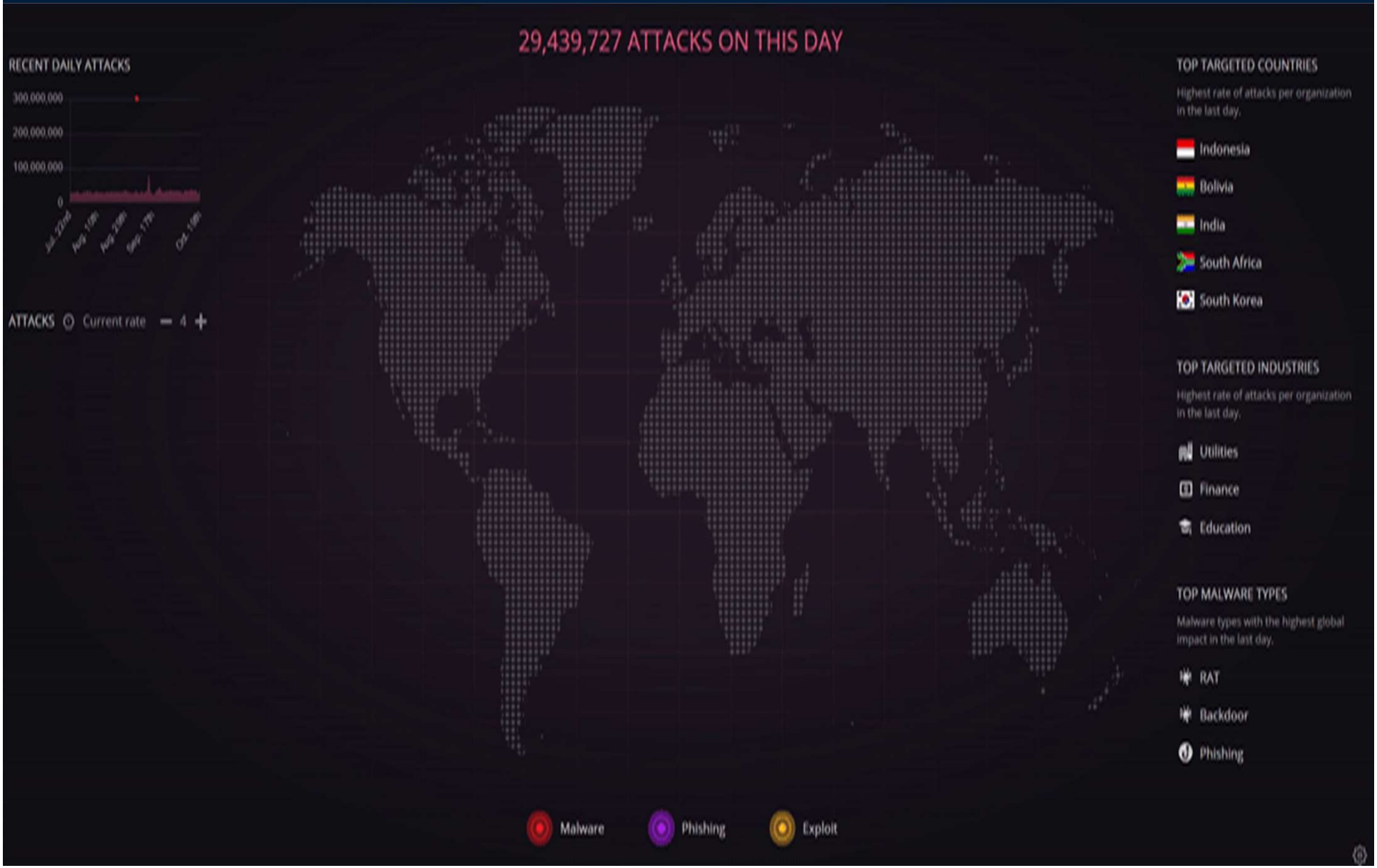
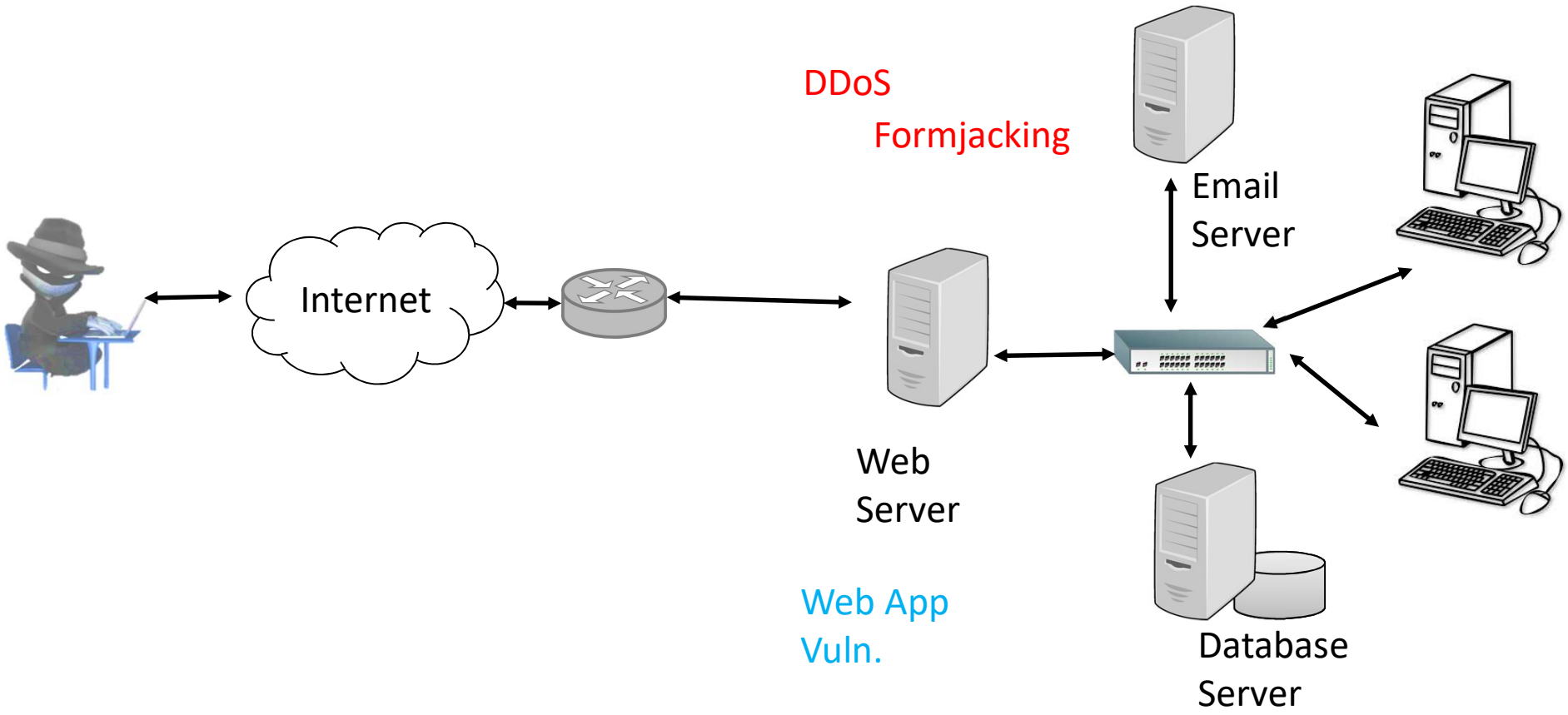
CMT116 Risk Assessment Methodologies



An Attack Scenario

Risk 1 The likelihood of a hacker taking advantage of a web application vulnerability to steal credit card info, resulting in a business loss.

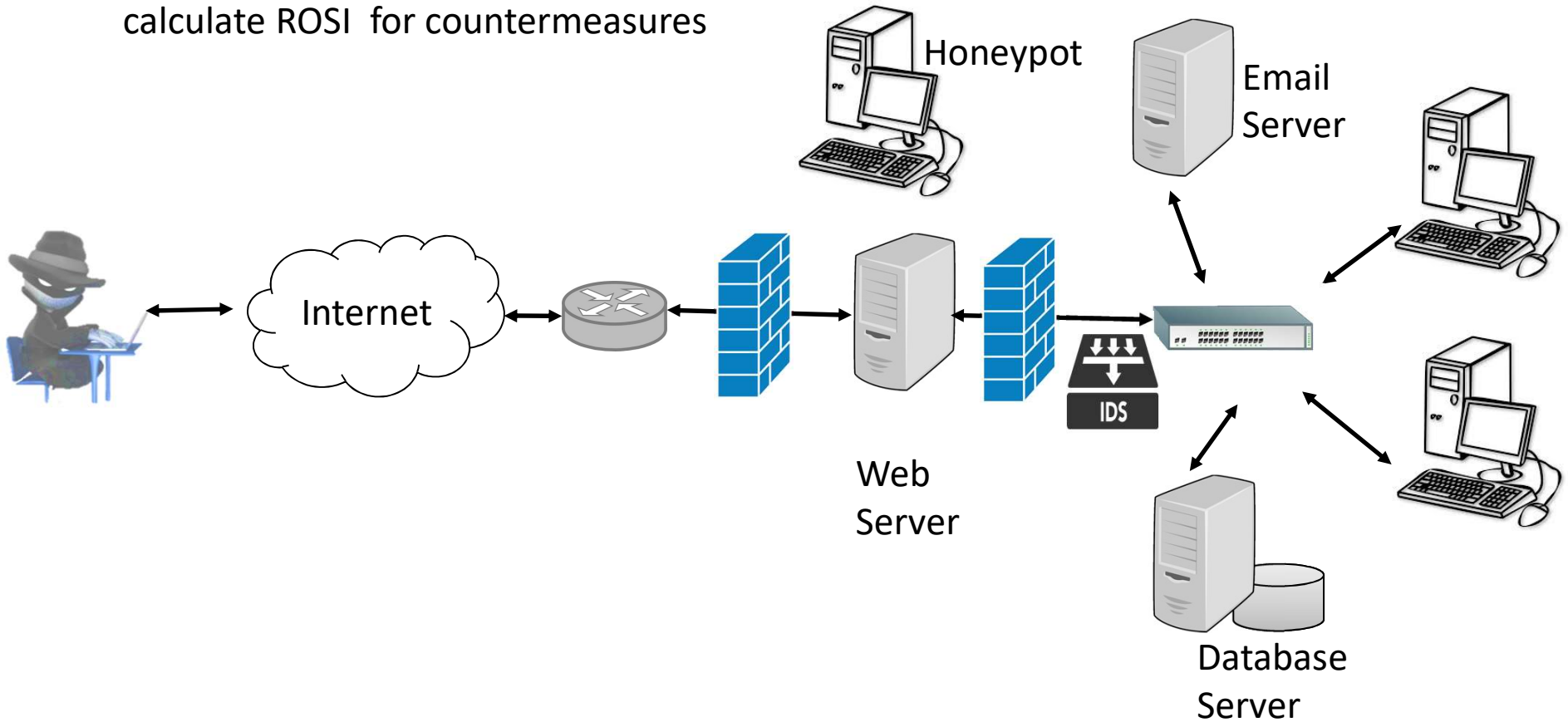


An Attack Scenario

Assess Risk – Quantitative to calculate the impact to business if credit card info is stolen, SLE, ALE.

Qualitative- A group of expert to identify the severity, probability and impact of a threat (Steal credit card info).

calculate ROSI for countermeasures



Prioritizing Risk- Quantitative

Asset	Threat	Single Loss Expectancy (SLE)	Annualized Rate of Occurrence (ARO)	Annualized Loss Expectancy (ALE)
Facility	Fire	$230,000	0.1	$23,000
Trade secret	Stolen	$40,000	0.01	$400
File server	Failed	$11,500	0.1	$1,150
Data	Virus	$6,500	1.0	$6,500
Customer credit card info	Stolen	$300,000	3.0	$900,000

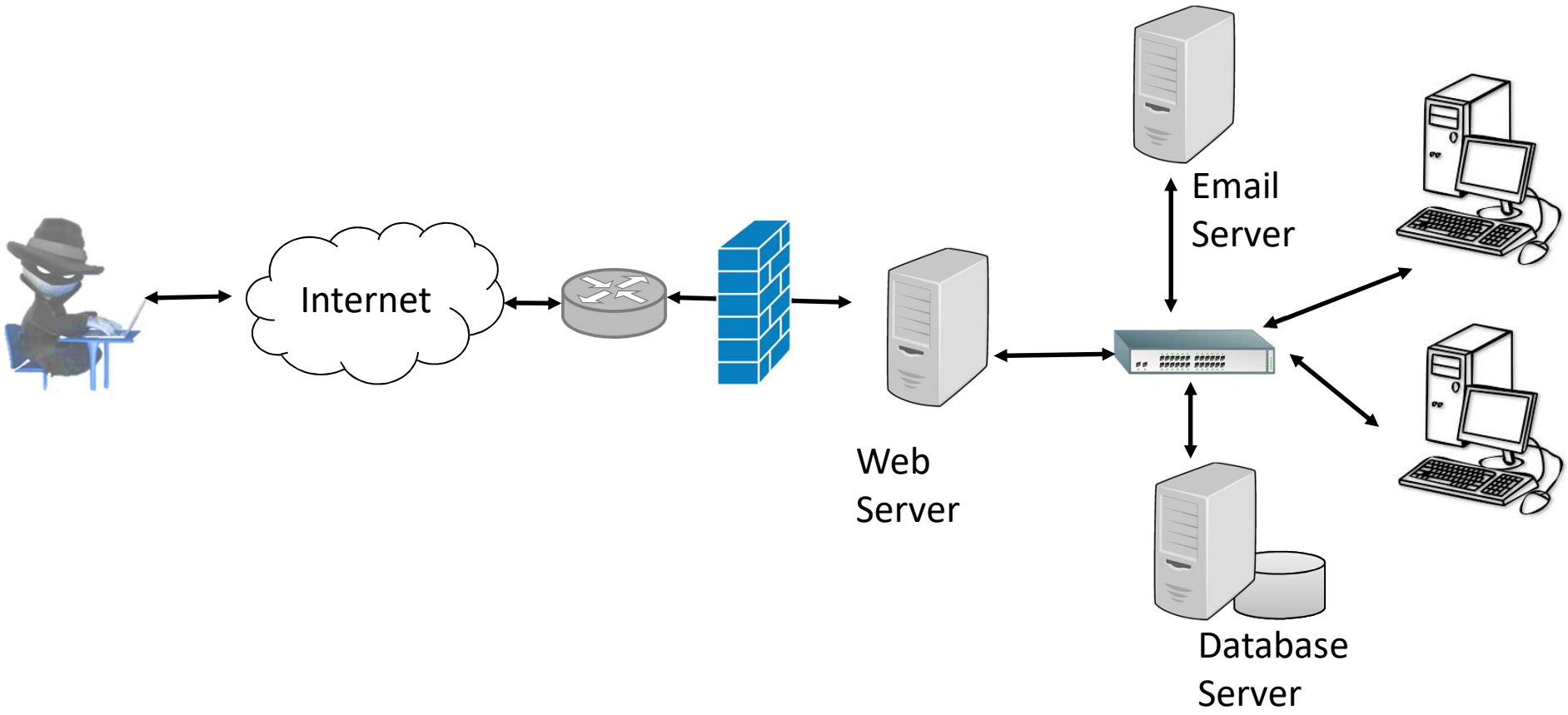
Risk management – Qualitative

Threat = Hacker Accessing Confidential Information	Severity of Threat	Probability of threat Taking Place	Potential Loss to the company	Effectiveness of a firewall	Effectiveness of a IDS
IT Manager	4	2	4	4	3
Database Administrator	4	4	4	3	4
Application Programmer	2	3	3	4	2
System Operator	3	4	3	4	2
Operational Manager	5	4	4	4	4
Results	3.6	3.4	3.6	3.8	3

Recommendation to CSO

An Attack Scenario

Handle Risk – Mitigate, Accept, Transfer or Avoid
If mitigate- Choose countermeasure, implement counter measure and monitor



Risk Assessment Methodologies

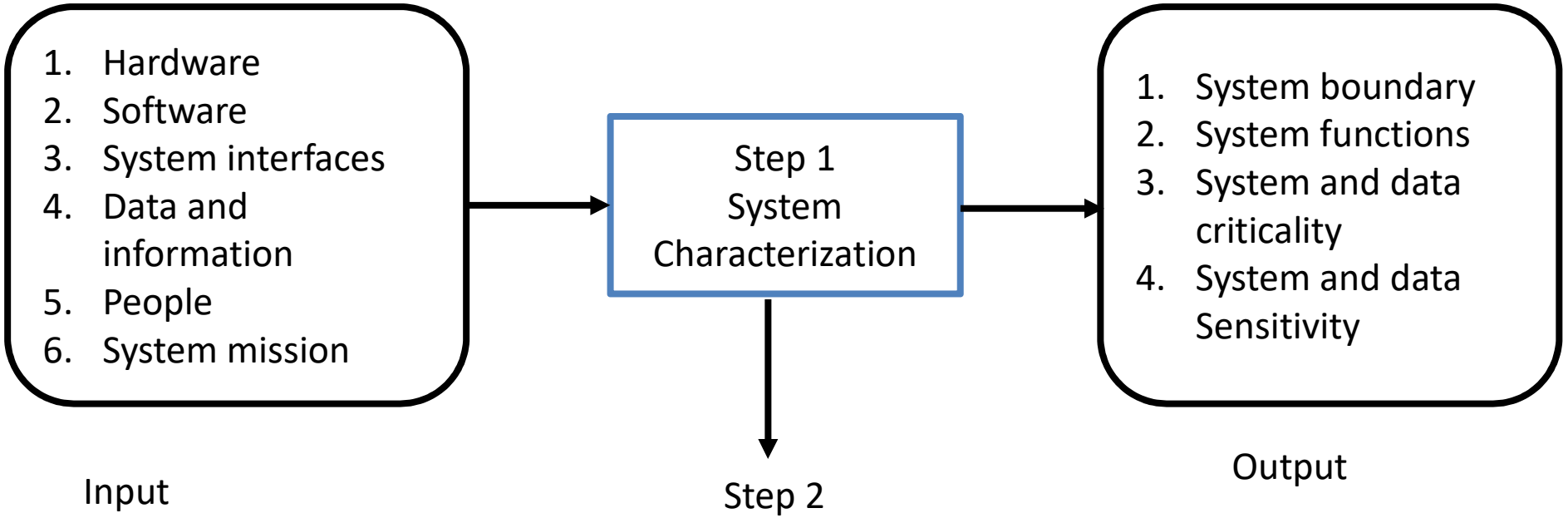
- Different Standards to assess risk
  - NIST 800-30
  - FRAP
  - OCTAVE
  - ISO/IEC 27005
  - AS/NZS 4360
  - CRAMM

NIST 800-30 Risk Management Guide for Information Technology Systems

It lays out the following steps

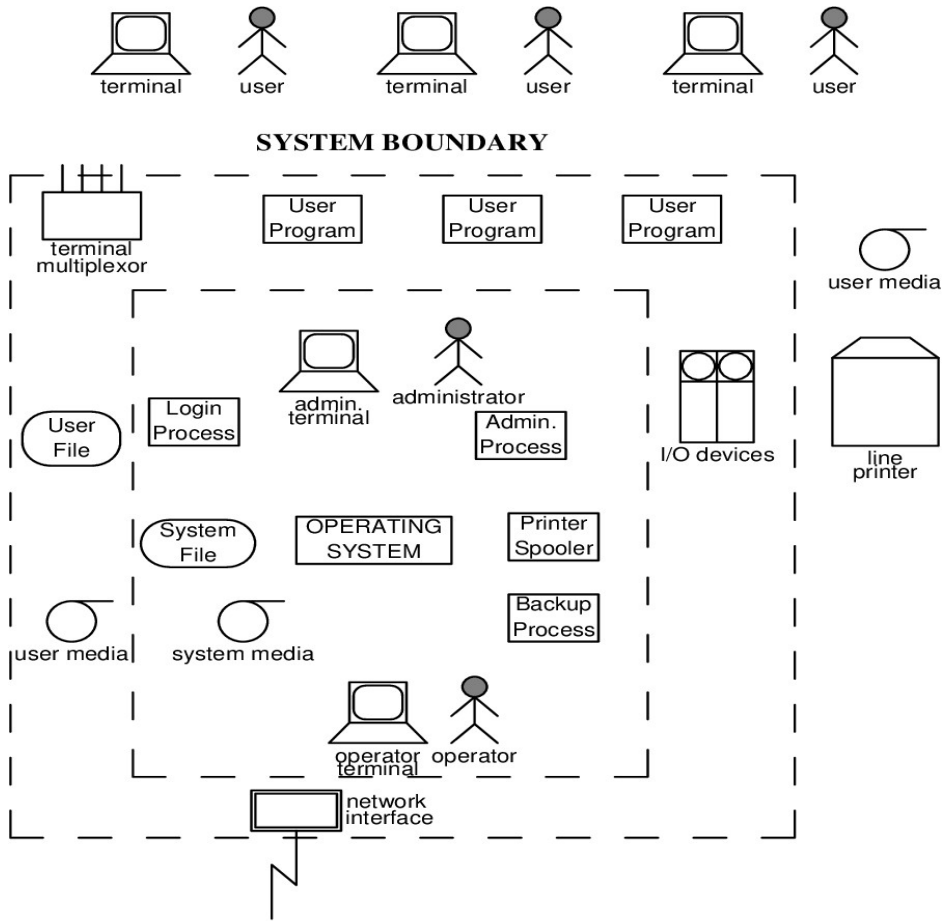
1. System characterization
2. Threat identification
3. Vulnerability identification
4. Control analysis
5. Likelihood determination
6. Impact analysis
7. Risk determination
8. Control recommendations
9. Results documentation

NIST 800-30 System characterization

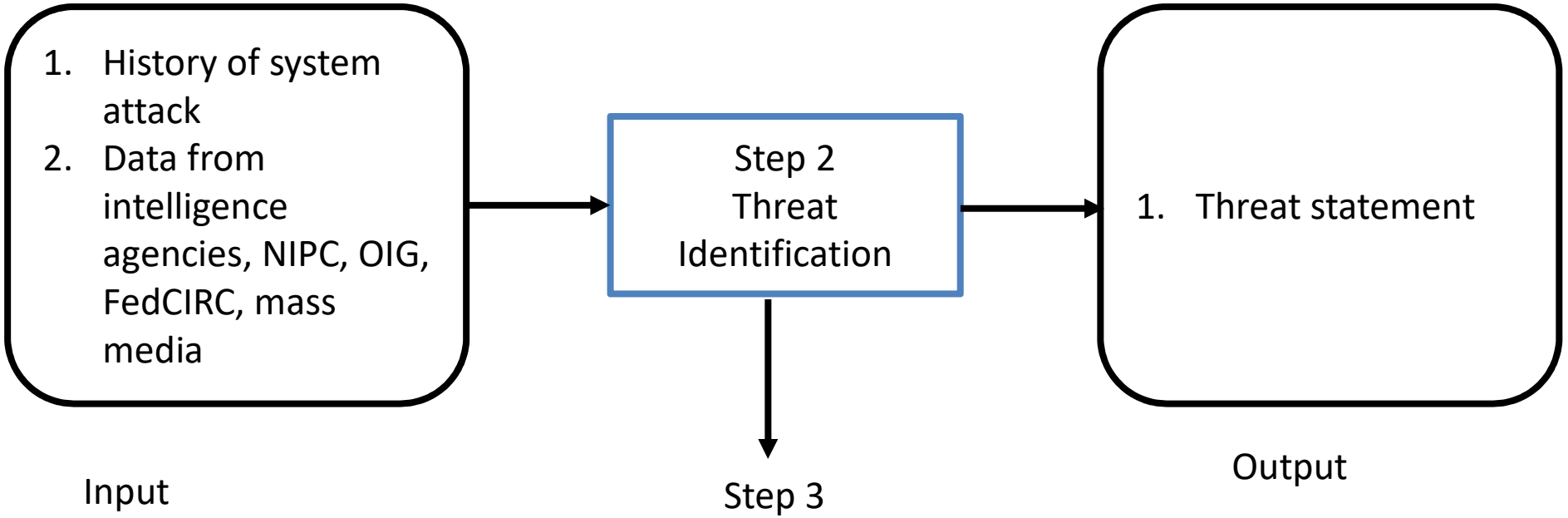


NIST 800-30 System characterization

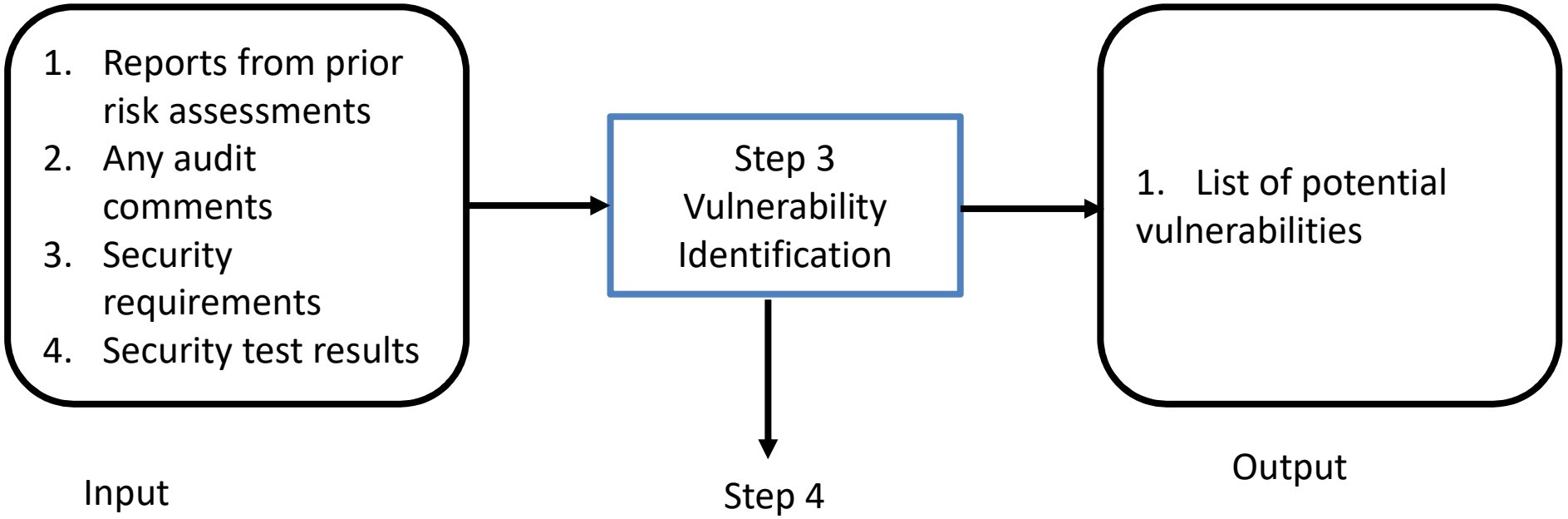
1. System boundary
2. System functions
3. System and data criticality
4. System and data Sensitivity



NIST 800-30 Threat Identification



NIST 800-30 Vulnerability Identification



NIST 800-30 Vulnerability Identification

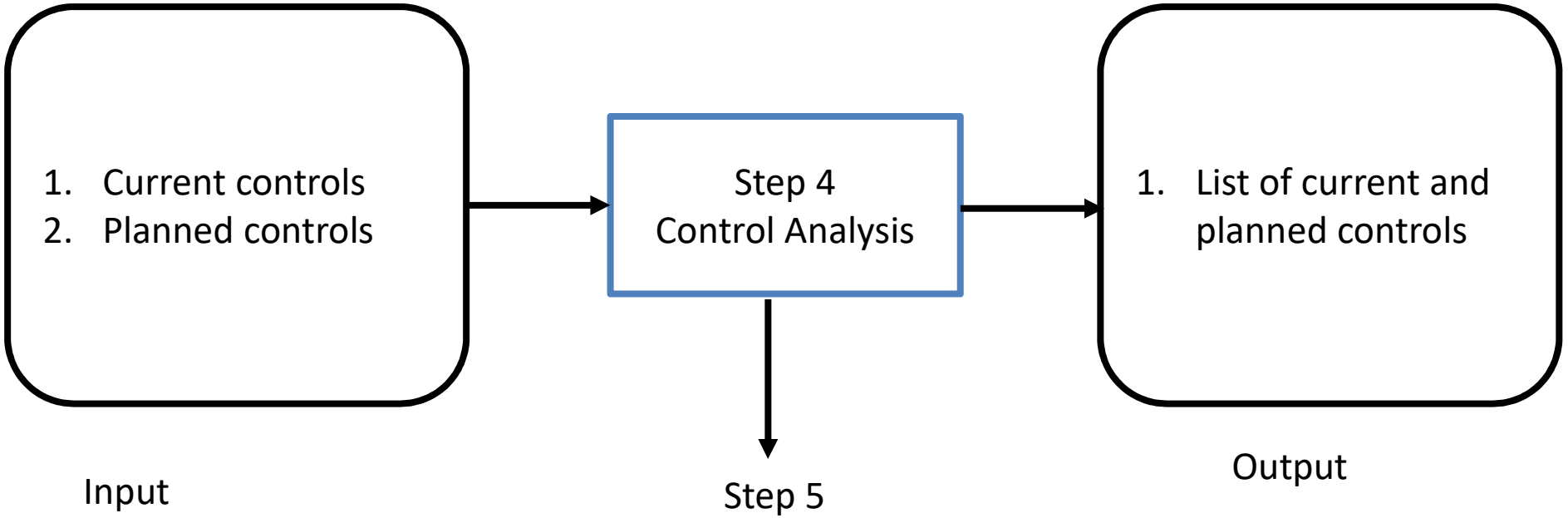
Sources

1. Security Focus (www.securityfocus.com) searchable databases of vulnerabilities and relevant news groups.
2. Incidents.org (www.incidents.org) - information on current threat activities.
3. Packet Storm (packetstormsecurity.org)
4. InfoSysSec (www.infosyssec.com)
5. SANS (www.sans.org)

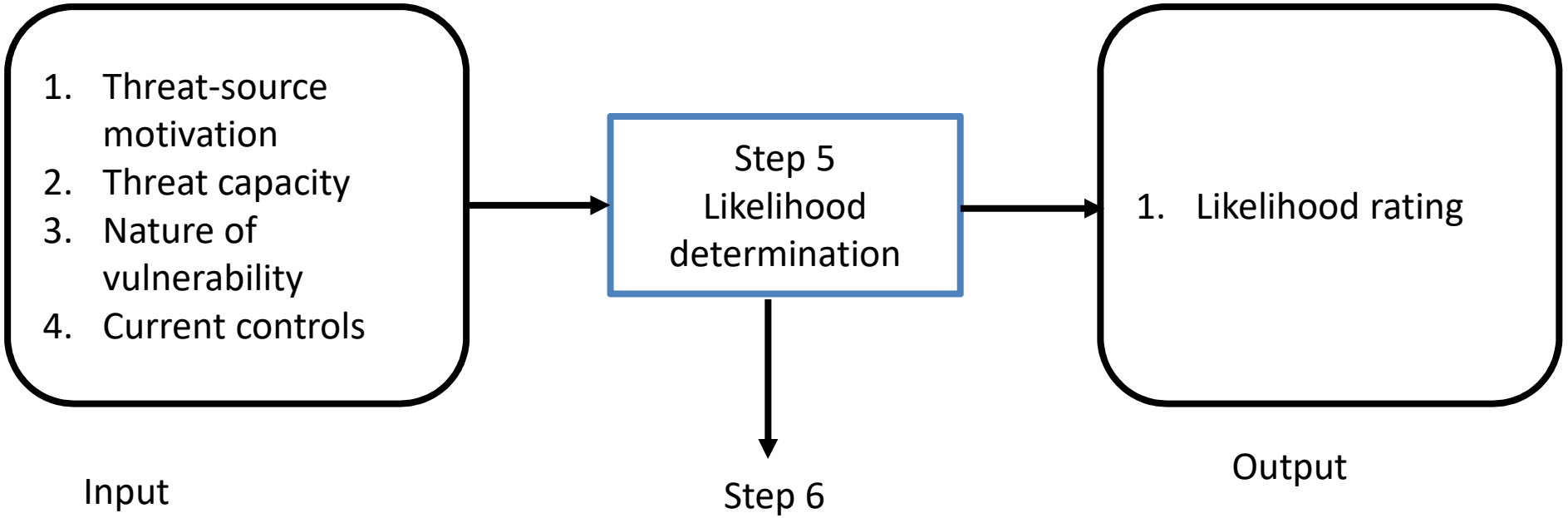
Security Test

1. Service pack levels
2. Port scanning
3. Services running
4. Wireless leakage
5. Operating system type
6. Intrusion detection testing
7. Network applications running
8. Physical location of the systems
9. Firewall testing
10. Access control permissions.
11. Network Surveying

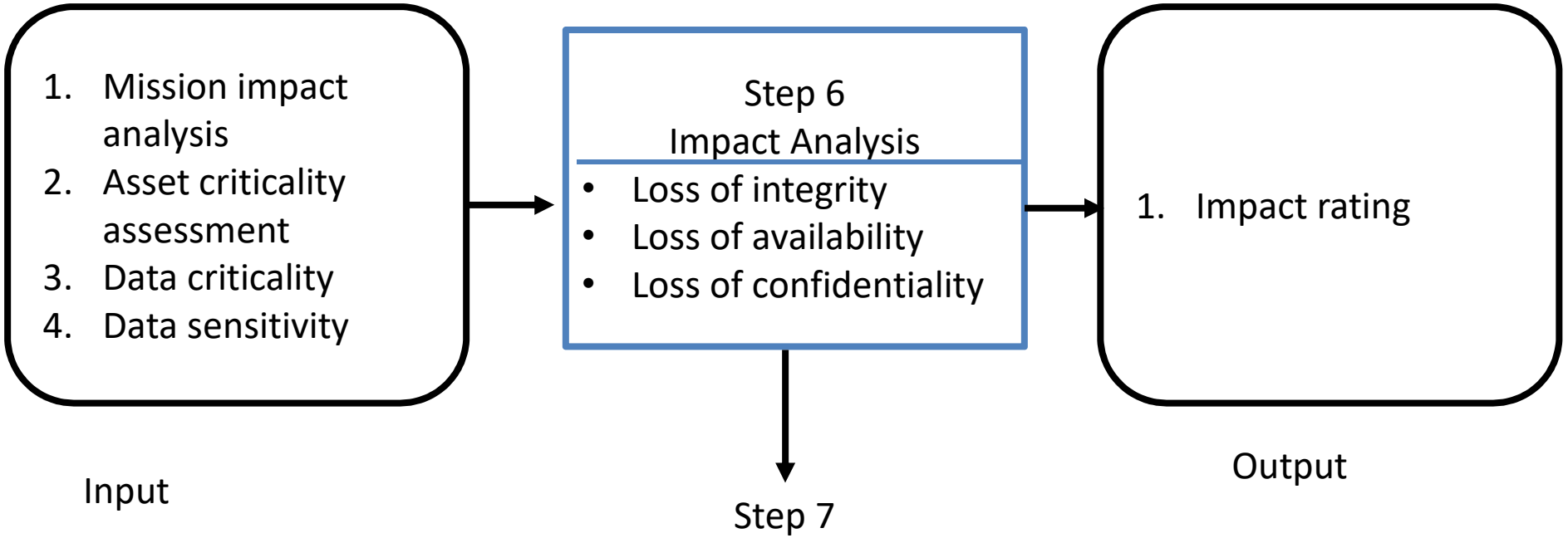
NIST 800-30 Control Analysis



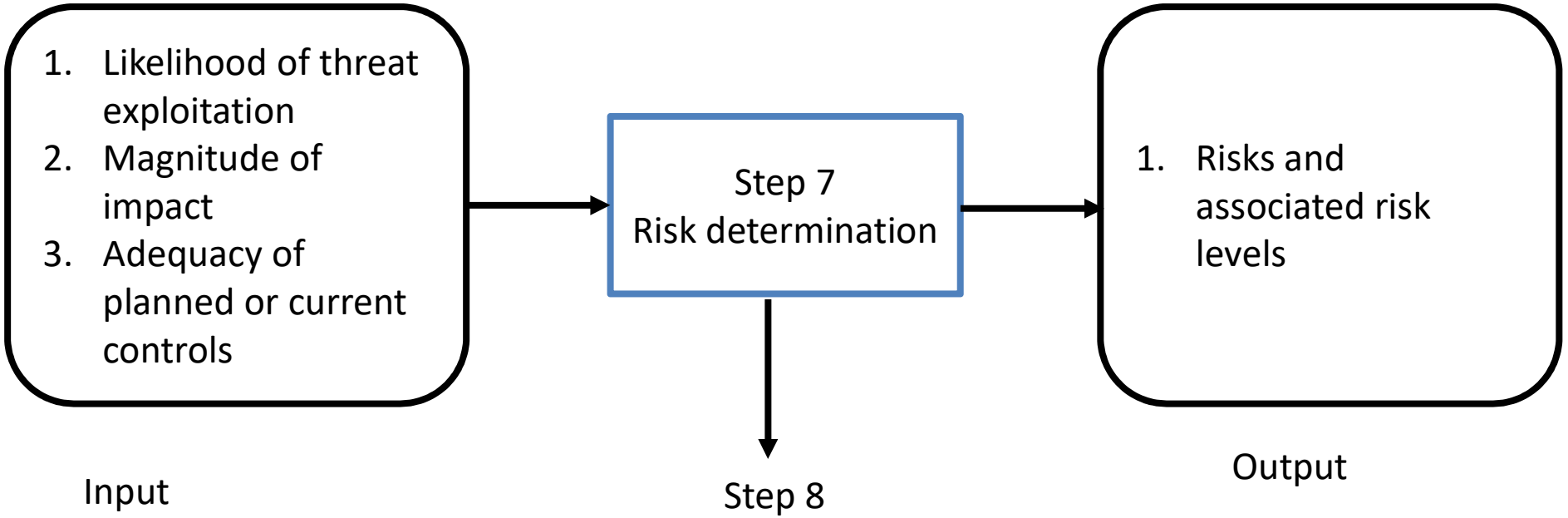
NIST 800-30 Likelihood Determination



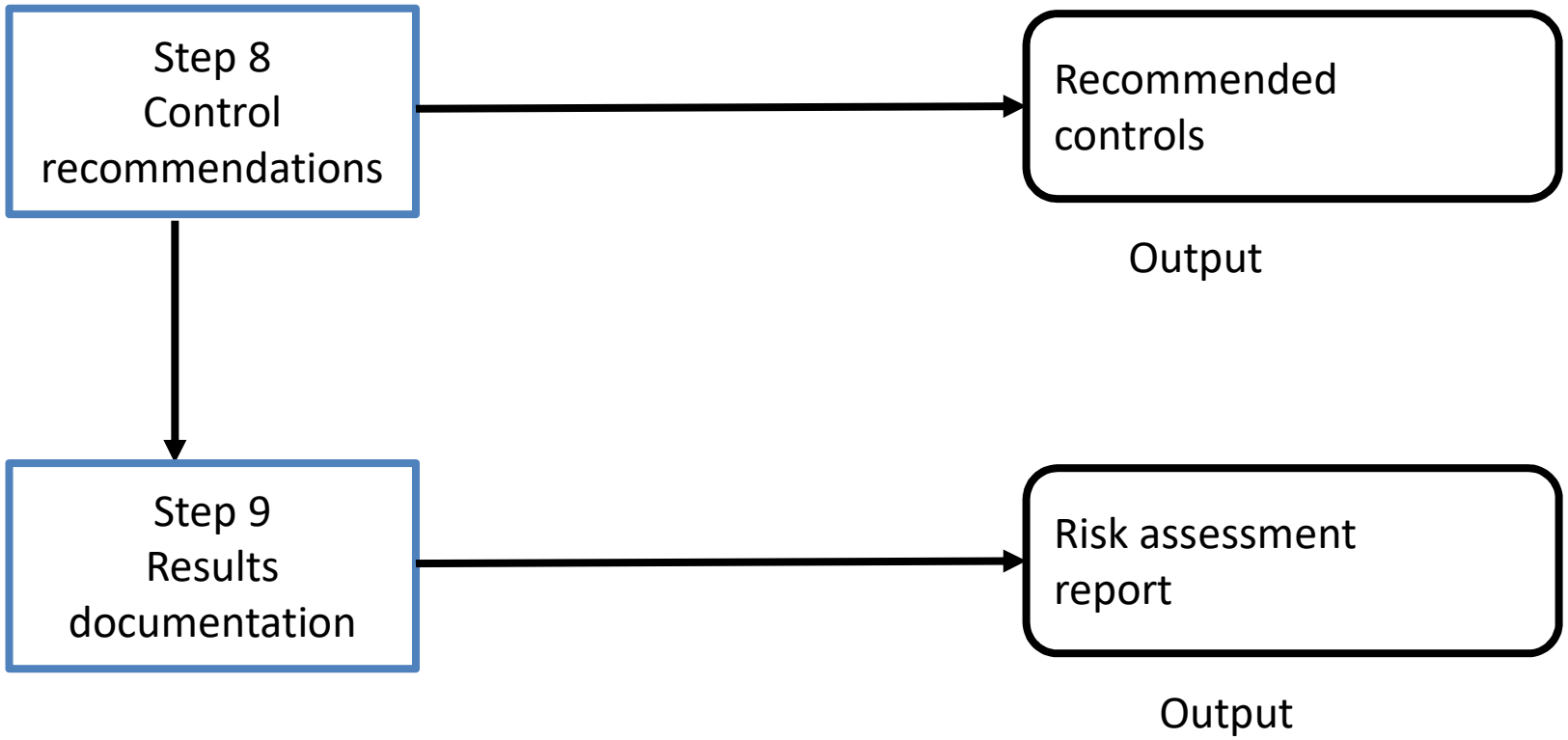
NIST 800-30 Impact analysis



NIST 800-30 Risk determination



NIST 800-30 Control & Results Recommendations

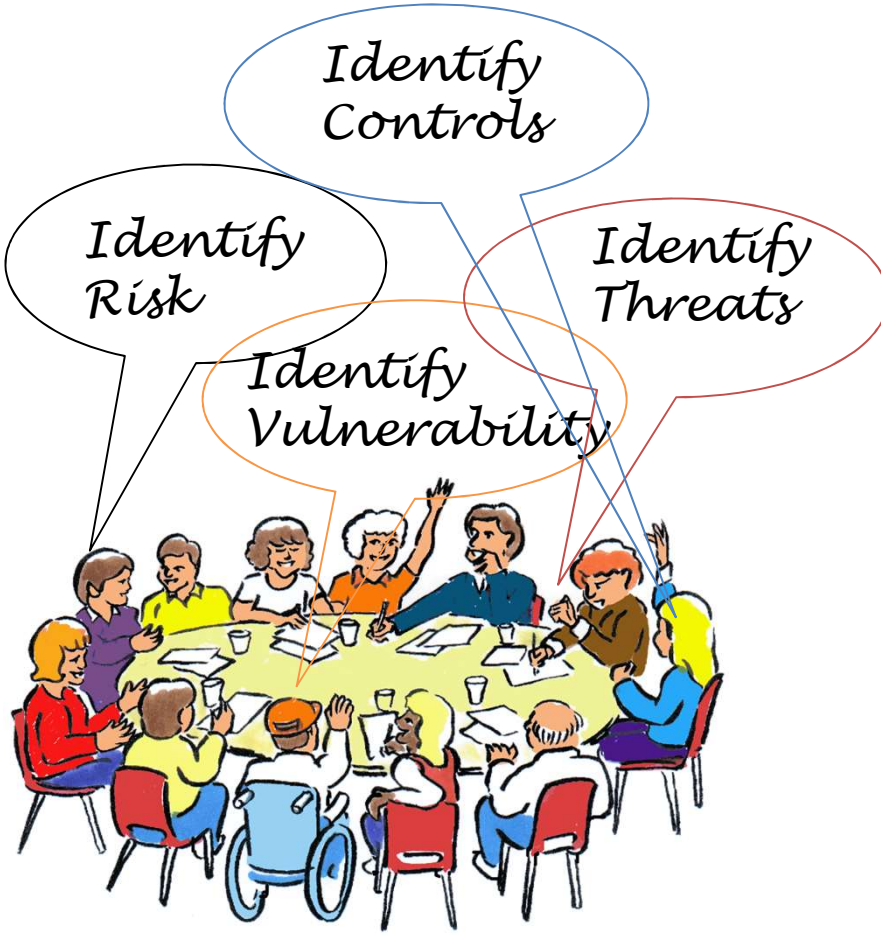


Facilitated Risk Analysis Process (FRAP)

- It is a qualitative methodology
- It focuses on the systems that really need assessing to reduce costs and time obligations.
- It is to be used to analyse one system, application, or business process at a time.
- Data is gathered and threats to business operations are prioritized based upon their criticality

Facilitated Risk Analysis Process (FRAP)

- A brainstorming session to list threats,
- The assignment of a simple probability (i.e. High/Medium/Low) to each threat,
- The assignment of simple impact (i.e. High/Medium/Low) to each threat,
- The identification of controls for the listed threats, and
- A management summary



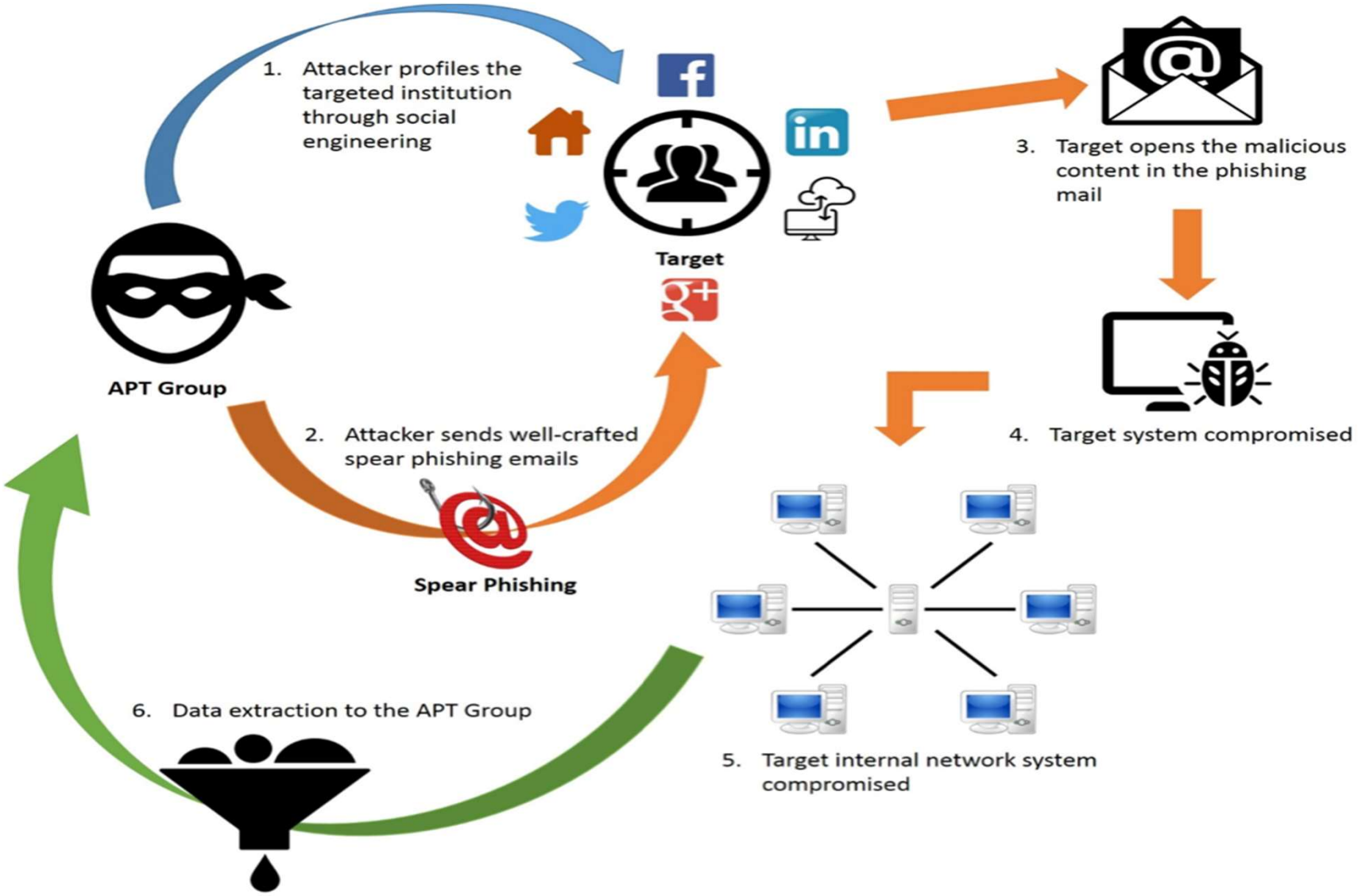
Facilitated Risk Analysis Process (FRAP)

- The FRAP users believe that additional effort to develop precisely quantified risks are not cost effective because:–
  - Such estimates are time consuming
  - risk documentation becomes too voluminous for practical use
  - specific loss estimates are generally not needed to determine if controls are needed

Facilitated Risk Analysis Process (FRAP)

- Each risk analysis session takes approximately 4 hours and Includes 7 to 15 people.
- Team does not attempt to obtain or develop specific numbers for threat likelihood or annual loss estimates but to sets priorities
- After identifying and categorizing risks, the groups identifies controls that can be implemented to reduce the risk.
- The Team's conclusions as to what risks exist and what controls are needed are documented along with a related action plan for control implementation.

Spear Phishing Case Scenario



Prioritizing Risk- Qualitative

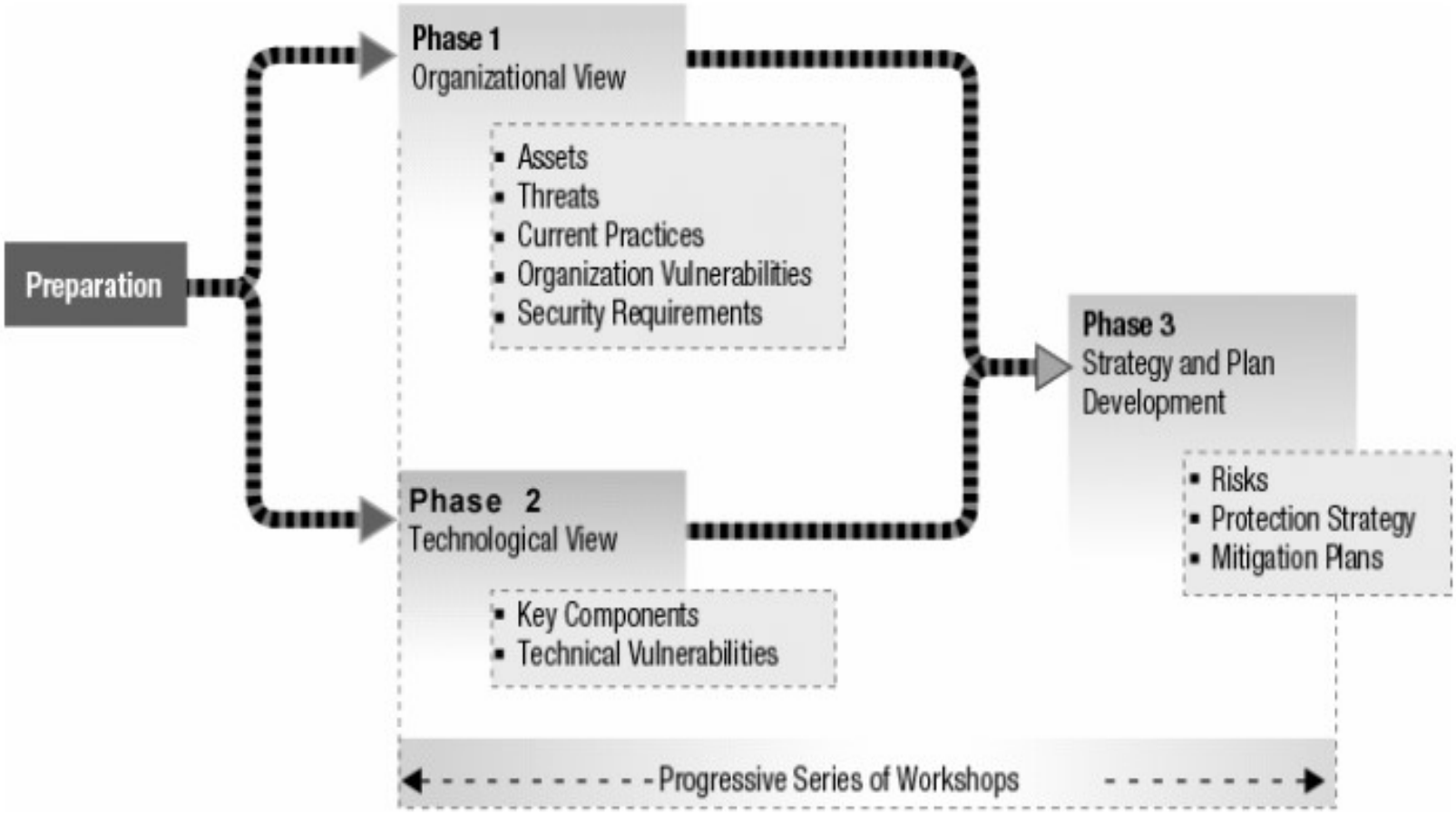
Threat descriptor (a)	Consequence (asset) value (b)	Likelihood of threat occurrence (c)	Measure of risk (d)	Threat ranking (e)
Threat A	5	2	10	2
Threat B	2	4	8	3
Threat C	3	5	15	1
Threat D	1	3	3	5
Threat E	4	1	4	4
Threat F	2	4	8	3

Risk = Consequence value * Likelihood of threat

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)

- Created by Carnegie Mellon University's Software Engineering Institute.
- The method is performed in a series of workshops conducted and facilitated by an interdisciplinary analysis team.
- The intended audience for the OCTAVE method is large organizations with 300 or more employees.
- Identify assets that are important to the mission of the organization
- Identify vulnerabilities and threats to those assets
- Determine and evaluate the potential consequences to the organization if threats are realized

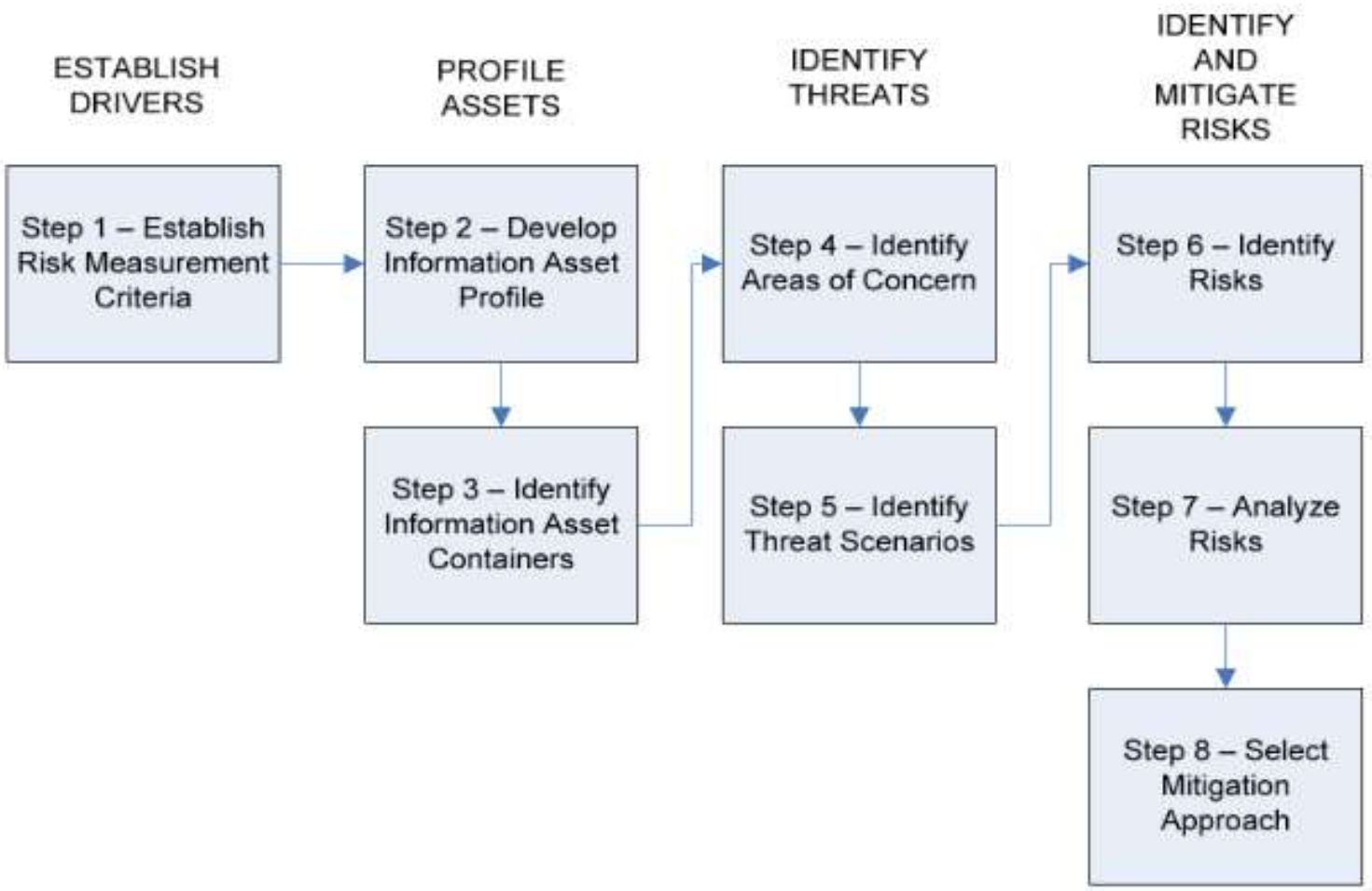
Three OCTAVE Method Phases



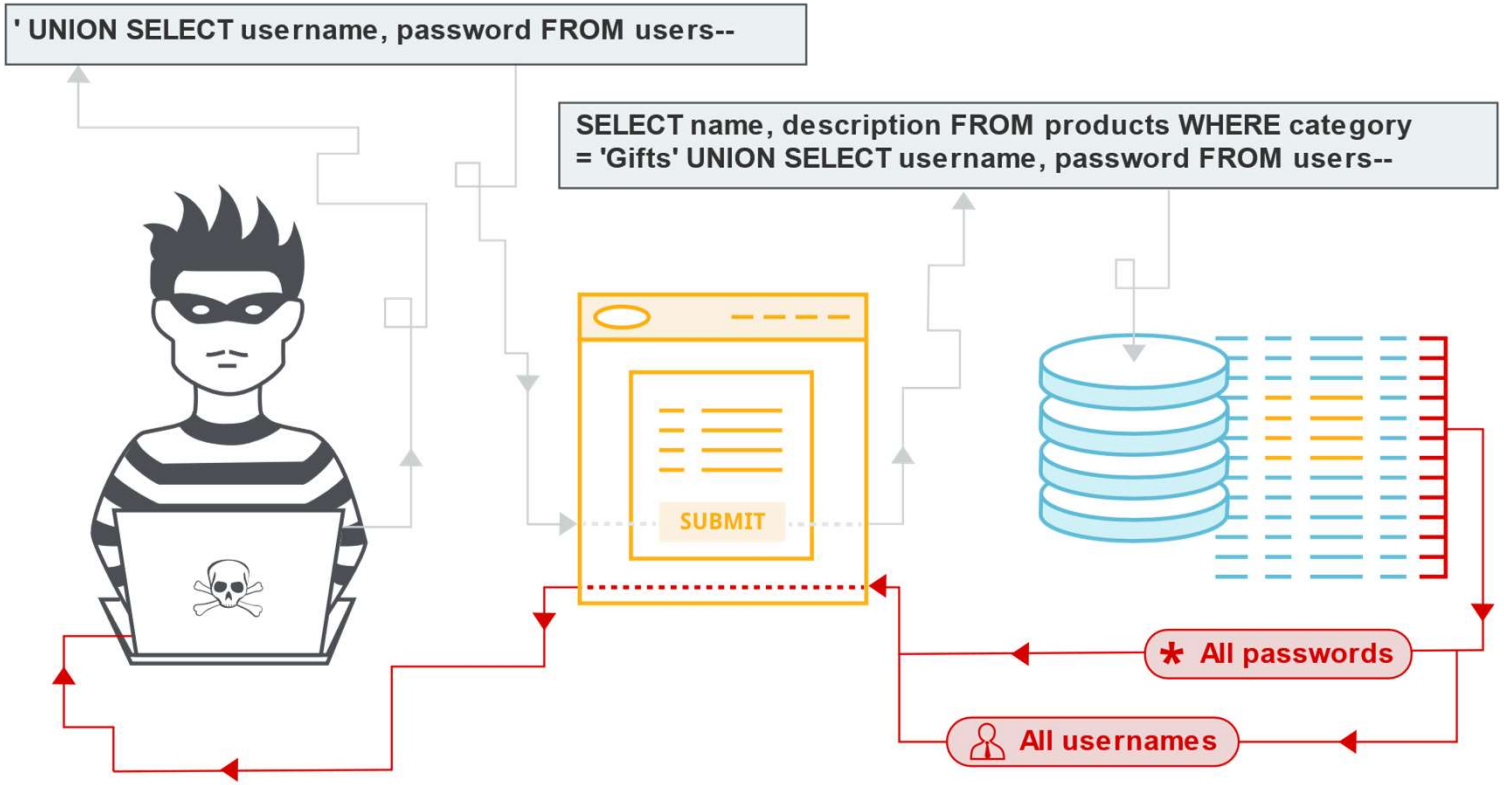
OCTAVE Allegro

- This approach differs from previous OCTAVE approaches by focusing primarily on information assets in the context
  - How they are used
  - Where they are stored
  - How they are transported,
  - How they are processed,
  - How they are exposed to threats, vulnerabilities.

OCTAVE Allegro



OCTAVE Allegro



OCTAVE Allegro

Step 1
Establish Risk Measurement Criteria

Impact Area	High	Medium	Low
Confidential Data Loss	More than 10% revenue loss	Between 5-10% revenue loss	Less than 5 % revenue loss

Step 2
Develop Information Asset Profile

Information Asset	Rationale for Selection	Description	Owner	Confidentiality	Integrity	Availability
Database Server	Leakage of data	All data stored	Network Admin	Key data must be kept secret	Only Admin can make change	Data must be made available

OCTAVE Allegro

Step 3: Identify Information Asset Containers

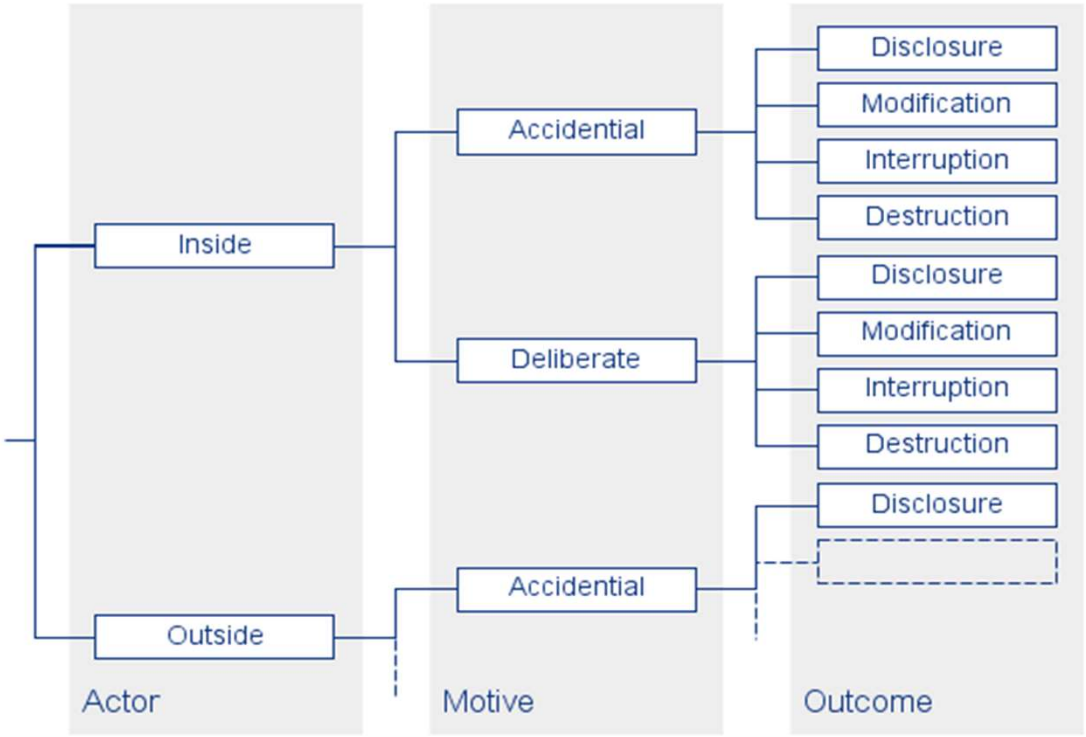
Container	Description	Owner	Type	Class
Server	Database server	Admin	Internal	Technical

Step 4: Identify Areas of Concern.

Area of Concern	Actor	Mean	Motive	Outcome
Data loss	Hacker	Web App Vuln	Deliberate Confidential data	Disclosure

OCTAVE Allegro

Step 5: Identify Threat Scenario



OCTAVE Allegro

Step 6: Identify Risk

Area of Concern	Actor	Motive	Outcome	Consequences
Data loss	Admin	Deliberate-Confidential data	Disclosure	Loss of $900,000

Step 7: Risk Analysis

Impact Area	Rank	Impact	Value	Score
Fines/Legal Penalties	5	High	3	15
Reputation	4	High	3	12
Safety and Health	3	Medium	2	6
Productivity	2	Medium	2	4
Financial	1	Low	1	1
Total Risk Score				**38**

OCTAVE Allegro

Step 8: Mitigation Approach

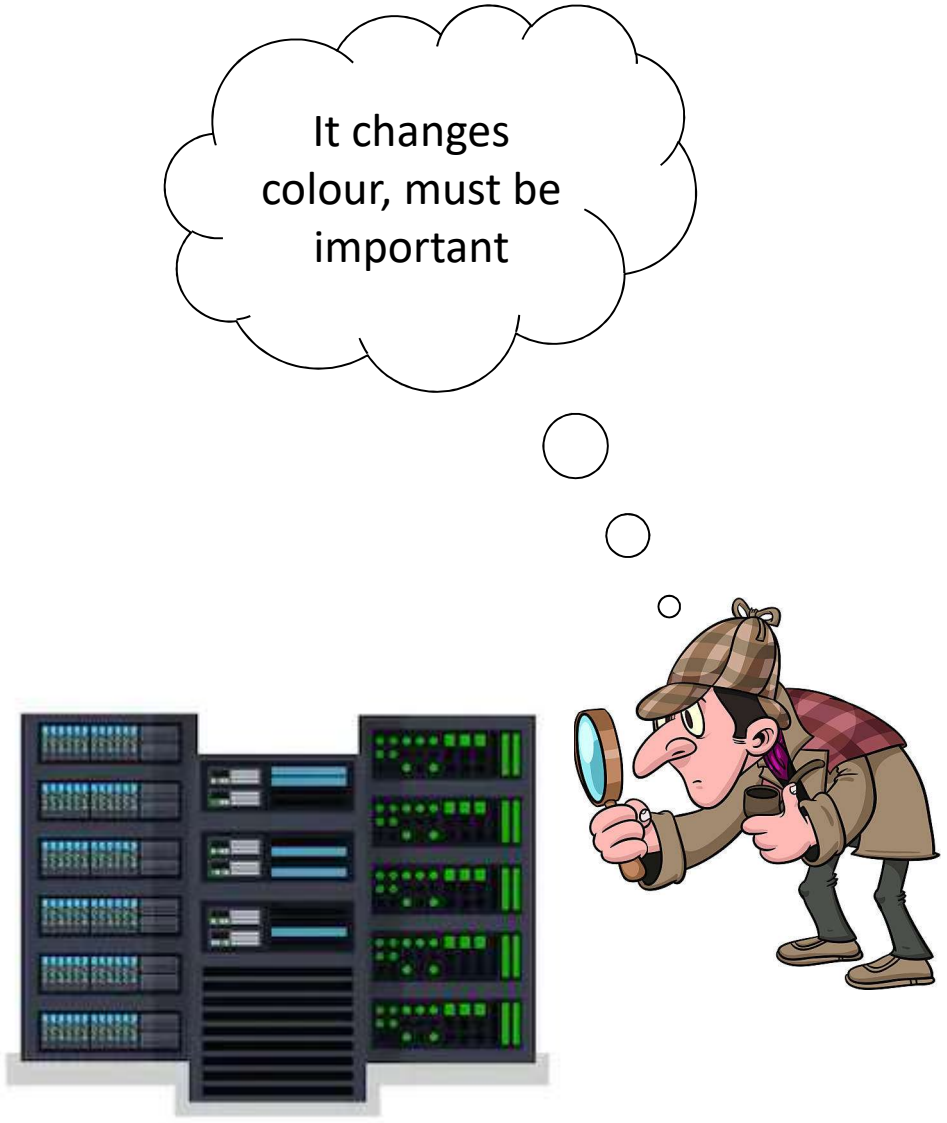
1. Mitigate
2. Avoid
3. Transfer
4. Accept

ISO/IEC 27005

1. Identification of assets.
2. Identification of legal and business requirements that are relevant for the identified assets.
3. Valuation of the identified assets, taking account of the identified legal and business requirements and the impacts of a loss of confidentiality, integrity and availability.
4. Identification of significant threats and vulnerabilities for the identified assets.
5. Assessment of the likelihood of the threats and vulnerabilities to occur.
6. Calculation of risk.
7. Evaluation of risks against a predefined risk scale.

ISO/IEC 27005 – Asset Identification

- The important assets within the scope of the ISMS should be clearly identified and appropriately valued.
- An inventory of these assets should be put together and maintained
- An owner should be identified for each of the identified assets,



Identification of legal and business requirements

- The unique set of threats and vulnerabilities which could lead to significant losses if they occur.
- The legal, statutory and contractual requirements which are applicable to the organization, its trading partners, contractors and service providers.
- The unique set of principles, objectives and requirements for information processing that an organization has developed t support its business operations and processes

Asset valuation

- To assess their values in terms of their importance to the business or their potential values in different business opportunities.
- It is also important to take account of the identified legal and business requirements and the impacts resulting from a loss of CIA.
- In order to consistently assess the asset values, a valuation scale for assets should be defined

Identification and assessment of threats and vulnerabilities

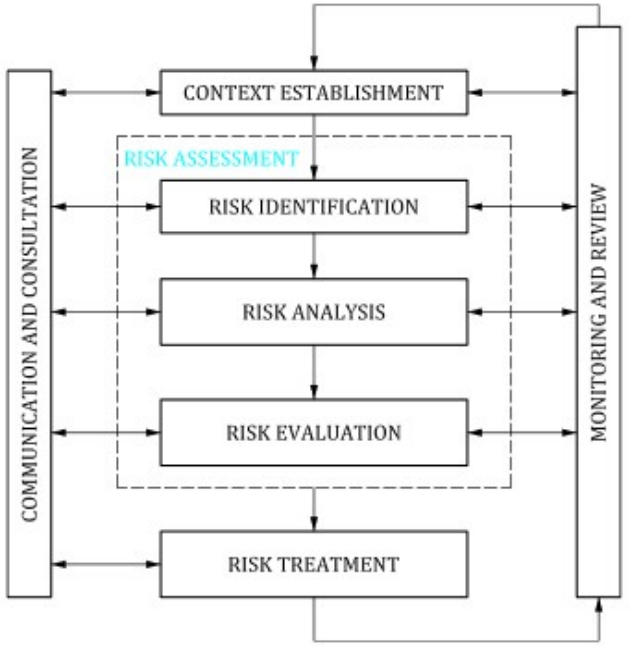
- Implemented controls
- Identification of threats and vulnerabilities
- Threats can originate from accidental or deliberate sources or events.
- A threat would need to exploit one or more vulnerabilities of the systems, applications or services to successfully cause harm to assets.
- Threats may originate from within the organization as well as external to it.

Assessment of the threats and vulnerabilities

- Deliberate threats.
- Accidental threats.
- Past incidents.
- New developments and trends.

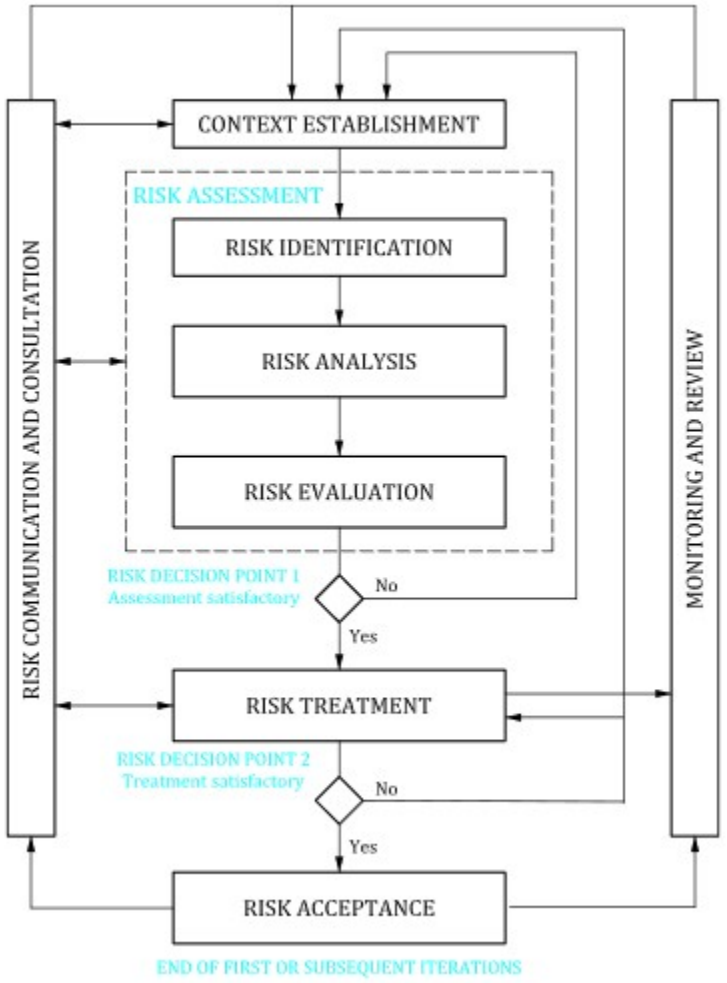
Risk calculation and evaluation

- The risks are calculated from the combination of asset values and the assessed likelihood of related threats and vulnerabilities to come together and cause an incident.
- How the two contributing factors (the impact and the likelihood value) are combined to calculate the risk.
- The results of the risk assessment process should be documented in a risk assessment report



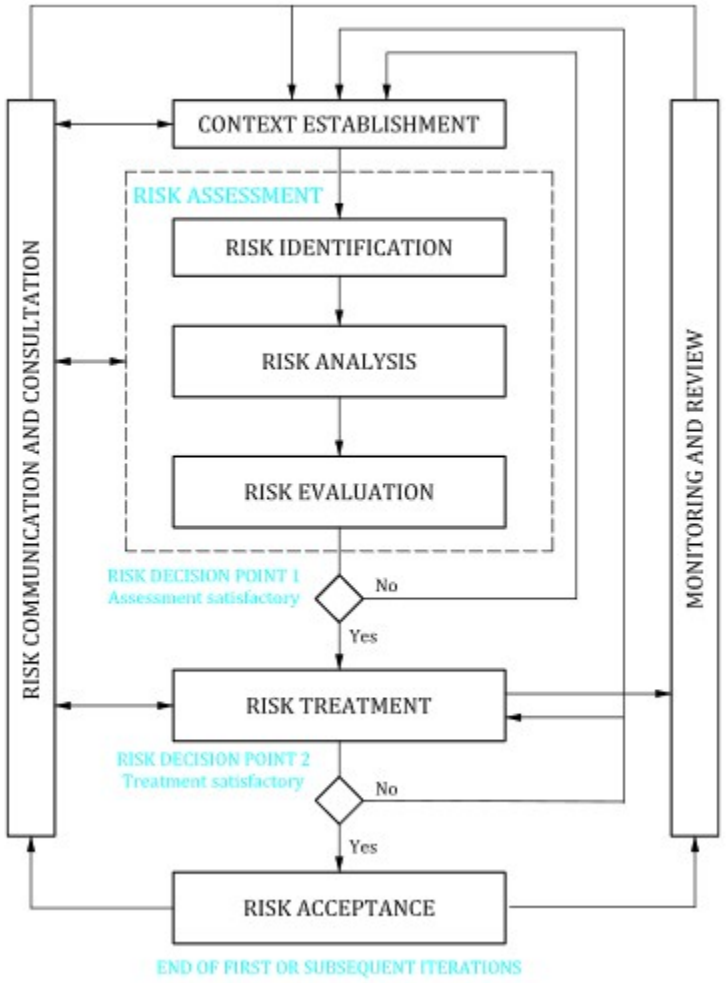
The risk assessor

- The person who performs the information security risk assessments.
- The person should have a basic understanding of how the business works and the risk appetite of the business
- They should have practical understanding of a suitable risk assessment method and any associated tools, software or forms.
- They have enough interpersonal skills to obtain the necessary information from the people in the organization and to communicate the results of the risk assessment in a way that is easily understood by decision-making management.

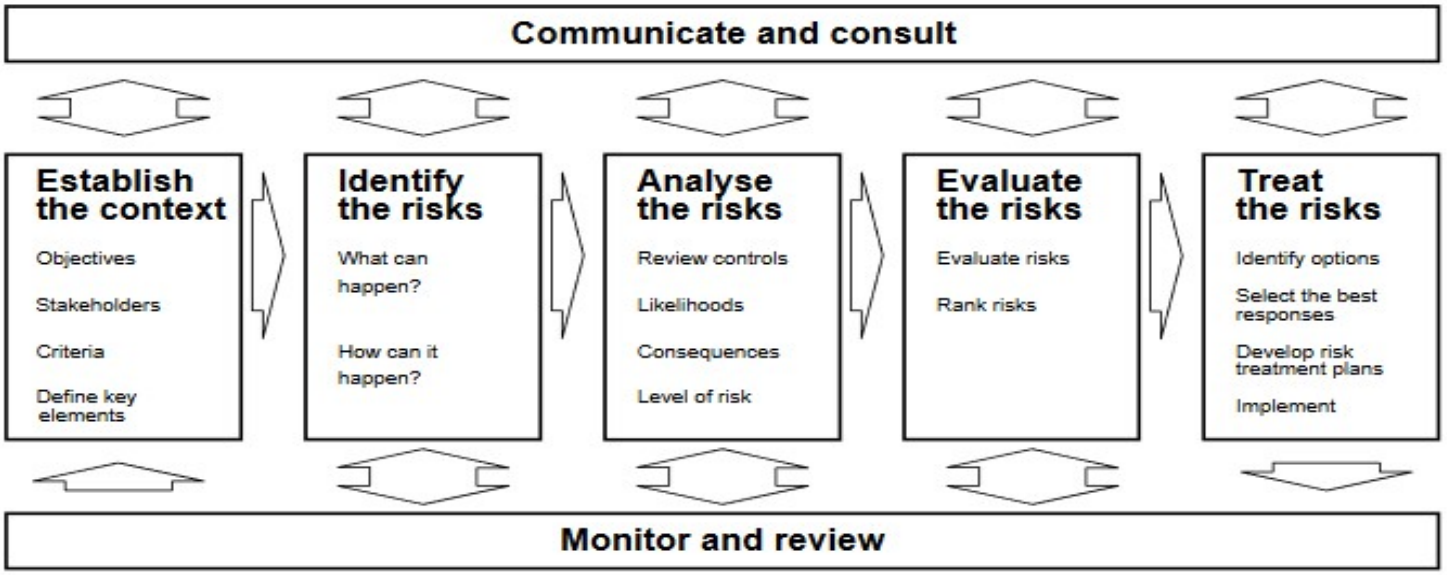


The risk assessor

- The person who performs the information security risk assessments.
- The person should have a basic understanding of how the business works and the risk appetite of the business
- They should have practical understanding of a suitable risk assessment method and any associated tools, software or forms.
- They have enough interpersonal skills to obtain the necessary information from the people in the organization and to communicate the results of the risk assessment in a way that is easily understood by decision-making management.



AS/NZS 4360



- This Australian and New Zealand methodology can be used to understand a company's financial, capital, human safety, and business decisions risks.
- This risk methodology is more focused on the health of a company from a business point of view, not security.

CRAMM

- Central Computing and Telecommunications Agency Risk Analysis and Management Method was created by the United Kingdom.
- Its automated tools are sold by Siemens.
- It works in three distinct stages:
  - Define objectives
  - Assess risks
  - Identify countermeasures.
- It just has everything (questionnaires, asset dependency modelling, assessment formulas, compliancy reporting) in automated tool format.

Today's Task

- Group Activity:
  - Using the Betterbuy scenario complete the network diagram
  - Read through NIST 800-30 risk assessment methodology and use it to
    - Identify all the threats the company is facing SME.
    - Using quantitative method to prioritize risks.