جامعة الامير سلطان
PRINCE SULTAN
UNIVERSITY
1998

Risk Assessment Approaches

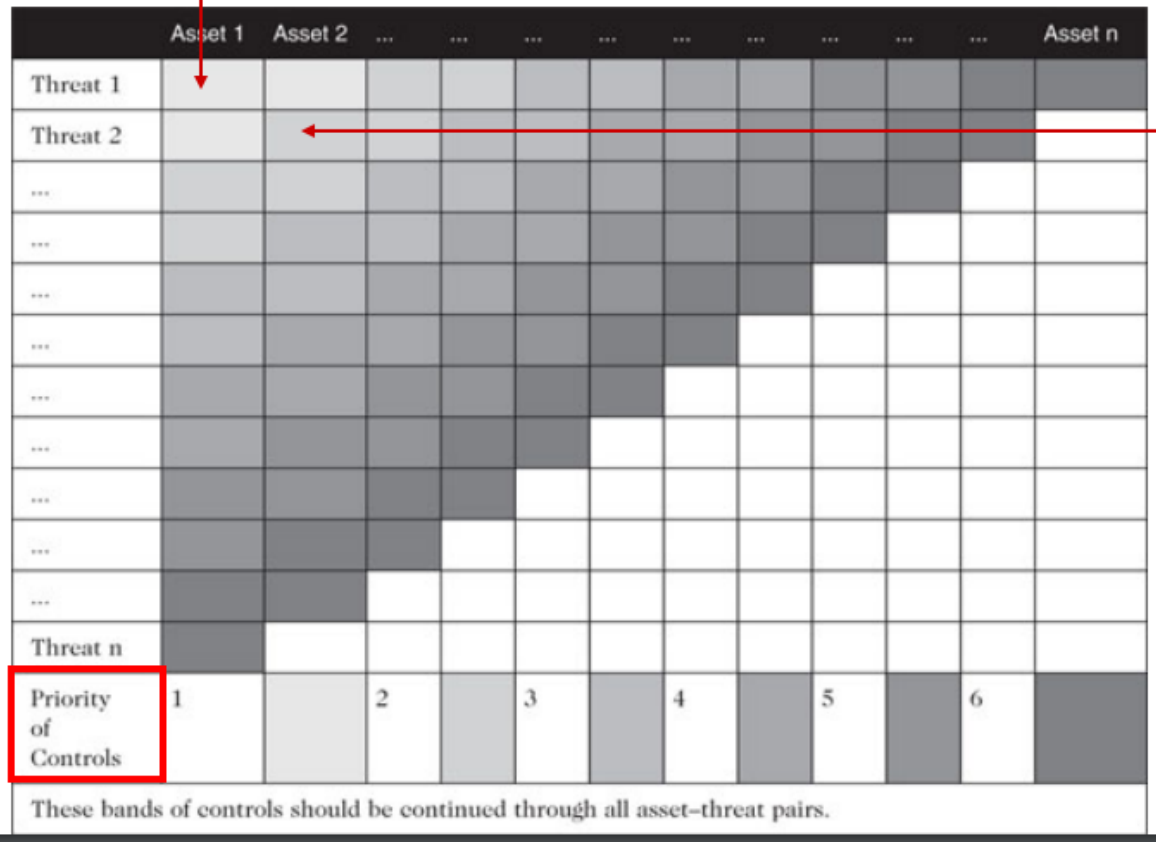
CYS403

جامعة الامير سلطان
Prince Sultan University

- CLO 2: Synthesize the principles of cyber security risk management and a framework of components: identification, protection, detection, response and recovery.
- CLO 3: Develop a working knowledge of types of policy, how policy is created, how to implement and manage policy, measurement practices, and audit of policy

TVA worksheet

If one or more vulnerabilities exist between T1 and A1, they can be categorized as:
T1V1A1 – Vulnerability 1 that exists between Threat 1 and Asset 1
T1V2A1 – Vulnerability 2 that exists between Threat 1 and Asset 1, …



If intersection between T2 and A2 has no vulnerability, the risk assessment team simply crosses out that box.

Class Activity

- Check LMS

- Quiz will be next Sunday 13/09/2026

What is next?

- Risk assessment: Quantitative OR Qualitative

Risk assessment

- Risk assessment is performed to identify the most serious risks.
- There are two primary methods used to create a risk assessment,
  - Quantitative: calculating the monetary values with predefined formulas.
  - Qualitative: uses values/words assigned to the probability of a risk occurring and the impact of a risk if it occurs.

Importance of Risk assessment

- Risk assessments are an important part of the risk management process.
- Without an RA, it becomes difficult to determine which systems should be protected.
- It also remains unclear how to protect them. However, an RA will help you identify the most important systems to protect.
- It will also give you insight into what controls will provide the most value.

Risk assessment

- After identifying threats and vulnerabilities, and asset value.
  - It is necessary to know the likelihood and impact of each threat on the assets.
  - Based on that we shall prioritize these risks to know which risks must be treated first.

Quantitative risk assessment example

EVENT	LIKELIHOOD (A)	IMPACT (B)	RISK FACTOR (A x B)
Fire in data center	0.7	0.9	0.63
Loss of power	0.5	0.8	0.40
Staff illness	0.6	0.5	0.30
Hurricane	0.4	0.9	0.36
Water leak	0.3	0.5	0.15
Employee forgot to log off	0.8	0.3	0.24

Risk assessment

- RA is a continuous process.
- RA should be conducted
  - **When evaluating risk in SDLC, Project initiation, startup time of company, etc.**
  - **When evaluating a security control: during the periodic monitoring.**
  - **After control implemented: to ensure its suitability and functionality.**

Critical Components of a Risk Assessment

[1]. Scope.

[2]. Critical areas

[3]. Team

Critical Components of a Risk Assessment

[1]. Scope: identifies the boundary of the RA (what are included and what are not included).

- the scope of the RA helps to keep the RA on track.

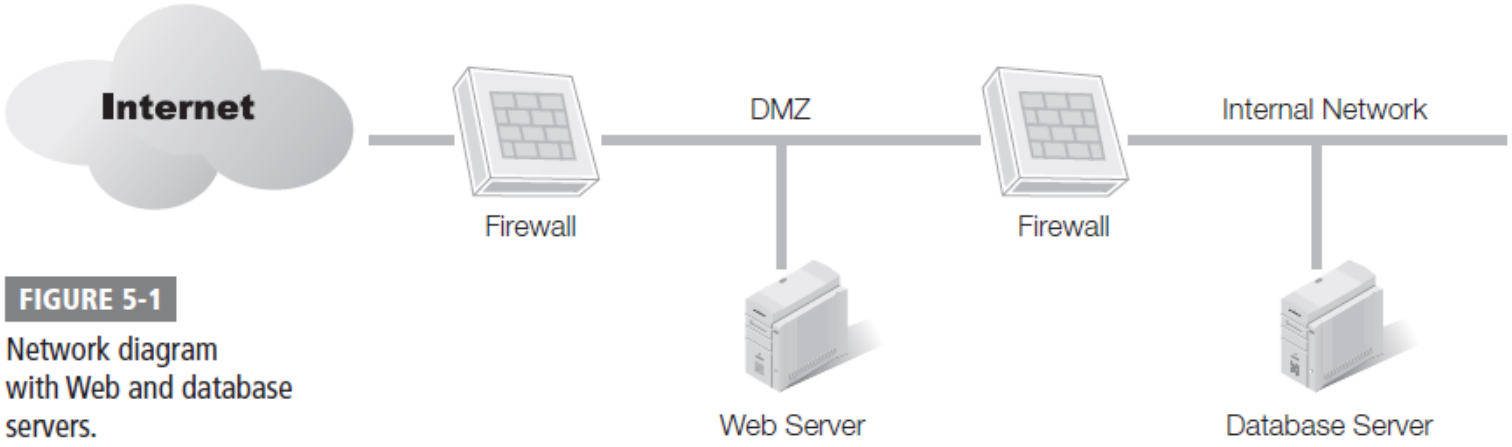


FIGURE 5-1
Network diagram with Web and database servers.

Critical Components of a Risk Assessment

[2]. critical areas: The RA also identifies critical areas that should be included.

- For example, a scope could include a Web server, a database server, and a firewall.
  - Web server: SPOF, OS update batch,
  - Database server: only data that are exchanged with webserver.
  - Firewall: inspecting all the traffic
- This helps the RA team focus only on what's important.

Critical Components of a Risk Assessment

[3]. Team: RA team personnel should not be the same people who are responsible for correcting deficiencies.

- This helps avoid a conflict of interest.
- But, the input from the responsible people is very important.

Types of Risk assessment

- Quantitative: This is an objective method.
  - It uses numbers such as actual dollar values.
  - Require a significant amount of data, which needs a long time to gather.
  - a simple math problem with the use of formulas.

Types of Risk assessment

- Qualitative—This is a subjective method.
  - It uses relative values based on opinions from experts.
  - Experts provide their input on the probability and impact of a risk. A qualitative RA can be completed rather quickly.

Quantitative Risk Assessments

- Some of the key terms associated with quantitative risk assessments are:
  - **Single loss expectancy (SLE)**—The total loss expected from a single incident.
    - An incident occurs when a threat exploits a vulnerability. The loss is expressed as a dollar value such as $5,000. It includes the value of hardware, software, and data.
  - **Annual rate of occurrence (ARO)**—The number of times an incident is expected to occur in a year.
    - If an incident occurred once a month in the past year, the ARO is 12. Assuming nothing changes, it's likely that it will occur 12 times next year.

Quantitative Risk Assessments

- Some of the key terms associated with quantitative risk assessments are:
  - **Annual loss expectancy (ALE)**—The expected loss for a year. ALE is calculated
    - by multiplying SLE X ARO. Because SLE is a given in a dollar value, ALE is given as a dollar value. For example, if the SLE is $5,000 and the ARO is 12, the ALE is $60,000.
  - **Safeguard value**—This is the cost of a control. Controls are used to mitigate risk.
    - For example, antivirus software could have an average cost of $50 for each computer. If you have 100 computers, the safeguard value is $5,000.

Class activity

- Consider this scenario: A company issues laptop computers to employees. The value of each laptop is $2,000. This includes the hardware, software, and data. About 100 laptops are being used at any time. In the past two years, the company has lost an average of one laptop per quarter. These laptops were stolen when systems were left unattended.

With this information, can you answer these questions?

- What's the SLE? ($2000)
- What's the ARO? (4)
- What's the ALE? ($8000)

Class activity

- The company could purchase hardware locks for the laptops in bulk at a cost of $10 each. The safeguard value is $10 * 100 laptops, or $1,000. It's estimated that if the locks are purchased, the ARO will decrease from 4 to 1. Should the company purchase these locks?
  - SLE?
  - ARO?
  - ALE?
  - Control cost?

Class activity

- The company could purchase hardware locks for the laptops in bulk at a cost of $10 each. The safeguard value is $10 * 100 laptops, or $1,000. It's estimated that if the locks are purchased, the ARO will decrease from 4 to 1. Should the company purchase these locks?
  - SLE=$2000
  - ARO=1*4=4
  - ALE= 2000*4=8000
  - Control cost= 1000

Class activity

- The company could purchase hardware locks for the laptops in bulk at a cost of $10 each. The safeguard value is $10 * 100 laptops, or $1,000. It's estimated that if the locks are purchased, the ARO will decrease from 4 to 1. Should the company purchase these locks?
  - Current ALE =$8,000 (ARO of 4 * $2,000) (before the control)
  - ARO with control =1
  - ALE with control = $2,000 (ARO of 1 * $2,000) (after the control)
  - Savings with control = ALE(before) –ALE (after)- Control Cost = 8000-2000-1000=5000.

Quantitative Risk assessment

- Benefits:
  - Mathematical calculation with accurate objective results.
  - Verifiable facts without debate.
  - Can be automated (e.g. excel sheet).
- Limitations:
  - accurate data isn't always available.
  - Hard to ensure that people use the control as expected

Qualitative Risk Assessments

- it determines the level of risk based on the probability and impact of a risk (Experts opinions).
  - **Probability**—The likelihood that a threat will exploit a vulnerability.
    - The risk occurs when a threat exploits a vulnerability.
    - A scale can be used to define the probability that a risk will occur.
      - word values such as Low, Medium, or High.
      - percentage values to these words. (e.g. 10% means low, 100% high)
  - **Impact**—The negative result if a risk occurs. Impact is used to identify the magnitude of a risk (amount of loss).
    - word values such as Low, Medium, or High.
    - percentage values to these words. (e.g. 10% means low, 100% high)

Qualitative Risk Assessments

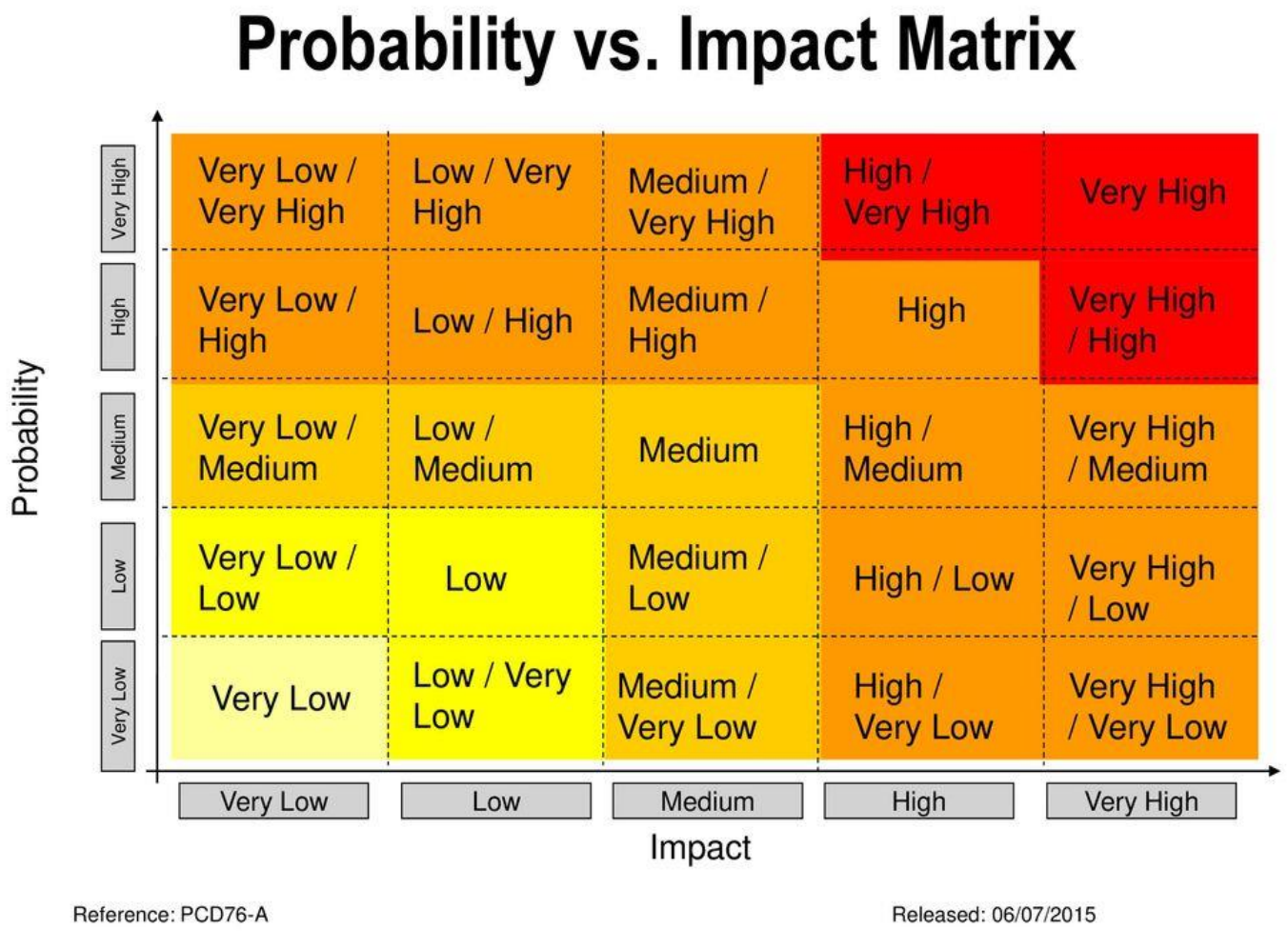
TABLE 5-1 Probability scale.

PROBABILITY	DESCRIPTION
Low	It is unlikely the risk will occur. Threats are not active. Vulnerabilities are either not known or have been mitigated. Low equates to a value of 10 percent.
Medium	There is a moderate chance the risk will occur. It has occurred in the past, but mitigation controls have reduced recent occurrences. Medium equates to a value of 50 percent.
High	There is a high probability the risk will occur. It has occurred in the past and will occur again if not mitigated. High equates to a value of 100 percent.

TABLE 5-2 Impact scale.

IMPACT	DESCRIPTION
Low	If the risk occurs, it will have minimal impact on the company. The attack will not impact any critical data or systems.
Medium	If the risk occurs, it will have a moderate impact on the company. It may affect critical data or systems, but not to a large extent.
High	If the risk occurs, it will have a high impact on the company. It will affect critical data or systems and cause substantial losses.

Qualitative Risk Assessments



Qualitative Risk Assessments

Risk level= Probability*Impact

TABLE 5-3 Qualitative analysis survey results.

CATEGORY	PROBABILITY	IMPACT	RISK LEVEL (1 to 100)
DoS attack	100	100	100 (1.0 × 100)
Web defacing	50	90	45 (0.5 × 90)
Loss of data from unauthorized access	30	10	3 (0.3 × 10)
Loss of Web site data due to hardware failure	30	27	9 (0.3*27)

Risk Assessments Report

Sample Risk Assessment Outline

A risk assessment ends with a report. This report can then be used by management to decide what controls to implement. The following is a list of topics that are commonly included in a risk assessment report:

- **Introduction**—The introduction provides the purpose and scope of the risk assessment. It includes descriptions about the components, users, and locations for the system considered in the RA.
- **Risk assessment approach**—This section identifies the approach used to complete the RA. It includes details on how the data was collected and who was involved. If a qualitative approach is used it will describe the risk scale.
- **System characterization**—This section provides more details on the system. It could include details on the hardware, software, or network connections. It may include diagrams to graphically show the assessed system.
- **Threat statement**—This section lists potential threats, threat sources, and threat actions. For example, one threat may be an attacker launching a denial of service (DoS) attack on an Internet facing server.
- **Risk assessment results**—Results can be listed as vulnerability/threat pairs representing a risk. The risk is described with existing security controls. The likelihood of the risk occurring with current controls is listed. How the risks are described depends on which analysis is used. A quantitative method uses terms such as SLE, ARO, and ALE. A qualitative method identifies probability and impact based on a defined scale. All of this data is supported with discussions identifying how the result was obtained.
- **Control recommendations**—A list of recommended safeguards or controls is provided. This list can include comments on the effectiveness of the controls. A quantitative method will often be accompanied by a CBA for each control. qualitative method will often rank the effectiveness of the control.
- **Summary**—The summary can be in one or more tables that summarize the results. This format makes it easy for management to see the highest risks based on the risk rating. It also makes it easy to approve any of the recommendations.

Risk Determination

- For the purpose of relative risk assessment:
  - Risk EQUALS
  - Likelihood of vulnerability occurrence
  - TIMES value (or impact)
  - MINUS percentage risk already controlled
  - PLUS an element of uncertainty

Risk = likelihood x value (impact) - %risk already controlled + element of uncertainty

Likelihood

- **Likelihood** is the probability that a specific vulnerability will be the object of a successful attack
- Assign numeric value:
  - number between 0.1 (low) and 1.0 (high), or a number between 1 and 100 (%)
- Zero not used since vulnerabilities with zero likelihood are removed from asset/vulnerability list

- **Information Asset A**
  - Value score (or impact) = 50
  - Has 1 vulnerability with likelihood of 1.0 and no current controls
  - Our assumptions and data are 90% accurate
- **Information Asset B**
  - Value score (or impact) = 100
  - Has 2 vulnerabilities
    - Vulnerability 2 with likelihood of 0.5 and current controls addressing 50% of its risk
    - Vulnerability 3 with likelihood of 0.1 and no current controls addressing 50% of its risk
  - Our assumptions and data are 80% accurate

Example (1)

- **Information Asset A**
  - Asset value=50
  - Has 1 vulnerability
    - Likelihood =1.0
    - no current controls
    - 90% accurate → uncertainty =1-0.9=0.1 or 10%

Risk = (50 x 1.0) – 0% x (50 x 1.0) + 10% (50 x 1.0)

= 50 – 0 + 5

= 55

– Risk EQUALS

– Likelihood of vulnerability occurrence

– TIMES value (or impact)

– MINUS percentage risk already controlled

– PLUS an element of uncertainty

Example (1 continued)

- **Information Asset B**
  - Value score (or impact) = 100
  - Has 2 vulnerabilities
    - Vulnerability 2 with likelihood of 0.5 and current controls addressing 50% of its risk
  - Our assumptions and data are 80% accurate
- **Asset B Vulnerability 2**

Risk = (100 x 0.5) – 50% (100 x 0.5) + 20% (100 x 0.5)

Risk = 50 – 25 + 10

Risk = 35

– Risk EQUALS
– Likelihood of vulnerability occurrence
– TIMES value (or impact)
– MINUS percentage risk already controlled
– PLUS an element of uncertainty

Example (1 continued)

- Information Asset B
  - Value score (or impact) = 100
  - Has 2 vulnerabilities
  - Vulnerability 3 with likelihood of 0.1 and no current controls
  - Our assumptions and data are 80% accurate
- Asset B Vulnerability 3

= (100 x 0.1) – 0% (100 x 0.1) + 20% (100 x 0.1)

= 10 – 0 + 2

= 12

– Risk EQUALS
– Likelihood of vulnerability occurrence
– TIMES value (or impact)
– MINUS percentage risk already controlled
– PLUS an element of uncertainty

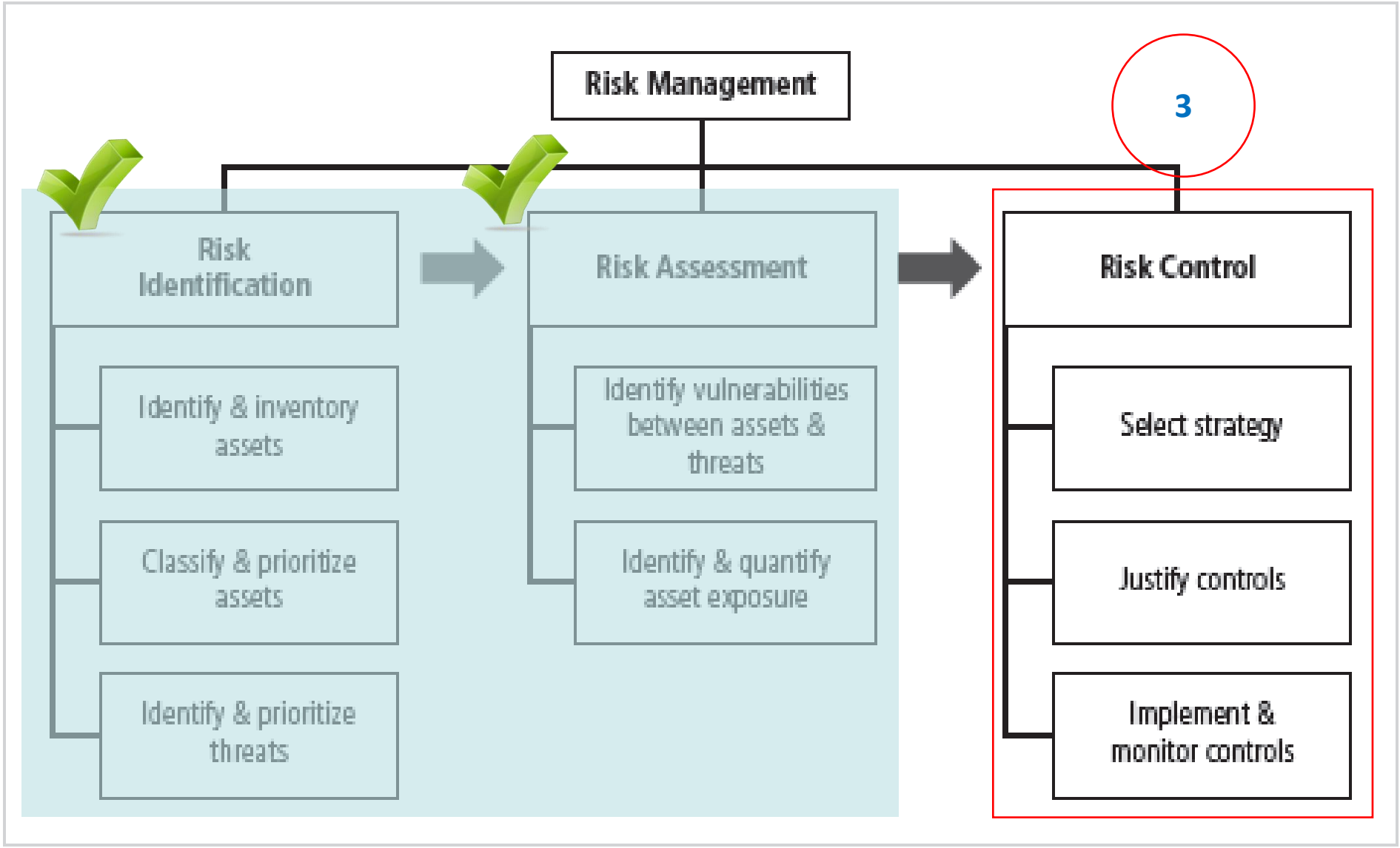
Documenting the Results of Risk Assessment

- Final summary comprised in ranked risk worksheet
- Ranked risk worksheet is initial working document for next step in risk management process: assessing and controlling risk

Ranked Risk Worksheet

Asset	Asset Impact or Relative Value	Vulnerability	Vulnerability Likelihood	Risk-Rating Factor
Customer service request via e-mail (inbound)	55	E-mail disruption due to hardware failure	0.2	11
Customer order via SSL (inbound)	100	Lost orders due to web server hardware failure	0.1	10
Customer order via SSL (inbound)	100	Lost orders due to Web server or ISP service failure	0.1	10
Customer service request via e-mail (inbound)	55	E-mail disruption due to SMTP mail relay attack	0.1	5.5
Customer service request via e-mail (inbound)	55	E-mail disruption due to ISP service failure	0.1	5.5
Customer order via SSL (inbound)	100	Lost orders due to Web server denial-of-service attack	0.025	2.5
Customer order via SSL (inbound)	100	Lost orders due to Web server software failure	0.01	1

Deliverable	Purpose
Information asset classification worksheet	Assembles information about information assets and their impact
Weighted criteria analysis worksheet	Assigns ranked value or impact weight to each information asset
Ranked vulnerability risk worksheet	Assigns ranked value of risk rating for each uncontrolled asset-vulnerability pair


Risk Management
3
Risk Identification
Identify & inventory assets
Classify & prioritize assets
Identify & prioritize threats
Risk Assessment
Identify vulnerabilities between assets & threats
Identify & quantify asset exposure
Risk Control
Select strategy
Justify controls
Implement & monitor controls