CYBER503x
Cybersecurity Risk Management

Unit 3: Risk Management Framework & Components 2

Risk Assessment
Step 3: Likelihood Determination

- Sample Likelihood (threat occurrence rate) definition:

Likelihood Level	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are infective. *Likely (76-100% chance), of successful exercise of threat within one year*
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability. *Probable (26-75% chance), , of successful exercise of threat within one year*
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised. *Not probable (0-25% chance) , of successful exercise of threat within one year*

Risk Assessment
Step 4: Impact Analysis

- To determine the adverse impact resulting from a successful threat exercise of a vulnerability.
  - Magnitude of Impact = Likelihood * Value

Sample Impact Definitions

- Impact can be described in terms of loss or degradation of any, or a combination of any, of the following security goals:

Impact	Confidentiality	Integrity	Availability
High	Loss of confidentiality leads to a **severe effect** on the organization.	Loss of integrity leads to a **severe effect** on the organization.	Loss of availability leads to a **severe effect** on the organization.
Medium	Loss of confidentiality leads to **a serious effect** on the organization.	Loss of integrity leads to **a serious effect** on the organization.	Loss of availability leads to **a serious effect** on the organization.
Low	Loss of confidentiality leads to a **limited effect** on the organization.	Loss of integrity leads to a **limited effect** on the organization	Loss of availability leads to a **limited effect** on the organization

Examples of Organizational Effect

Effect Type	Effect on Mission Capability	Financial Loss/Damage to Assets	Effect on Human Life
High	Long term loss of one or more primary mission capabilities	Over $100,000	Loss of life or life threatening injury
Medium	Long term loss of one or more minor or temporary loss of one or more primary mission capabilities	$5,000-$100,000	Significant harm, but not life threatening
Low	Temporary loss of one or more minor mission capabilities	Under $5,000	Minor harm (e.g., cuts and crapes)

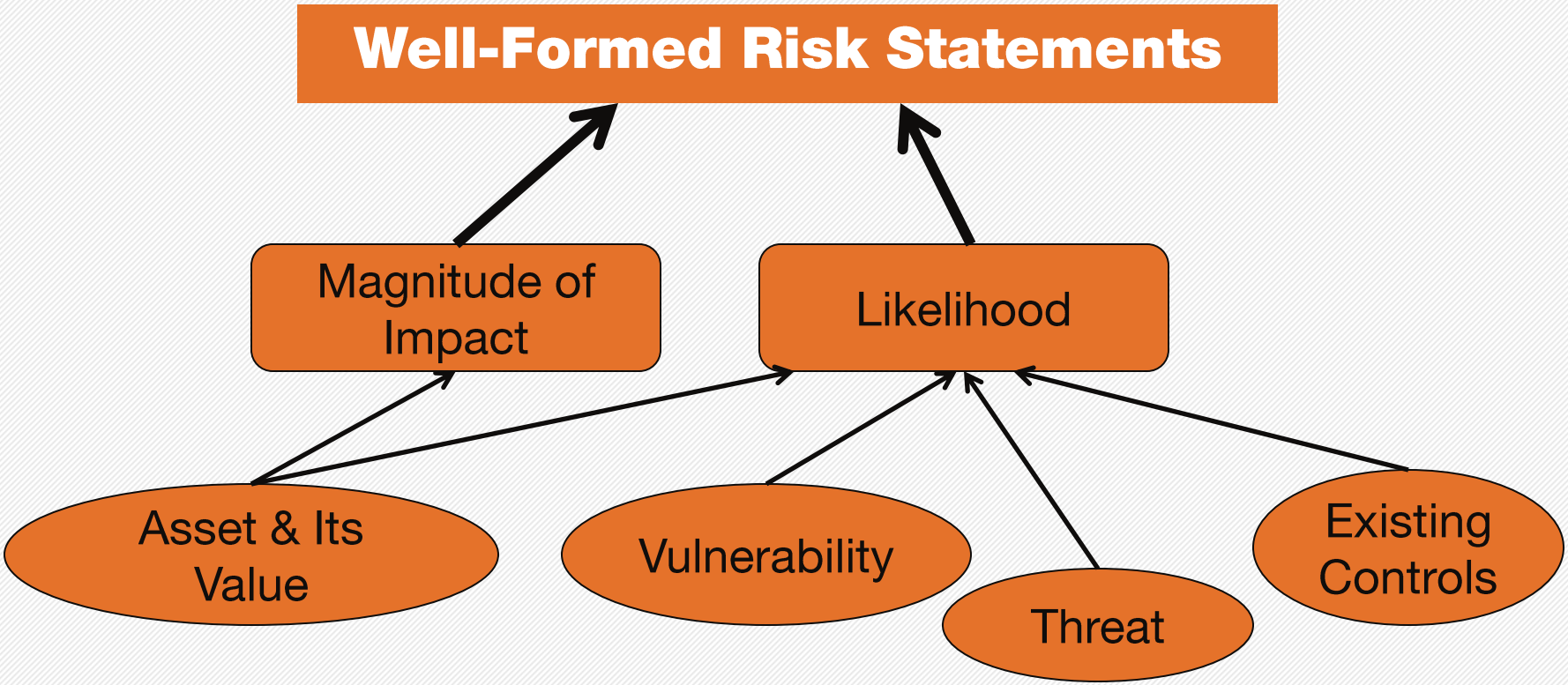
Impact Statements

- Output of this step is “impact statements” (either in word-sentences, or Summary Level tables)

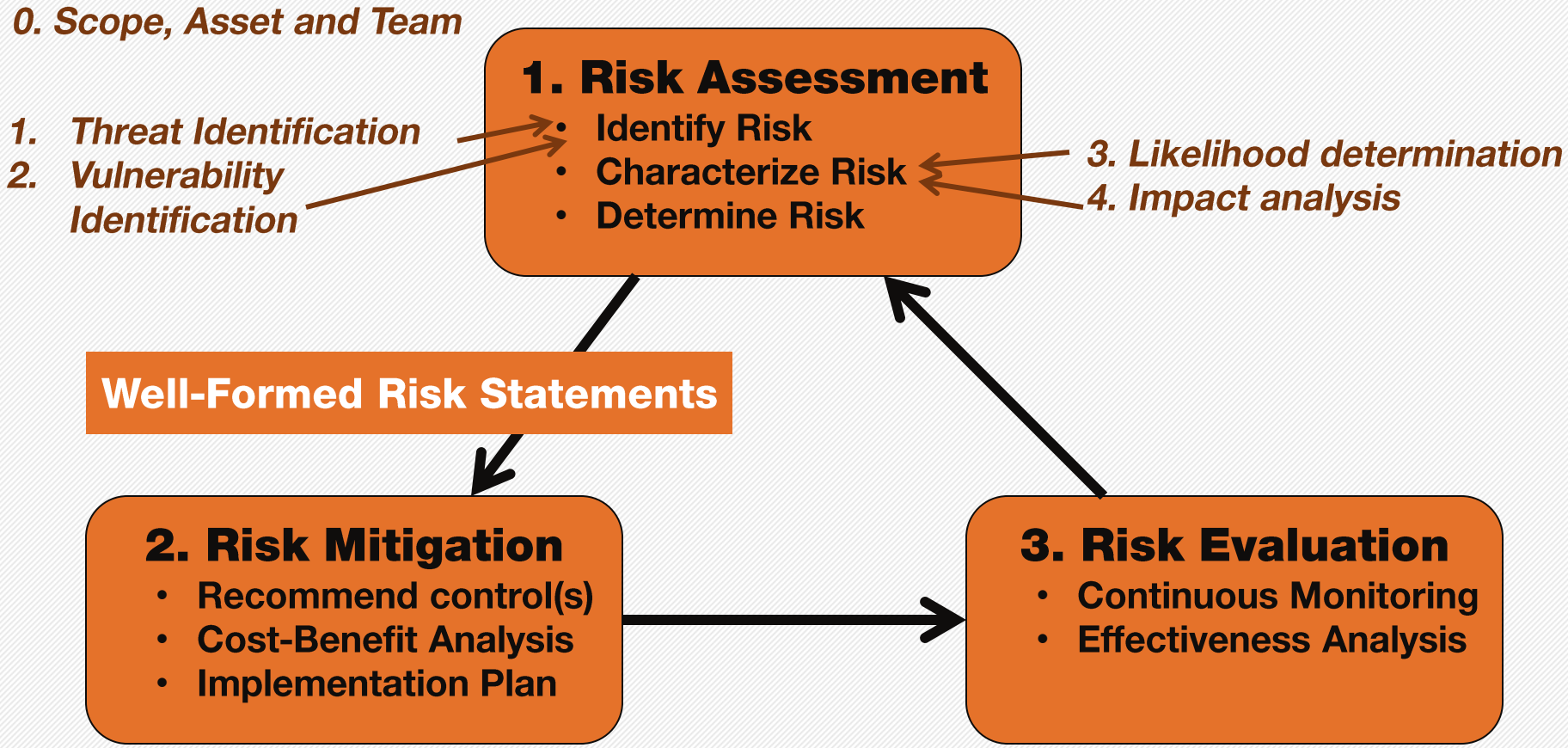
Risk Assessment
Final Step 5: Determine Risk

		Impact		
		High	**Moderate**	**Low**
Likelihood	**High**	High	High	Moderate
	Moderate	High	Moderate	Low
	Low	Moderate	Low	Low

Output of Risk Assessment



Risk Assessment: a recap



Example Introduction

- Using “ABC Bank” as an example:
  - Scope
  - Asset: Classification
  - Team

Asset Name	Asset Classification	Asset Owner
Consumer financial data	High Business Impact (HBI)	VP of Consumer Services

Example: Identify Risk

- Threat Identification:
  - Focuses on “What you are afraid of or are trying to avoid”
  - Integrity-related threat: *Unauthorized access to consumer data through theft of Financial Advisor credentials.*
- Vulnerability Identification:
  - Focuses on “How the threat could occur”
  - Three vulnerabilities considering the above threat:
    - *Theft of financial advisor credentials by trusted employee abuse non-technical attacks, e.g. social engineering, or eavesdropping*
    - *Theft of financial advisor credentials off LAN hosts through the use of outdated security configurations of antivirus signatures, host configuration, or outdated security patches.*
    - *Theft of financial advisor credentials off remote, or mobile hosts as a result of outdated security configurations.*

Characterize Risk: Likelihood Determination

Threat	Vulnerability	Exposure Level (H/M/L)	Existing Controls	Likelihood (H/M/L)
Unauthorized access to consumer data through theft of Financial Advisor credentials	1.1 Financial Advisor PSWD stealing thru poor host config: Remote Compromise	H	+Windows Update +Advisory emails +Antivirus updates on LAN connect + Configuration standards and Group Policy +updates on WAN	H
	1.2 Financial Advisor PSWD stealing thru poor host config: thru LAN managed device	H	Antivirus signature updates +Security Patch Management +Scanning and enforcement +Multimedia Advisory	M
	1.3 ABC Bank Employee Abuse	M	Awareness +Auditing +Segregation of duties	L
	1.4 Man in Middle	L	Virtual LAN architecture +Network infrastructure event auditing	L

Impact Analysis

Asset Name	Asset Class	Threat	Vulnerability	Exposure Level (H/M/L)	Existing Controls	Likelihood (H/M/L)	Impact Rating
Consumer financial data	HBI	Unauthorized access to consumer data through theft of Financial Advisor credentials	1.1 Financial Advisor PSWD stealing thru poor host config: Remote Compromise	H	+Windows Update +Advisory emails +Antivirus updates on LAN connect + Configuration standards and Group Policy +updates on WAN	H	H
			1.2 Financial Advisor PSWD stealing thru poor host config: thru LAN managed device	H	Antivirus signature updates +Security Patch Management +Scanning and enforcement +Multimedia Advisory	M	H
			1.3 ABC Bank Employee Abuse	M	Awareness +Auditing +Segregation of duties	M	M
			1.4 Man in Middle	L	Virtual LAN architecture +Network infrastructure event auditing	L	L

Risk Determination

Asset Name	Asset Class	Threat	Vulnerability	Exposure Level (H/M/L)	Existing Controls	Likelihood (H/M/L)	Impact Rating	Risk Level
Consumer financial data	HBI	Unauthorized access to consumer data through theft of Financial Advisor credentials	1.1 Financial Advisor PSWD stealing thru poor host config: Remote Compromise	H	+Windows Update +Advisory emails +Antivirus updates on LAN connect + Configuration standards and Group Policy +updates on WAN	H	H	H
			1.2 Financial Advisor PSWD stealing thru poor host config: thru LAN managed device	H	Antivirus signature updates +Security Patch Management +Scanning and enforcement +Multimedia Advisory	M	H	H
			1.3 ABC Bank Employee Abuse	M	Awareness +Auditing +Segregation of duties	M	M	M
			1.4 Man in Middle	L	Virtual LAN architecture +Network infrastructure event auditing	L	L	L

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

Final Risk Assessment Report

- The Well-Formed Risk Statements in table or paragraphs
- Consistent definitions on
  - Exposure Levels
  - Likelihood Levels
  - Impact Levels or Effects
- Risk Matrix – Determine Risk Level from Impact and Likelihood

Risk Assessment: Summary Level vs. Detail Level

- Pros:
  - Quick triage risks
- Cons:
  - Lack sufficient guidance for mitigation decisions

- Pros:
  - More detail view
  - Facilitates cost of control discussions in mitigation decisions
- Cons:
  - Time consuming

Detail Level Risk Assessment

- Detail level assessment can be triggered after review the summary results with stakeholders.
- The primary goal is to enable the organization to understand the rationale behind the most important risks to the company.
- It leverages many of the inputs used in the summary level list; however, the detailed view requires:
  - To be more specific in its impact and probability descriptions.
  - Specific statements on the effectiveness of the current controls
  - Delivers an estimate of each risk in quantifiable, monetary terms.
- Criteria for selecting risks from summary level:
  - High level risks: Every risk rated as high must be included on the detailed list.
  - Borderline risks: In some organization, even all moderate risks may be included in the detailed list.
  - Controversial risks: If a risk is new, not well understood, or viewed differently by stakeholders.

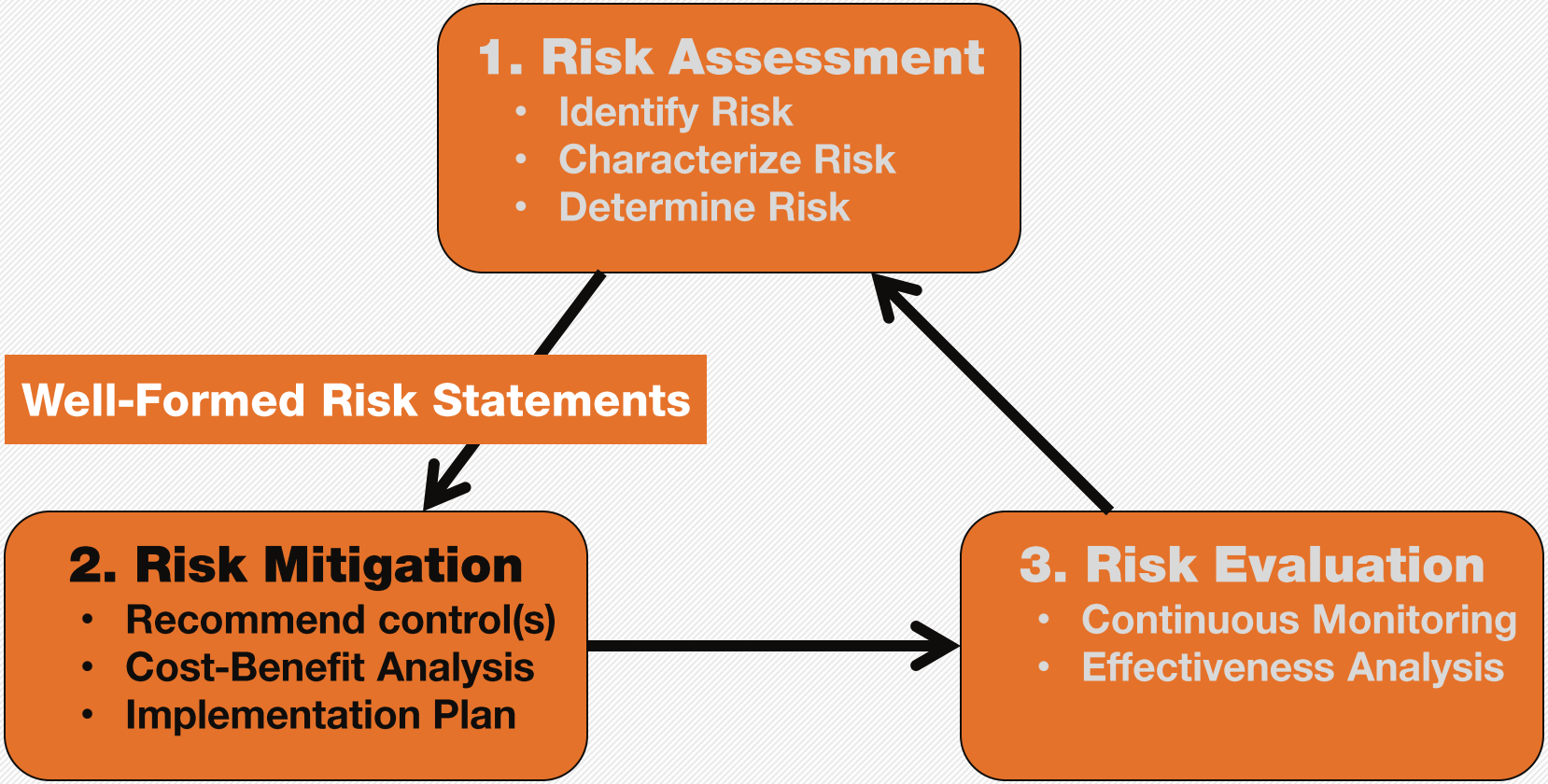
ABC Bank Example: Detailed Level View (1)

- Two risks for detailed level risk assessment or prioritization:
  - Remote Host Compromise (H)
  - LAN Host Compromise (H)
- Determine the likelihood
  - the likelihood of vulnerability based on its attributes and possible exploit
    - Attacker population
    - Remote vs. local access
    - Visibility of exploit
    - Automation of exploit
  - The likelihood of vulnerability based on the effectiveness of current controls

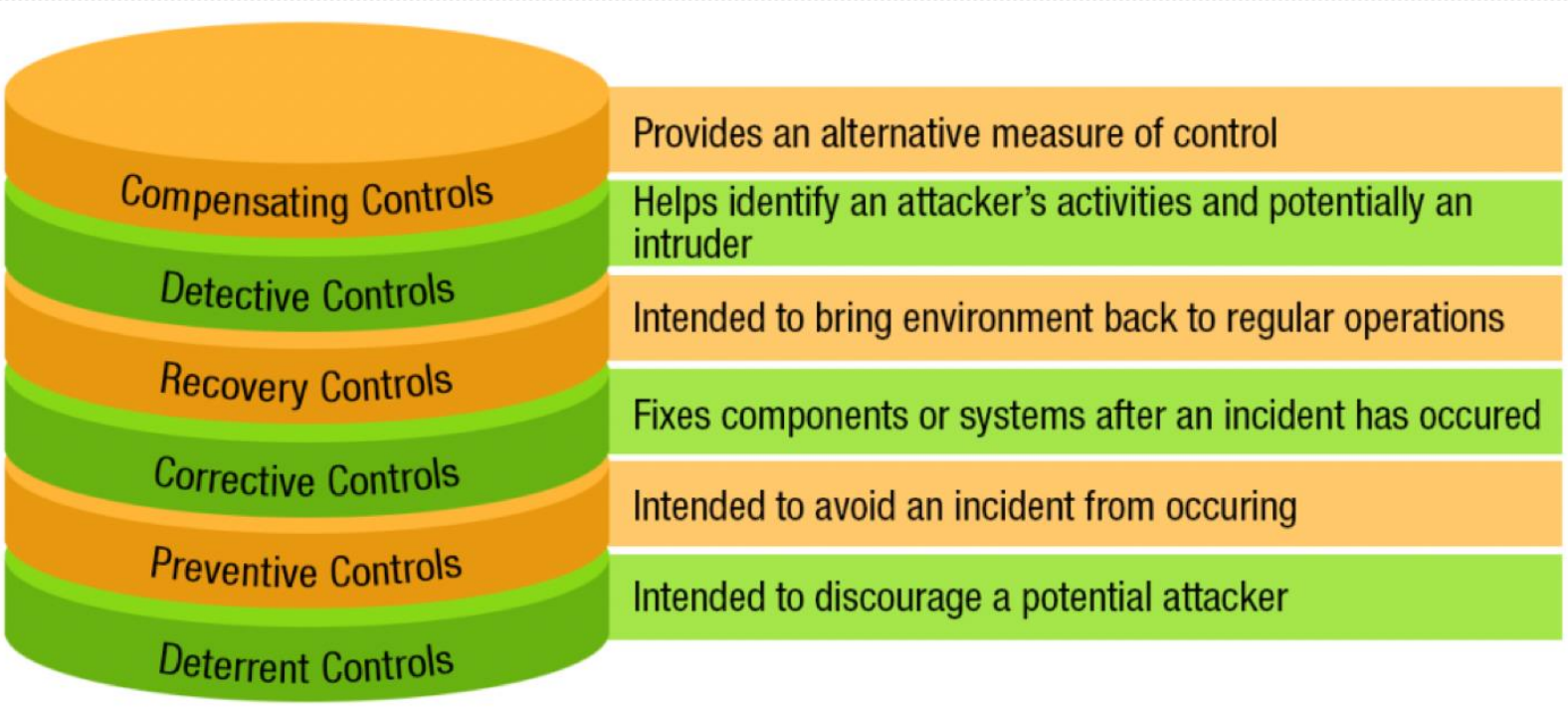
ABC Bank Example: Detailed Level View (2)

- Determine the impact more specifically
  - Exposure ratings for loss of integrity, confidentiality and availability
  - Exposure Factor: the extend of damage to the asset (100%-20%, adjust accordingly to your organization)
  - Impact Class Value for asset class
  - Impact = Impact Class Value * Exposure Factor

Risk Mitigation



Control Categories for Security Risk Mitigation



ABC Bank Example:

- The following represents a sample list of primary controls for the “LAN host compromise” from ABC Bank Example exercise:
  - Financial Advisor can only access accounts they own; thus the exposure is less than 100% (preventive)
  - Email notices to patch or update hosts are proactively sent to all users. (preventive)
  - The status of antivirus and security updates are measured on the LAN every few hours. This control reduces the time window when LAN hosts are vulnerable to attack. (detective/corrective)

Control Effectiveness

Control Effectiveness Question	Value	Description
Is accountability defined and enforced effectively?	0 (yes)	Policy creation and host compliance accountability are well defined.
Is awareness communicated and followed effectively?	0 (yes)	Regular notifications are sent to users and general awareness campaigns are conducted.
Are processes defined and practiced effectively?	0 (yes)	Compliance measurement and enforcement is documented and followed.
Does existing technology or controls reduce threat effectively?	1 (no)	Existing controls still allow a length of time between vulnerable and patched.
Are current audit practices sufficient to detect abuse or control deficiencies?	0 (yes)	Measurement and compliance auditing are effective given current tools.
Sum of all control attributes:	1	

A Plan of Action & Milestones (POAM)

- A Plan Of Action & Milestones (POAM) should be part of the risk mitigation report to management.
  - The POAM is a tool to communicate to management on the proposed and actual completion of the implementation of the risk management strategies.
  - For each milestone, a target completion date and an actual completion date is listed.
- The POAM is a tool to communicate to management, rather than a project management plan.

Cost-Benefit Analysis

- The cost-benefit analysis provides a consistent, comprehensive structure for identifying, scoping, and selecting the most effective and cost efficient mitigation solution to reduce risk to an acceptable level.
- Asset owner owns the cost-benefit analysis for the assets
- Security professional:
  - Recommend & evaluate control solutions
  - Defines the functional requirements for the controls for each risk
- Using a quantitative approach
  - Risk level before control (ALE before control)
  - Risk level after control (ALE after control)
  - Cost of control (annual cost of control)

Quantitative Asset Valuation

- The overall value in direct financial terms
  - An e-Commerce web site, 7 x 24, generating an average of $2000 per hour in revenue
  - The annual value of web site in terms of sales revenue = $2000 x 24 x 365 = $17,520,200
- The immediate financial impact of losing the asset
  - If the web site becomes unavailable for six hours
  - The calculated exposure = 6 /(24x365) = 0.0685%
  - Direct revenue loss = $17,520,000 x 0.0685% = $12000
- The indirect business impact of losing the asset
  - The company estimates that it would spend $10,000 on advertising to counteract the negative publicity from such an incident. Additionally, the company also estimates a loss of 1% of annual sales, or $175,200.
  - Total indirect loss = $175,200 + $10,000 = $185,200

Determining the Single Loss Expectancy (SLE)

- SLE is the total amount of revenue that is lost from a single occurrence of the risk.
- SLE is similar to the impact of a qualitative risk analysis.
- SLE = Asset Value x the Exposure Factor (EF), where EF represents the percentage of loss that a realized threat could have on a certain asset.

Example: *If a company has an asset value of $150,000, and a fire results in damages worth an estimated 25% of its value.*
SLE = $150,000 x 25% = $37,500.

Determining the Annual Rate of Occurrence (ARO)

- ARO is the number of times that you reasonably expect the risk to occur during one year.
- Making these estimates is very difficult, there is very little actuarial data available.
- To estimate the ARO, draw on your past experience and consult security risk management experts and consultants.
- ARO is similar to the probability (or likelihood) of a qualitative risk analysis (ranges from 0 to 100%)

Determine the Annual Loss Expectancy (ALE)

- ALE is total amount of money that your organization will lose in one year if nothing is done to mitigate the risk.
- ALE = SLE x ARO
- ALE provides a value that your organization can work with to budget what it will cost to establish controls or safeguards to prevent this type of damage.

Example: *if a fire at the same company results in $37,500 in damages, and the probability or ARO value of 0.1 (indicating once in ten years). Then the ALE value = $37,500 x 0.1 = $3,750*

Determining Cost of Controls

- It requires accurate estimates on how much acquiring, testing, deploying, operating and maintaining each control would cost.
  - Buying or developing the control solution
  - Deploying and configuring the control solution
  - Maintaining the control solution
  - Communicating new policies or procedures related to the new control to users
  - Training users and IT staff on how to use and support the control
  - Monitoring controls
  - Contending with the loss of convenience or productivity that the control might impose.

Return on Security Investment (ROSI)

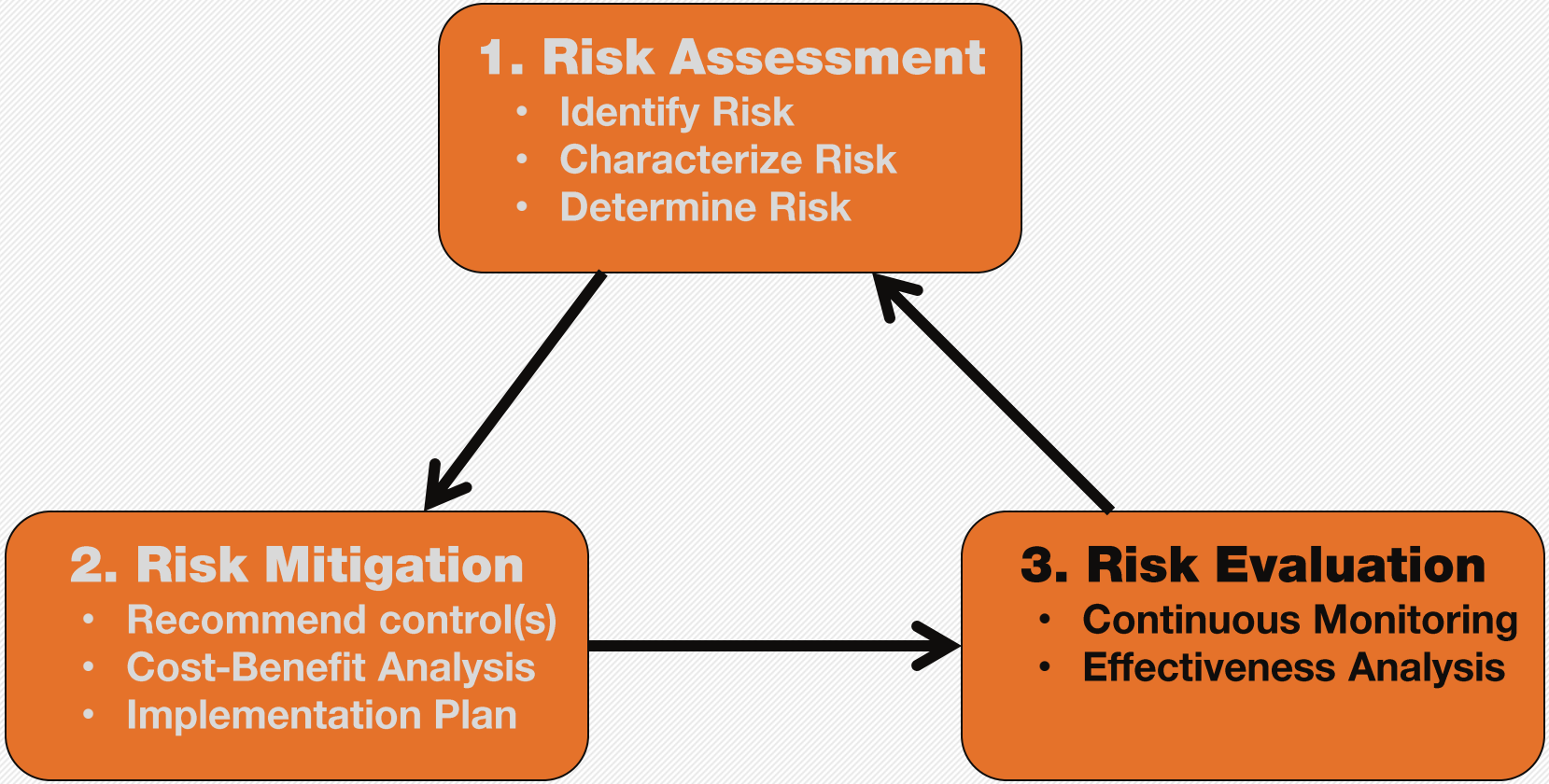
- ROSI =

  (ALE before control) –
  (ALE after control) –
  (annual cost of control)

- ROSI is cost-benefit analysis, to demonstrate that the cost of implementing the controls can be justified by the reduction in the level of risk.

  Example: *the ALE of the threat of an attacker bringing down a web server is $12,000, and after the suggested safeguard is implemented, the ALE is valued at $3000. The annual cost of maintenance and operation of the safeguard is $650.*
  So the ROSI = $12,000-$3,000-$650 = $8,350

Risk Evaluation



Key Success Factors for Risk Management

- Keep the risk assessment process as simple as possible
  - Strike a balance between granularity for risk assessment and the amount of efforts required to calculate risks
- Never refer the risk management program as “my program”
  - Assemble a right team with right mixture of expertise
- Focus on “the business needs” not “the technology excellence”
  - The primary goal of risk management program is to support business decision making
- Tailor the basic risk management principles to your organization context
  - Avoid discussing how to address risks before you have decided whether the risk is important.