurance and
 - Impact
- ***Order identified threat events based on the associated risk level***
 - Highest Risks on Top of the list
- ***Prioritize threats with risks at the same level***

Fabio Massacci - EIT Security Engineering Fall 2015

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

NIST: Determine Risk (2)

Threat Source	Threat Event	Likely Occurrence	Impact
Alice	Install Malware	Moderate	Moderate
Outsider	SQL InjAttack	Very High	High

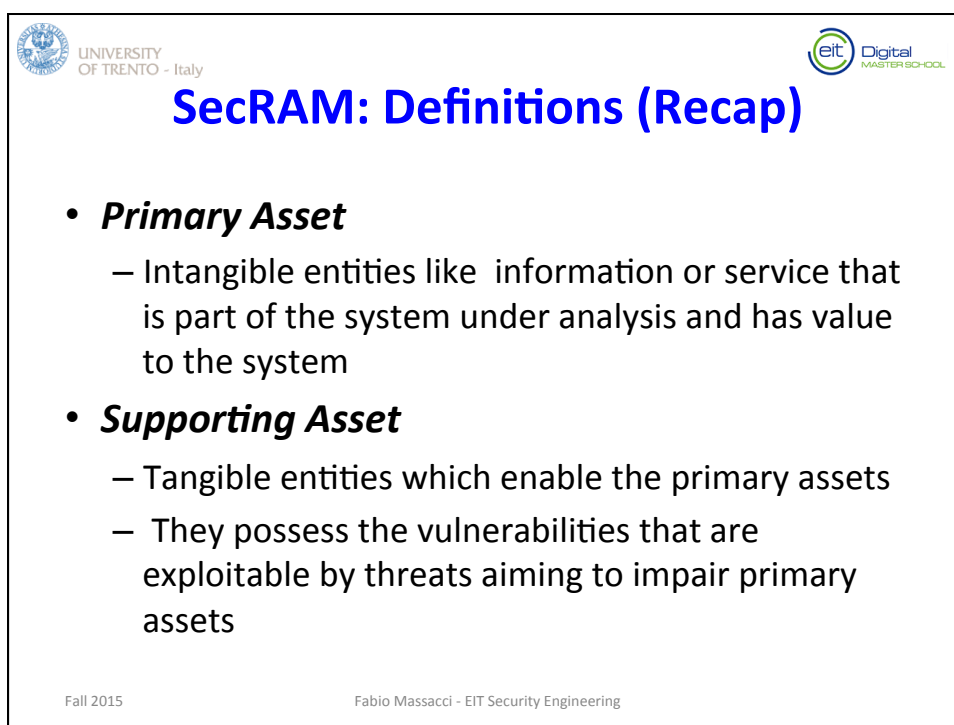
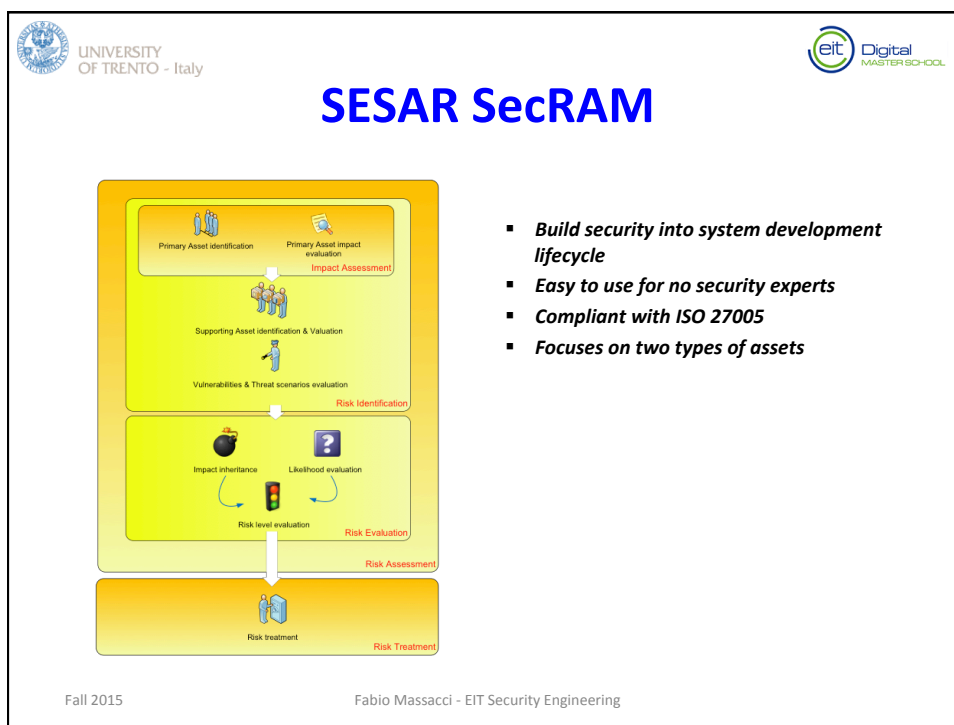
Impact	Very Low	Low	Moderate	High	Very High
Likelihood	Very High	Low	Moderate	High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low


Fabio Massacci - EIT Security Engineering Fall 2015

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL


SESAR SecRAM

Fall 2015 Fabio Massacci - EIT Security Engineering






UNIVERSITY
OF TRENTO - Italy




SecRAM: Definitions (Recap)

- **Threat Source (or Agent)**
 - 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

Fall 2015 Fabio Massacci - EIT Security Engineering




UNIVERSITY
OF TRENTO - Italy




SecRAM: Definitions (Recap)

- **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

Fall 2015 Fabio Massacci - EIT Security Engineering




UNIVERSITY
OF TRENTO - Italy




SecRAM: Definitions (Recap)

- **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 assets

Fall 2015 Fabio Massacci - EIT Security Engineering



UNIVERSITY
OF TRENTO - Italy



SecRAM: Definitions (Recap)

- **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

Fall 2015 Fabio Massacci - EIT Security Engineering

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

Application Scenario

- Poste Italiane: access to e-banking site**
Web application

Fall 2015 Fabio Massacci - EIT Security Engineering


UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

SecRAM: Primary Asset Identification


- Services**
- Information**

Primary Asset ID	Primary Asset	Type
PA ₁	Customer Information (Address, other info)	Information
PA ₂	Money (access to or actual value)	Information (value) + Service (Ability to use it)
PA ₃	Credentials	Information

Fall 2015 Fabio Massacci - EIT Security Engineering




UNIVERSITY OF TRENTO - Italy




SecRAM: Impact Table

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

Fall 2015 Fabio Massacci - EIT Security Engineering




UNIVERSITY OF TRENTO - Italy




OTP Loss - Impact Estimation

- **Threat Scenario**
 - User loses one time password due to malware infection
- **Compute Impact**

Fall 2015 Fabio Massacci - EIT Security Engineering




UNIVERSITY OF TRENTO - Italy




One Time Password Lost

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

Fall 2015 Fabio Massacci - EIT Security Engineering



UNIVERSITY OF TRENTO - Italy



Most Dangerous Place in Your Home?

- **Shower in the morning**
 - Probability that a person had an incident in that room
 - $Pr = 10^{-3}$
- **Dining Room for breakfast and dinner**
 - $Pr = 10^{-6}$
- **Bed at night**
 - $Pr = 10^{-9}$
- **Gym on Tuesday and Thursday**
 - $Pr = 2 \cdot 10^{-3}$
- **Kitchen on Saturday**
 - $Pr = 4 \cdot 10^{-3}$

Fall 2015 Fabio Massacci - EIT Security Engineering



UNIVERSITY
OF TRENTO - Italy




Most Dangerous Place in Your Home?


- ***If events are repeated you must account for scale***
 - Pr that something bad will happen in the next 10 years
- ***Shower x 1 day x 7day/week x 54 weeks x 10 years***
 - Pr = 10^{-3} → **0.98 == for sure**
- ***Dining Room for breakfast and dinner***
 - Pr = 10^{-6} → 0.01
- ***Bed at night***
 - Pr = 10^{-9} → 0.00
- ***Gym on Tuesday and Thursday***
 - Pr = $2 \cdot 10^{-3}$ → 0.66
- ***Kitchen on saturday***
 - Pr = $3 \cdot 10^{-3}$ → 0.80

Fall 2015

Fabio Massacci - EIT Security Engineering



UNIVERSITY
OF TRENTO - Italy




OTP Lost by Several Users


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

Fall 2015

Fabio Massacci - EIT Security Engineering




UNIVERSITY OF TRENTO - Italy




Beware of Scale/Repeated Events

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

Fall 2015
Fabio Massacci - EIT Security Engineering




UNIVERSITY OF TRENTO - Italy




SecRAM: Impact Assessment

Primary Asset	CIA	Personnel	Capacity	Performance	Economic	Branding	Regulatory	Environment	Overall Impact
One-Time Password	C				One customer = 1 Several customers (automated attacks) = 4	4	Depends (4) or maybe (3) or even none		
	I				=above	=			
	A				Maybe zero if only "visible to others" if taken away = above				

Fall 2015
Fabio Massacci - EIT Security Engineering




UNIVERSITY OF TRENTO - Italy




SecRAM: Impact Assessment

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

Fall 2015 Fabio Massacci - EIT Security Engineering




UNIVERSITY OF TRENTO - Italy




SecRAM: 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***

Fall 2015 Fabio Massacci - EIT Security Engineering




UNIVERSITY OF TRENTO - Italy




SecRAM: Supporting Assets Table

Primary Asset	One-Time Password	Credit Card Info
Supporting Asset			
Mobile Device	X	X	
One-Time Password Device	X		

Fall 2015 Fabio Massacci - EIT Security Engineering




UNIVERSITY OF TRENTO - Italy




SecRAM: Threat Scenarios

- ***For each supporting asset***
 - Identify relevant threats (threat catalogue)
 - Identify which criteria are targeted by the threat (confidentiality, integrity, availability)
 - Build a table
 - Linking threats to supporting assets
 - Impacts on primary asset CIA
- ***Each row is a “Threat Scenario”***
 - Describe what can go wrong

Fall 2015 Fabio Massacci - EIT Security Engineering



UNIVERSITY OF TRENTO - Italy




SecRAM: Threat Scenario Table


Supporting Assets	Threats	Primary Assets		
		One-Time Password		
		C	I	A
Mobile Device	Hack/malware installed	4	4	0
	Theft	4	4	

Something wrong and missing in this table

Fall 2015 Fabio Massacci - EIT Security Engineering




UNIVERSITY OF TRENTO - Italy




SecRAM: Threat Scenario Table

Supporting Assets	Threats	Vulnerability	Primary Assets		
			One-Time Password		
			C	I	A
Mobile device of a single user	Theft	Individual user careless with his device	1	1	1
Mobile device of single user	Malicious Code	Code downloadable by all users visiting a site with wrong operating system	1	1	1
Mobile devices of several users	Malicious Code	Code downloadable by all users visiting a site with wrong operating system	4	4	0

Fall 2015 Fabio Massacci - EIT Security Engineering




UNIVERSITY OF TRENTO - Italy




A Better View of Impact

Supporting Assets	Threats	Vulnerability	Impact on Primary Assets					
			OTP of one user			OTP of many users		
			C	I	A	C	I	A
Mobile of a one user	Theft	Individual user careless with his device	1	1	1	NA	NA	NA
Mobile of one user	Malware	Code downloadable by all users visiting a phishing web site	1	1	0			
Mobile devices of many users	Malware	Code downloadable by all users visiting a phishing site				4	4	0
Mobiles of many users	Theft	Many users careless with their device				4	4	4

Fall 2015 Fabio Massacci - EIT Security Engineering




UNIVERSITY OF TRENTO - Italy




SecRAM: Impact Evaluation

- **Inherited Impact**
 - Maximum impact of all CIA criteria and all primary assets (via supporting assets) targeted by the threat
- **Reviewed Impact**
 - Usually equal or lower than Inherited Impact
 - Inherited maybe an overkill → analysis of the scenario may rule out the full blow impact

Fall 2015 Fabio Massacci - EIT Security Engineering




UNIVERSITY OF TRENTO - Italy




SecRAM: Final Impact Evaluation

Supporting Assets	Threats	Vulnerability	Primary Assets			Inherited Impact	Reviewed Impact
			One-Time Password of single user				
			C	I	A		
Mobile Device	Theft	User careless with device and OTP app with password	2	2	2	2	0
Mobile Device	Theft	User careless and OTP app without a password	2	2	2	2	2
	Malware	Phishing web site and OTP app with password	2	2	0	2	1

Fall 2015
Fabio Massacci - EIT Security Engineering



UNIVERSITY OF TRENTO - Italy




SecRAM: Likelihood table


- **Disaggregate Values along dimensions**
 - Aggregate them for final value
 - Can use max, min or expert judgement

Likelihood areas	1. Not Credible	2. Remote	3. Occasional	4. Probable	5. Frequent
LA1: SKILLS	Inside information	Expert knowledge	Specialist knowledge	Engineering knowledge	No limitation
LA2: MEANS	Extremely scarce	Hard to obtain	Available with difficulty	Publicly available	No limitation
LA3: OPPORTUNITY	Never	Seldom	Regularly	Frequently	Always
LA4: PROFIT	None	Little	Fair	Significant	Large
LA5: ATTENTION	No media attention	Little attention of local media	Fair attention of local media	Regional media attention	World-wide media attention
LA6: IMPUNITY	Certainty of punishment	High chance of punishment	Fair chance of punishment	Little chance of punishment	No chance of punishment
LA7: DETECTION	Certainty of detection	High chance of detection	Fair chance of detection	Detection due to 'chance'	Not possible to predict or detect

Fall 2015
Fabio Massacci - EIT Security Engineering




UNIVERSITY OF TRENTO - Italy




Likelihood Estimation

- **Threat Scenario**
 - Student failed degree because of plagiarism. Expelled by University. Decide to pay those £\$%& professors what they deserve...
- **Which is less likely?**
 - Suicidal Car Bomb
 - Remotely Piloted Car Bomb
- **Why?**

Fall 2015 Fabio Massacci - EIT Security Engineering



UNIVERSITY OF TRENTO - Italy



Suicidal Car Bomb

Likelihood areas	1. Not Credible	2. Remote	3. Occasional	4. Probable	5. Frequent
LA1: SKILLS	Inside information	Expert knowledge	Specialist knowledge	Engineering knowledge	No limitation
LA2: MEANS	Extremely scarce	Hard to obtain	Available with difficulty	Publicly available	No limitation
LA3: OPPORTUNITY	Never	Seldom	Regularly	Frequently	Always
LA4: PROFIT	None	Little	Fair	Significant	Large
LA5: ATTENTION	No media attention	Little attention of local media	Fair attention of local media	Regional media attention	World-wide media attention
LA6: IMPUNITY	Certainty of punishment	High chance of punishment	Fair chance of punishment	Little chance of punishment	No chance of punishment
LA7: DETECTION	Certainty of detection	High chance of detection	Fair chance of detection	Detection due to 'chance'	Not possible to predict or detect

Fall 2015 Fabio Massacci - EIT Security Engineering

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

Remotely Piloted Car Bomb

Likelihood areas	1. Not Credible	2. Remote	3. Occasional	4. Probable	5. Frequent
LA1: SKILLS	Inside information	Expert knowledge	Specialist knowledge	Engineering knowledge	No limitation
LA2: MEANS	Extremely scarce	Hard to obtain	Available with difficulty	Publicly available	No limitation
LA3: OPPORTUNITY	Never	Seldom	Regularly	Frequently	Always
LA4: PROFIT	None	Little	Fair	Significant	Large
LA5: ATTENTION	No media attention	Little attention of local media	Fair attention of local media	Regional media attention	World-wide media attention
LA6: IMPUNITY	Certainty of punishment	High chance of punishment	Fair chance of punishment	Little chance of punishment	No chance of punishment
LA7: DETECTION	Certainty of detection	High chance of detection	Fair chance of detection	Detection due to 'chance'	Not possible to predict or detect


Fall 2015
Fabio Massacci - EIT Security Engineering

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL


Remotely vs Suicidal Car Bomb

Likelihood areas	1. Not Credible	2. Remote	3. Occasional	4. Probable	5. Frequent
LA1: SKILLS	Inside information	Expert knowledge	Specialist knowledge	Engineering knowledge	No limitation
LA2: MEANS	Extremely scarce	Hard to obtain	Available with difficulty	Publicly available	No limitation
LA3: OPPORTUNITY	Never	Seldom	Regularly	Frequently	Always
LA4: PROFIT	None	Little	Fair	Significant	Large
LA5: ATTENTION	No media attention	Little attention of local media	Fair attention of local media	Regional media attention	World-wide media attention
LA6: IMPUNITY	Certainty of punishment	High chance of punishment	Fair chance of punishment	Little chance of punishment	No chance of punishment
LA7: DETECTION	Certainty of detection	High chance of detection	Fair chance of detection	Detection due to 'chance'	Not possible to predict or detect

Fall 2015
Fabio Massacci - EIT Security Engineering




UNIVERSITY OF TRENTO - Italy




Summary 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 application/project/activity
2. Unlikely	There is a low chance that the scenario successfully occurs during the life time of the application
1. Very Unlikely	There is little or no chance that the scenario successfully occurs in a short time

Fall 2015
Fabio Massacci - EIT Security Engineering



UNIVERSITY OF TRENTO - Italy



Risk Assessment

Likelihood	Mitigated Impact				
	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

Fall 2015
Fabio Massacci - EIT Security Engineering

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

The risk assessment table

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

Fall 2015 Fabio Massacci - EIT Security Engineering

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL


SecRAM: 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)


```

graph TD
    A([Risk Assessment Results]) --> B{Satisfactory Assessment?}
    B --> C[Risk Treatment Options]
    subgraph Risk_Treatment [Risk Treatment]
        C --> D[Accept (or Tolerate) Risk]
        C --> E[Reduce (or Treat) Risk]
        C --> F[Avoid (or Terminate) Risk]
        C --> G[Transfer Risk]
    end
    D --> H([Residual Risks?])
    E --> H
    F --> H
    G --> H
    H --> I{Satisfactory Treatment?}
    
```

Fall 2015 Fabio Massacci - EIT Security Engineering




UNIVERSITY OF TRENTO - Italy




SecRAM: 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

Fall 2015 Fabio Massacci - EIT Security Engineering




UNIVERSITY OF TRENTO - Italy




SecRAM: 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

Fall 2015 Fabio Massacci - EIT Security Engineering




UNIVERSITY
OF TRENTO - Italy




Always remember...

- ***“In general, qualitative risk rating systems satisfying conditions found in real-world rating systems and guidance documents and proposed as reasonable make two types of errors:***
 - (1) Reversed rankings, i.e., assigning higher qualitative risk ratings to situations that have lower quantitative risks; and
 - (2) Uninformative ratings, e.g., frequently assigning the most severe qualitative risk label (such as “high”) to situations with arbitrarily small quantitative risks and assigning the same ratings to risks that differ by many orders of magnitude”
 - (L.A. Cox, D. Babayev, W. Hube 2008)

Fall 2015 Fabio Massacci - EIT Security Engineering



UNIVERSITY
OF TRENTO - Italy



Outcomes of a Risk Assessment

- ***Target of Evaluation***
 - Assets
 - Value associated with assets
- ***Threat Analysis***
 - Threats
 - Vulnerabilities
 - Risk Estimation
 - Costs associated with risks
- ***Mitigation Analysis***
 - Controls to reduce the risks
 - Costs associated with recommendations
- ***A cost-benefit analysis***
 - Risk Appetite




UNIVERSITY
OF TRENTO - Italy




SRA – First Part of The Course

- **Target of Evaluation**
 - Assets
 - Value associated with assets
- **Threat Analysis**
 - Threats
 - Vulnerabilities
 - Qualitative Risk Estimation
 - Costs associated with risks
- **Mitigation Analysis**
 - Controls to reduce the risks
 - Costs associated with recommendations
- **A cost-benefit analysis**
 - Risk appetite



UNIVERSITY
OF TRENTO - Italy



Suggested Readings

- **Textbook (*Managing Risk in Information Systems, 2nd ed*)**
 - Chapter 4-5.
- **NIST SP 800-30**
 - Guide for Conducting Risk Assessments. Freely Available from NIST web site
- **NIST SP 800-53**
 - Security and Privacy Controls for Federal Information Systems and Organizations. Freely Available from NIST web site
- **SecRAM guide**
 - See Course Web Page
- **Mike Davis. “Buda’s Wagon: A Brief History of the Car Bomb” Verso Books. 2008.**
- **L.A. Cox, D. Babayev, W. Hube. “Some Limitations of Qualitative Risk Rating Systems”. *Risk Analysis*, 25(3), 2005**
 - <http://onlinelibrary.wiley.com/doi/10.1111/j.1539-6924.2005.00615.x/epdf>
(available from UNITN network)

Fabio Massacci - EIT Security
Engineering

Fall 2015