UNIVERSITY
OF TRENTO - Italy

eit Digital
MASTER SCHOOL

Security Engineering
Fall 2015

Lecture 04 – SESAR SECRAM

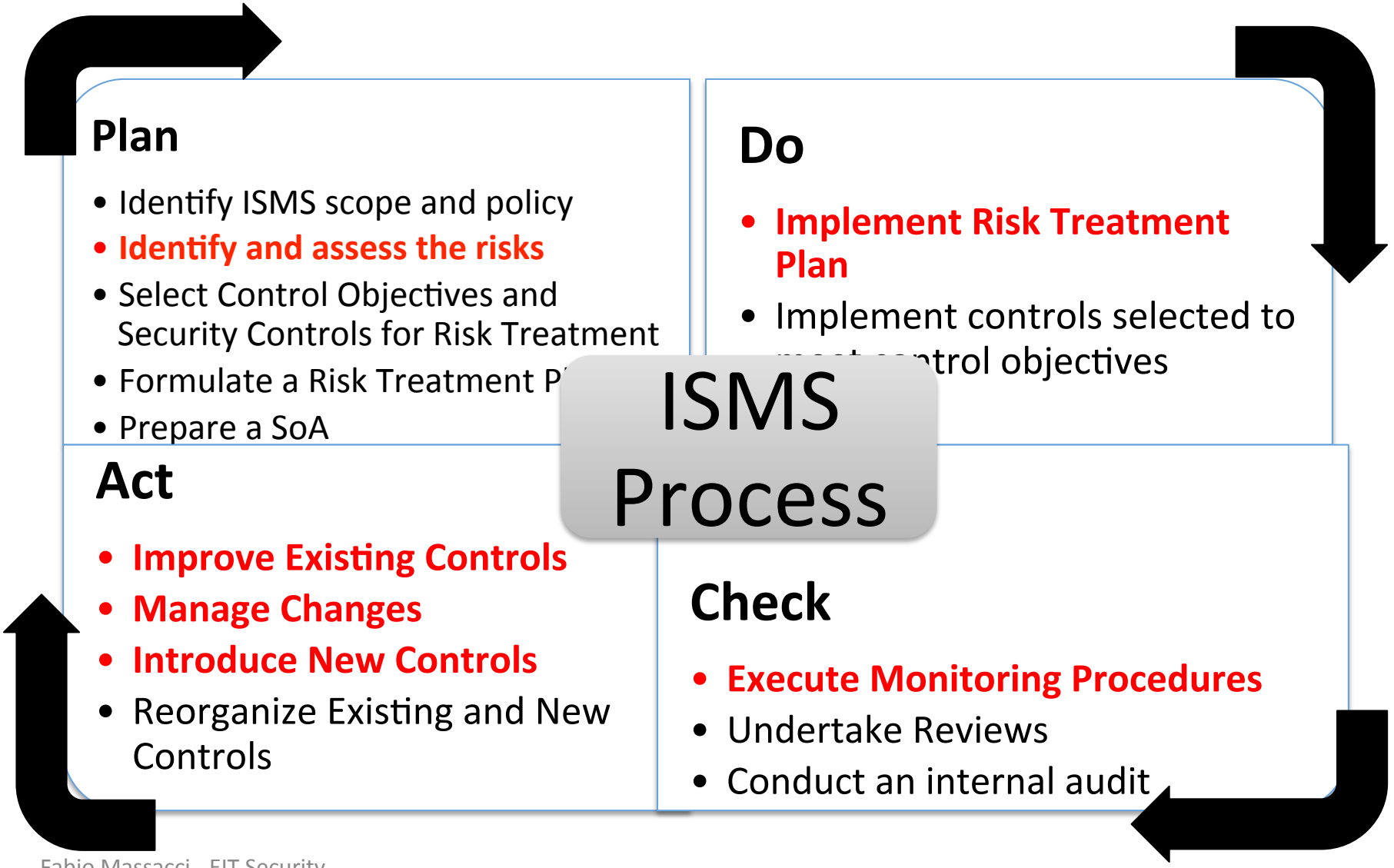
Fabio Massacci

Lecture Outline

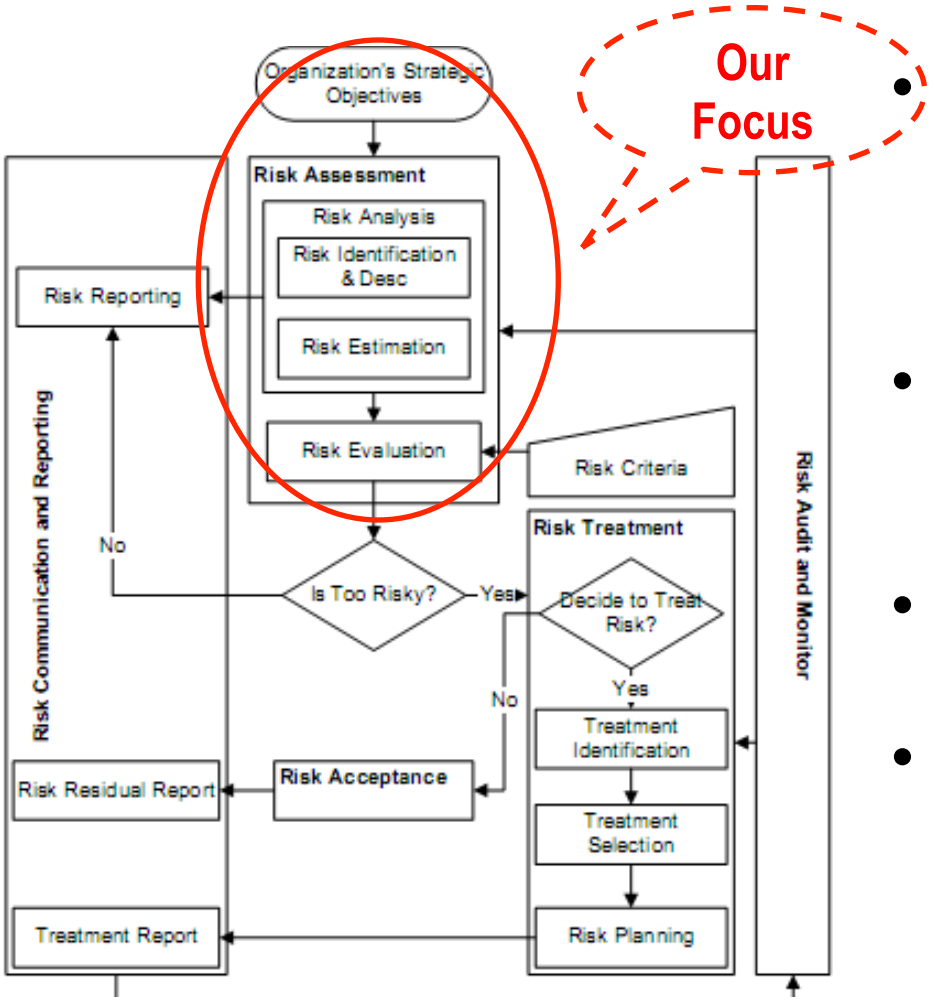
- ***Introduction to Risk Assessment***
  - Risk Model
  - Assessment Approaches
  - Analysis Approaches
- ***Standards for Risk Assessment***
  - ISO/IEC 27005, ISO\IEC 31000,NIST 800-30
- ***SESAR SECRAM***

Introduction to Risk Assessment

Recall: Plan-Do-Check-Act Process

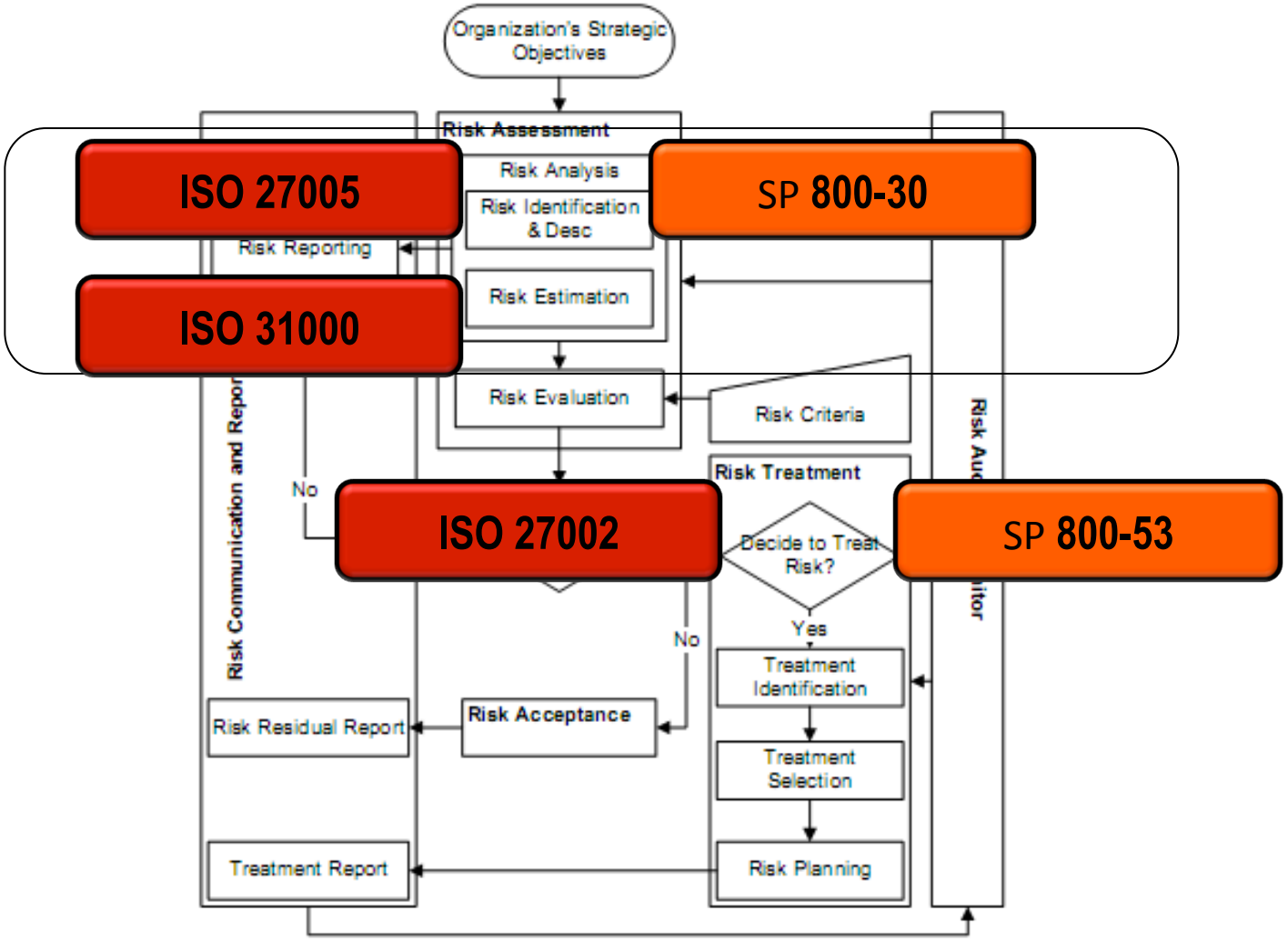


What is Risk Management?



- ***Risk Assessment***
  - Identify
  - Estimate
  - Evaluate
- ***Risk Mitigation***
  - Possible security controls
  - Adopt the suitable controls
- ***Risk Acceptance***
  - Evaluate the residual risk
- ***Risk Communication***
  - Communicate throughout the organization

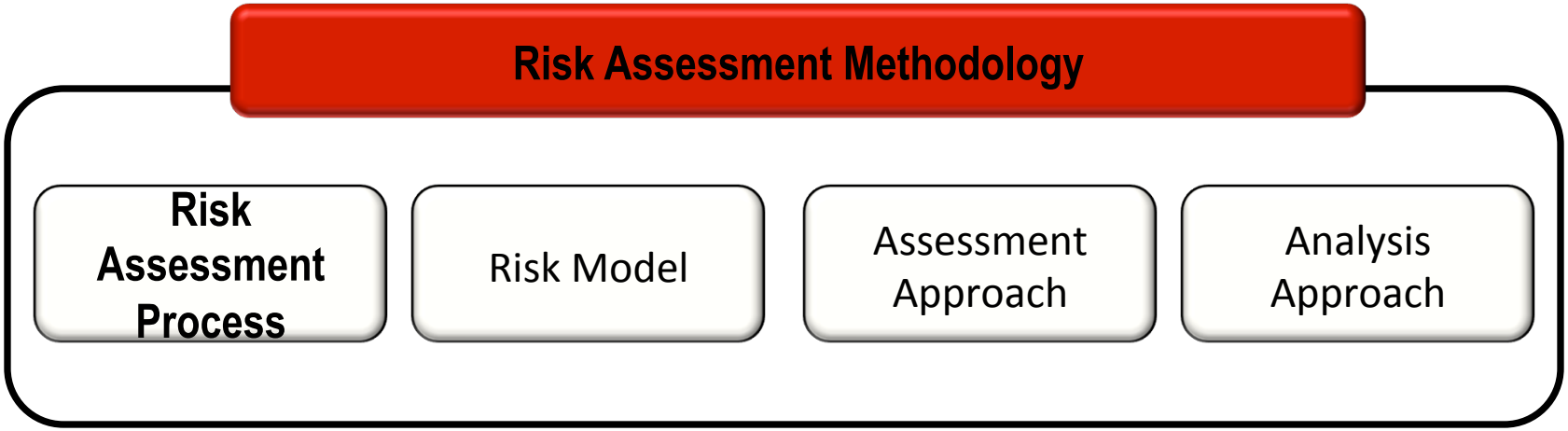
Risk Management Standards: ISO vs NIST



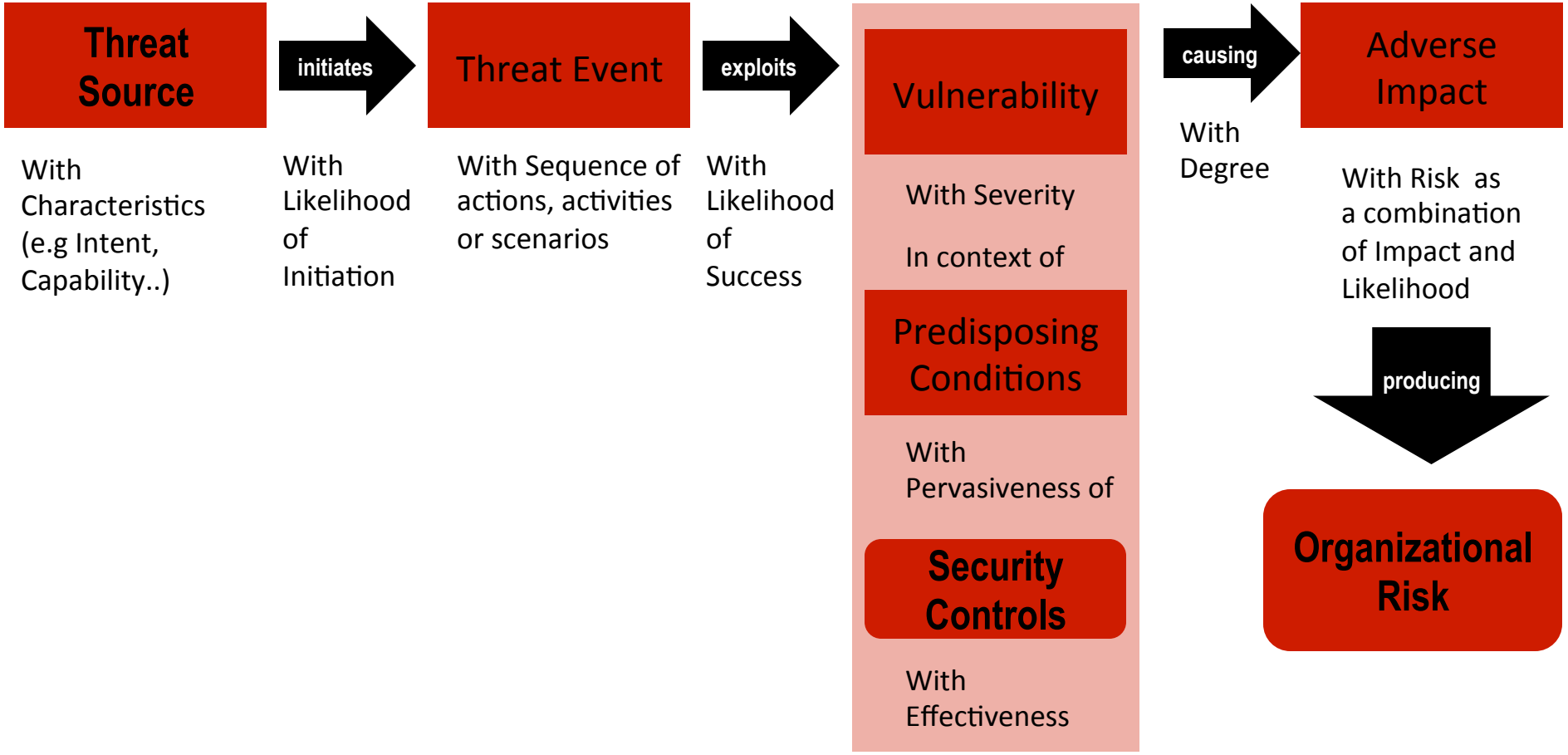
What is Risk Assessment?

- ***Process to determine risks that affect organization's operations, assets, individuals, other organizations and even the nation***
- ***Main steps***
  - Identifying security risks
  - Estimating security risks
  - Prioritizing security risks

What is a Risk Assessment Methodology?



What is a Risk Model?



Threat Event, Threat Source, Threat Scenarios

- ***Threat Source***
  - Entity who causes the threat
  - e.g attacker who wants to steal credit card numbers
- ***Threat Event***
  - Event or circumstance with potential adversely impact to organizational assets
  - e.g create counterfeit/spoof merchant web site
- ***Threat Scenario***
  - Set of discrete threat events that cause harm
  - E.g cross-site-scripting + phishing

Vulnerability & Predisposing Condition

- ***Vulnerability***
  - Weakness that could be exploited by a threat source
  - e.g inject arbitrary JavaScript code into the PayPal web site search function
- ***Predisposing condition***
  - Condition which affects the likelihood that a threat event results in adverse impact to organizational assets
  - e.g the web site looks trusted
  - e.g the use of a corporate network rather than a open network

Likelihood, Impact, Risk, Uncertainty

- ***Likelihood***
  - Probability that a threat event will occur
  - Probability that a threat event results in an adverse impact
- ***Adverse Impact***
  - Magnitude of the harm caused by a threat event
- ***Risk***
  - Function of Likelihood and Adverse Impact
- ***Uncertainty***
  - Imprecision/Degree of Belief/Lack of knowledge in Estimating Risk Factors
-

What is Risk Assessment?

- ***Aims to evaluate risk factors***
- ***Two main approaches***
  - Quantitative
    - Employ methods, principle or rules based on the use of numbers (scale 0-10)
  - Qualitative
    - Employ methods, principle or rules based on non-numerical categories or levels (e.g very low, low, moderate, high, very high)

Quantitative vs Qualitative Approach

Quantitative Approach

- ***Impact of individual cardholder data disclosure***
  - 10.000 USD/customer
- ***Likelihood of occurance 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 occurance of XSS threat event: High***
- ***Risk :***

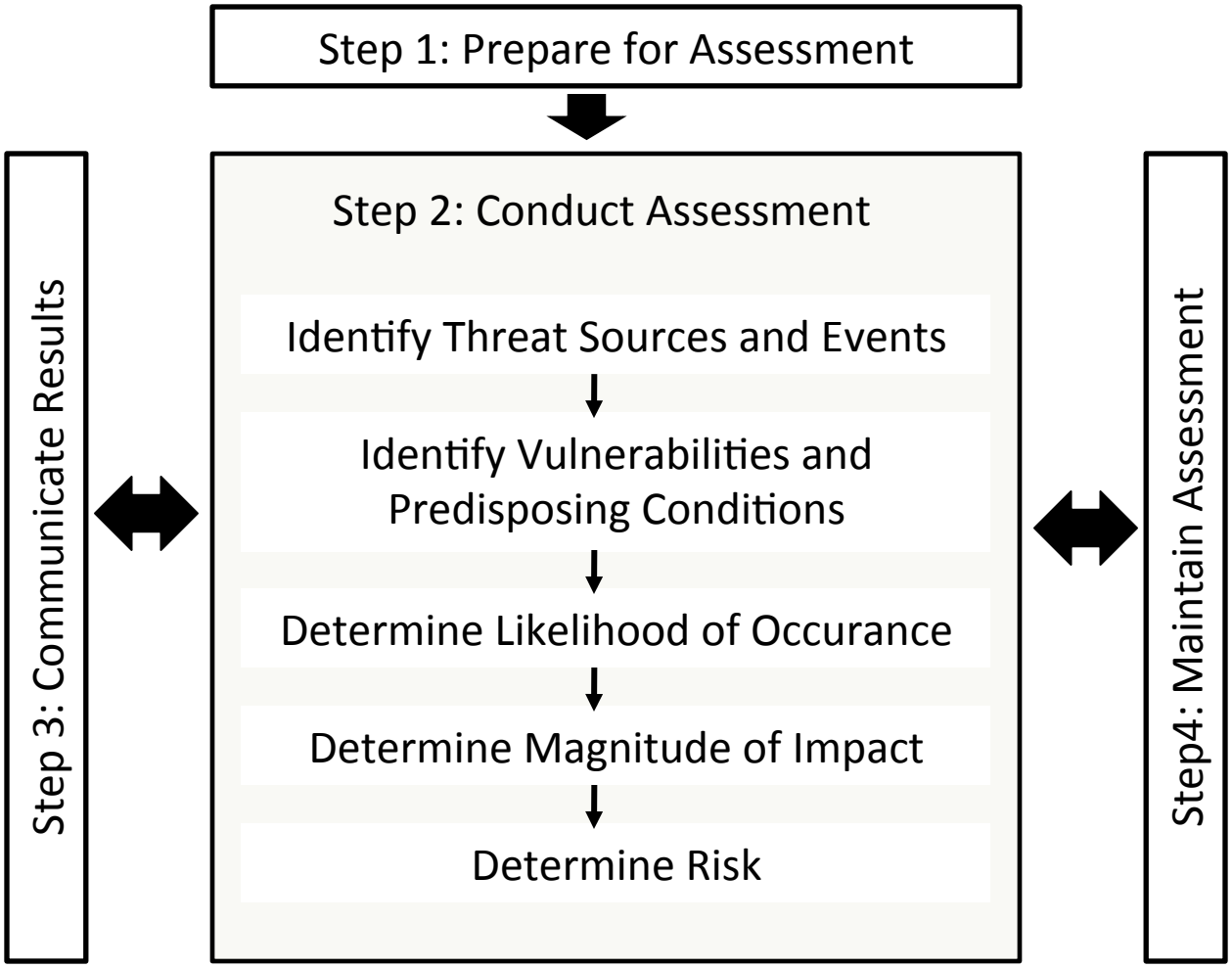
Impact/ Likelihood	Very High	High
Very High	Very High	High
High	Very High	High
Moderate	High	Moderate
Low	Moderate	Low
Very Low	Low	Low

What is Risk Analysis?

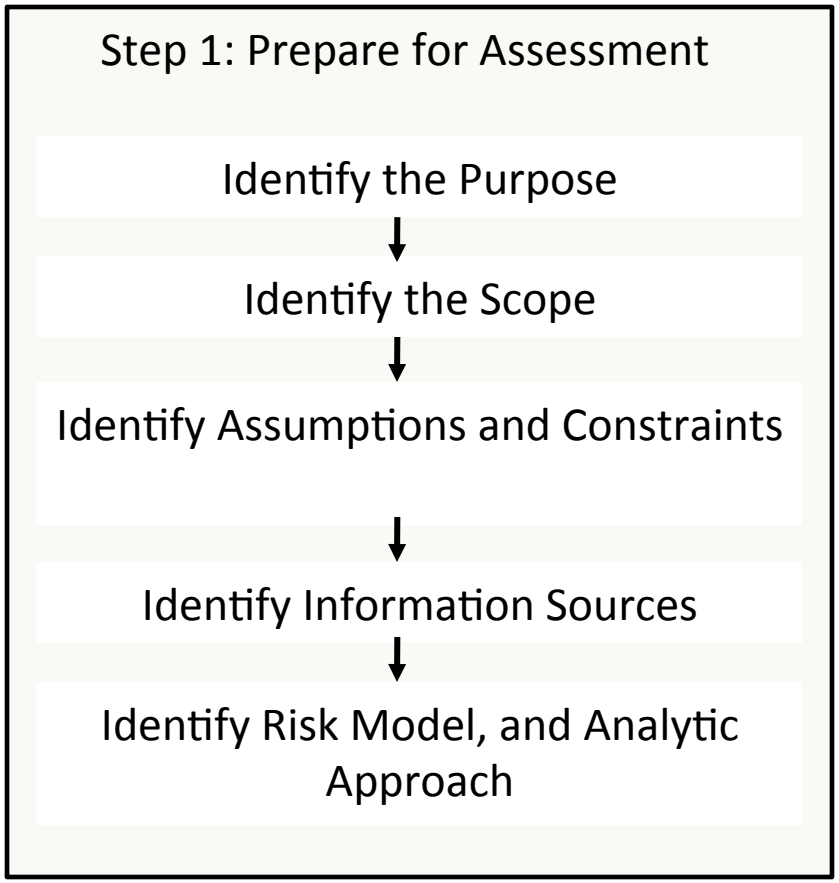
- ***The process of identifying, assessing risks***
- ***Possible approaches:***
  - Threat-oriented
  - Asset/Impact-oriented
  - Vulnerability-oriented

NIST 800-30 standard for risk assessment

NIST 800-30: Risk Assessment Process



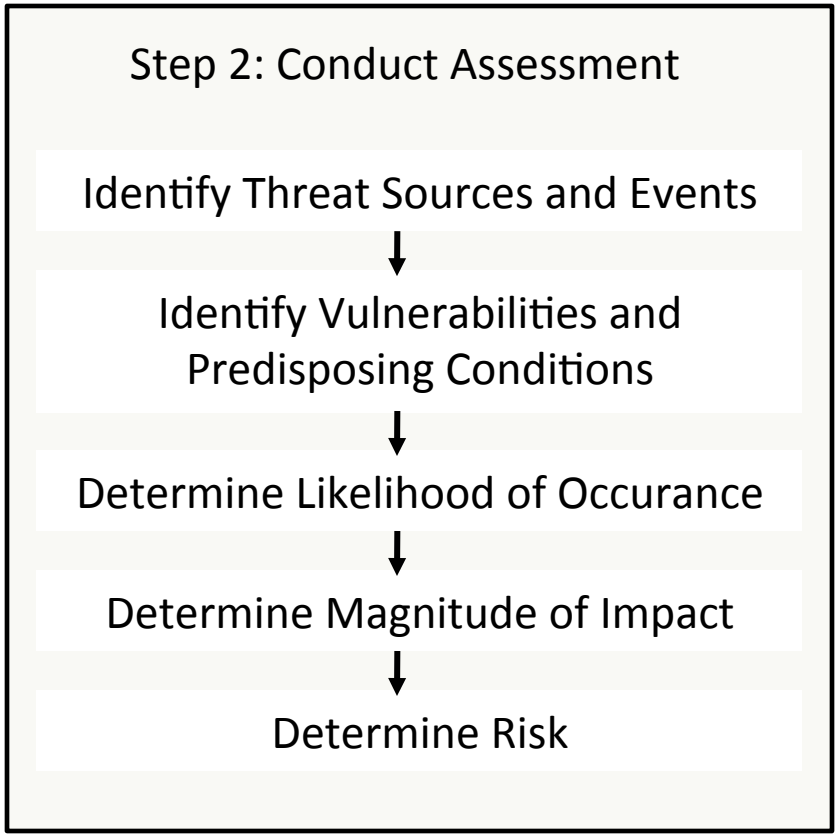
NIST 800-30 : Preparing for the Risk Assessment



NIST 800-30 : Preparing for the Risk Assessment

- ***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

NIST 800-30 : Conduct Assessment



Conduct Assessment: Identify Threats

- ***Identity 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

Conduct Assessment: Identify Threats

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

Conduct Assessment : Identify Vulnerabilities

- ***Identify vulnerabilities using organization-defined information sources***
- ***Assess the severity of identified vulnerabilities***
- ***Identify predisponing conditions***
- ***Assess the pervasiness of predisposing conditions***

Conduct Assessment : 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

Determine Likelihood (1)

- ***Determine Likelihood of Occurance***
  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 of the two
     - Consider Likelihood of Initiation
     - Consider Likelihood of Impact
     - Average of the two

Determine Likelihood (2)

- **Likelihood of Threat Initiation Scale**

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

Determine Likelihood (3)

- **Likelihood of Adverse Impact Scale**

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

Determine Likelihood (4)

Likelihood of Impact/ Likelihood of Initiation	Very Low	Low	Moderate	High	Very High
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

Threat Source	Threat Event	Likelihood of Initiation	Likelihood of Impact
Alice	Install Malware	Moderate	High
Outsider	SQL Injection Attack	Very High	Very High

Conduct Assessment: 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

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

Conduct Assessment: Determine Impact (3)

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

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***

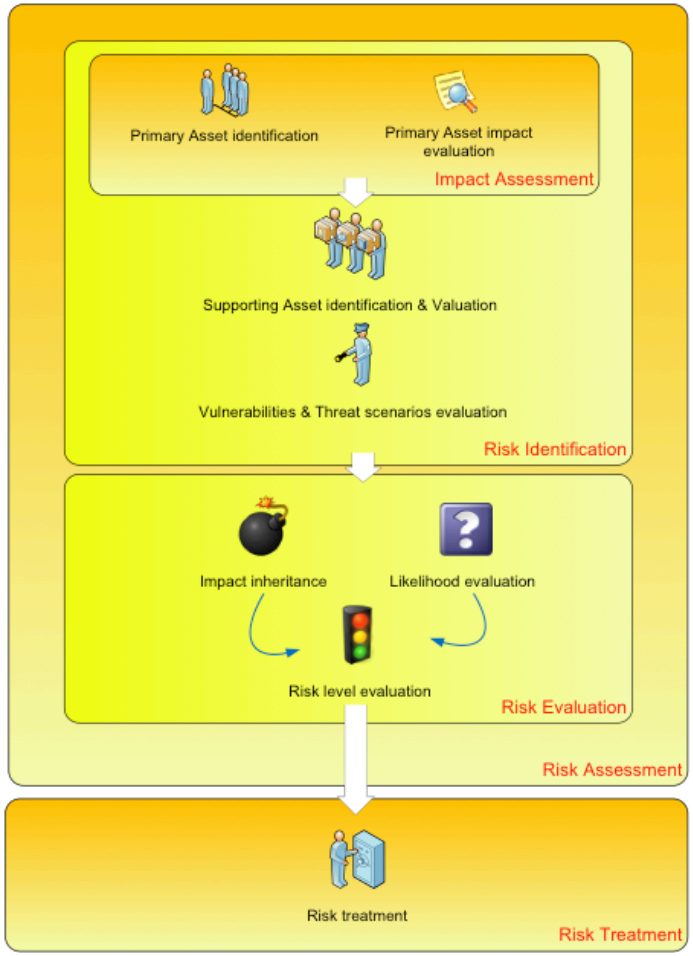
Conduct Assessment: Determine Risk (2)

Impact/ Likelihood	Very Low	Low	Moderate	High	Very High
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

Threat Source	Threat Event	Likelihood of Occurance	Impact
Alice	Install Malware	Moderate	Moderate
Outsider	SQL Injection Attack	Very High	Very High

SESAR SecRAM

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***

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

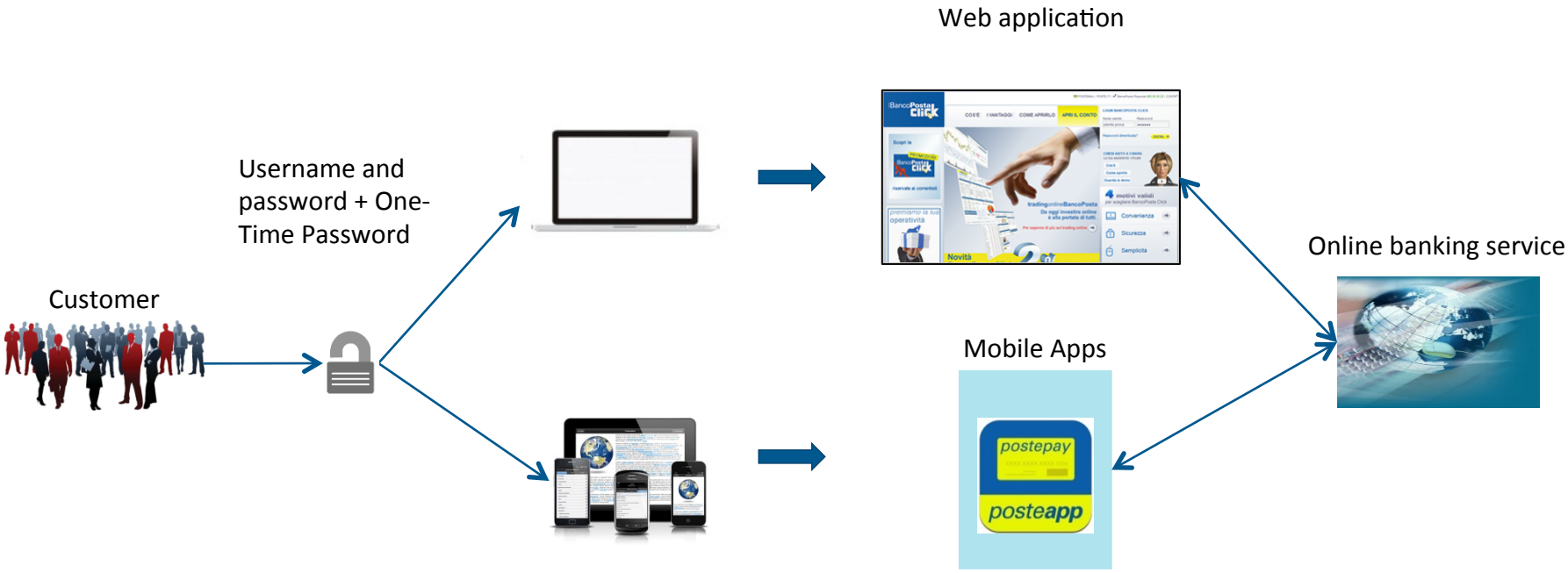
Definitions

- ***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 assets

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	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

Impact

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

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				

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								

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***

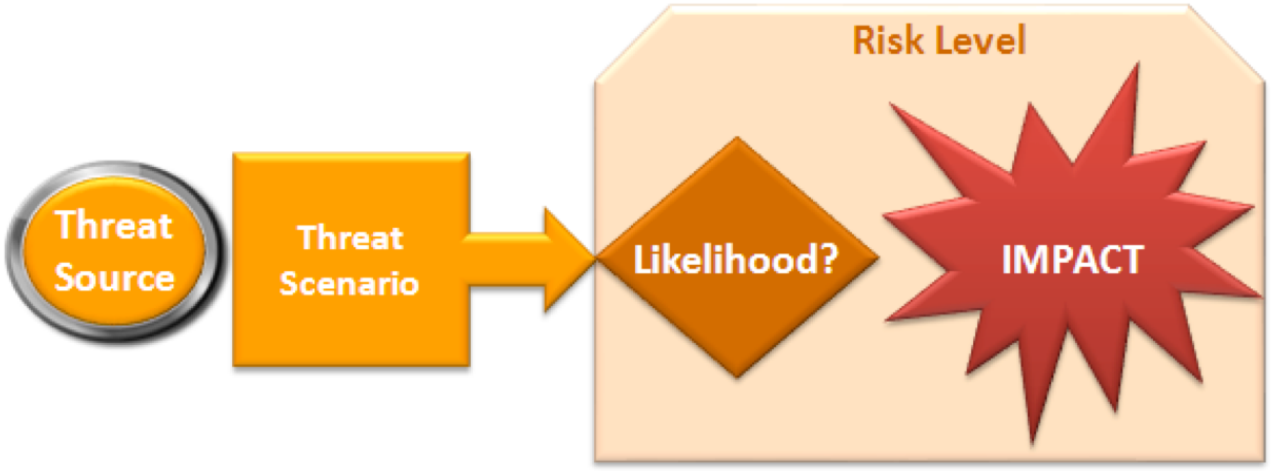
Supporting Assets Table

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

Threat Scenarios

Threat scenarios

– Threat × Supporting Asset → Impact on Primary Asset



Threat scenario steps

- ***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

The 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

The 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

Better View

			Impact on Primary Assets					
Supporting Assets	**Threats**	**Vulnerability**	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

Risk Evaluation

Impact Evaluation

- ***Inherited Impact***
  - Maximum impact of all CIA criteria and all the primary assets (via supporting assets) targeted by the threat
- ***Reviewed Impact***
  - Usually equal or lower than Inherited Impact

The impact Evaluation table

			Primary Assets				
Supporting Assets	**Threats**	**Vulnerability**	One-Time Password of single user			**Inherited Impact**	**Reviewed Impact**
			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

Disaggregated Likelihood table

Likelihood areas	1. Not Credible	2. Remote	3. Occasional	4. Probable	5. Frequent
LA1: SSKILLS	Inside information	Expert knowledge	Specialist knowledge	Engineering knowledge	No limitation
LA2: MEANS	Extremely scarse	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

Sucidal 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 scarse	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

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 scarse	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

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

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

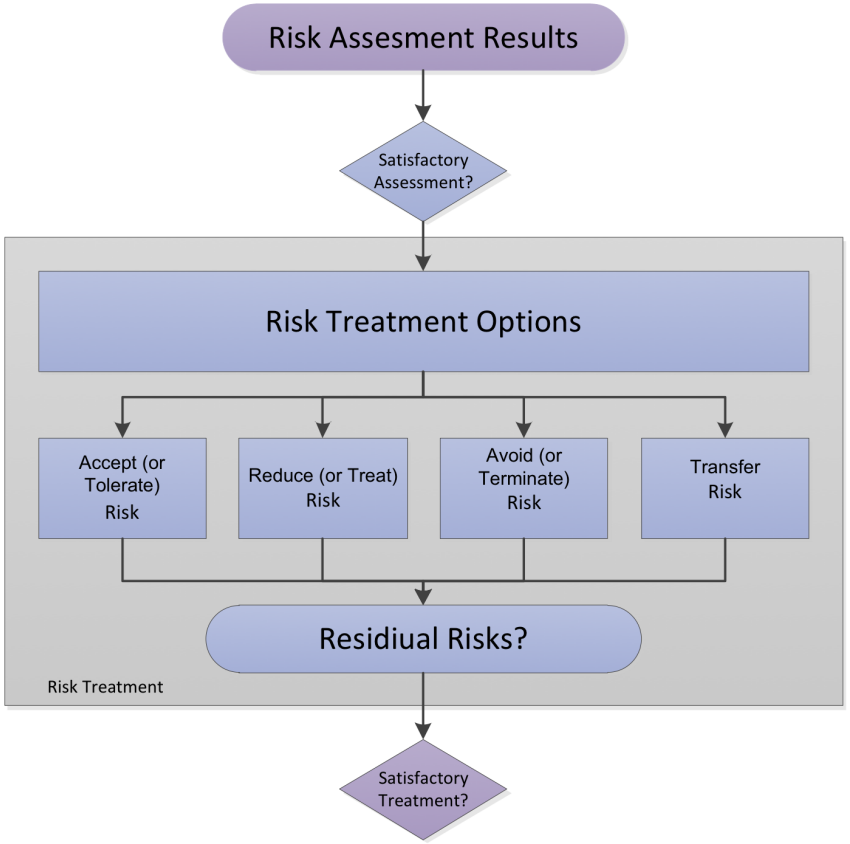
The risk assessment table

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

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)

Registration

- ***Choose a partner to work with for the assignments***
- ***Go to Course Web Site and Register***
  - Your name, last name, email and student ID
  - The name, last name, email and student ID of your partner

Suggested Readings

- ***Chapter 16. Stallings, Brown. Computer Security***
- ***NIST SP 800-30***
  - Guide for Conducting Risk Assesments. 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
- 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)