جامعة الحسين التقنية
Al Hussein Technical University

Information Security Management

J/618/7447
10203300

جامعة الحسين التقنية
Al Hussein Technical University

Topic 2: INFORMATION RISK

Eman Alzyoud
School of Computing and Informatics
Eman.Alzyoud@HTU.EDU.JO

Table of content:

- Threats to, and vulnerabilities of, information systems .
- Risk management
- Cost vs. Benefit of Security Controls
- Gap Analysis.
- Use of recognised sources of threat intelligence and vulnerabilities to predict possible, current, and future threats, e.g. horizon scanning.

Risk Terms

ASSETS	RISK	THREAT	VULNERABILITY	IMPACT
Valuable resource you are trying to protect	The potential that a chosen action or activity will lead to a loss	Negative action that may harm a system	Weakness that allows a threat to cause harm	The severity of the damage, sometimes expressed in dollars

Risk Terms cont.

Asset Valuation, is value assigned to an asset based on a number of factors, including importance to the organization, use in critical process, actual cost, and nonmonetary expenses/costs (such as time, attention, productivity, and research and development).

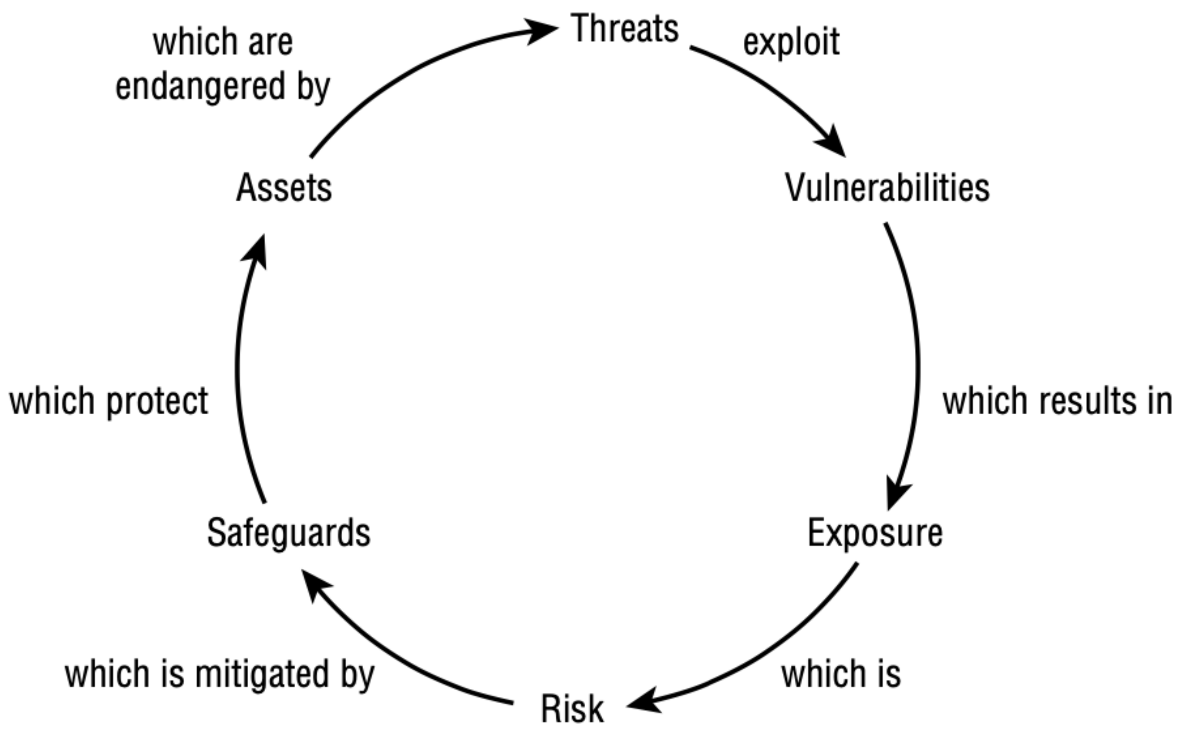
Exposure, is being susceptible to asset loss because of a threat; there is the possibility that a vulnerability can or will be exploited by a threat agent or event. Exposure doesn’t mean that a realized threat (an event that results in loss) is actually occurring, just that there is the potential for harm to occur. The quantitative risk analysis value of exposure factor (EF) is derived from this concept.

Safeguards, security control, protection mechanism, or countermeasure is anything that removes or reduces a vulnerability or protects against one or more specific threats. This concept is also known as a risk response.

Attack, is the intentional attempted exploitation of a vulnerability by a threat agent to cause damage, loss, or disclosure of assets. An attack can also be viewed as any violation or failure to adhere to an organization’s security policy. A malicious event does not need to succeed in violating security to be considered an attack.

Breach, intrusion, or penetration is the occurrence of a security mechanism being bypassed or thwarted by a threat agent. A breach is a successful attack.

The cyclical relationships of risk elements



Threat categorization

There are a number of types of information-related threats.

- **Physical threats** include deliberate forms of threat, such as theft and vandalism, and also accidental threats, such as trackside communications or signaling cables becoming damaged

- **Outages and failures** include such things as the absence of vital people resources, which is often overlooked as this is not specifically technology-linked; loss of power supplies, whether due to mains failure or the failure of uninterruptible power supplies (UPS) or backup generators; hardware failures, which are much less common these days, but still possible, especially in rotating disk drives; and software failures. Finally, there will be the threat of human errors, which may result in the loss of confidentiality, integrity and availability.

- **Hacking and abuse** are among the most serious forms of threat. They include social engineering and espionage, which often results in both identity and information theft; malware, such as viruses and ransomware; denial of service (DoS) attacks; and the wider-ranging distributed denial of service (DDoS) attacks, eavesdropping and unauthorized changes both to information and to credentials, such as escalating someone’s access privileges.

Threat categorization Cont.

- **Legal and contractual threats** include the organization's failure to meet its obligatory requirements in delivering service. While these types of threat may not result in the loss of confidentiality, integrity or availability, there will doubtless be consequences – financial penalties or loss of reputation – that will result. Breaches of legislation such as the Data Protection Act (DPA) or the terrorism, hi-tech General Data Protection Regulation (GDPR) will also have potentially serious consequences.

- **Accidents and Disasters** may cause information-related problems for organizations. Most of these will be accidental in nature, and will include natural disasters such as floods, landslides, earthquakes and tsunamis, but can also include environmental disasters such as chemical leaks and explosions.

Accidental threats are sometimes referred to as hazards, especially when concerned with external events. The implication is that there has been no deliberate attempt to carry out the threat – it has simply happened. There may be no one to blame for an accidental threat occurring, but there may be a means of dealing with the threat, as will be seen later.

Deliberate threats, on the other hand, occur when someone sets out with every intention of carrying out the threat. This type of threat in the computer world includes hacking, malicious software, sabotage, cyber crime and so on.

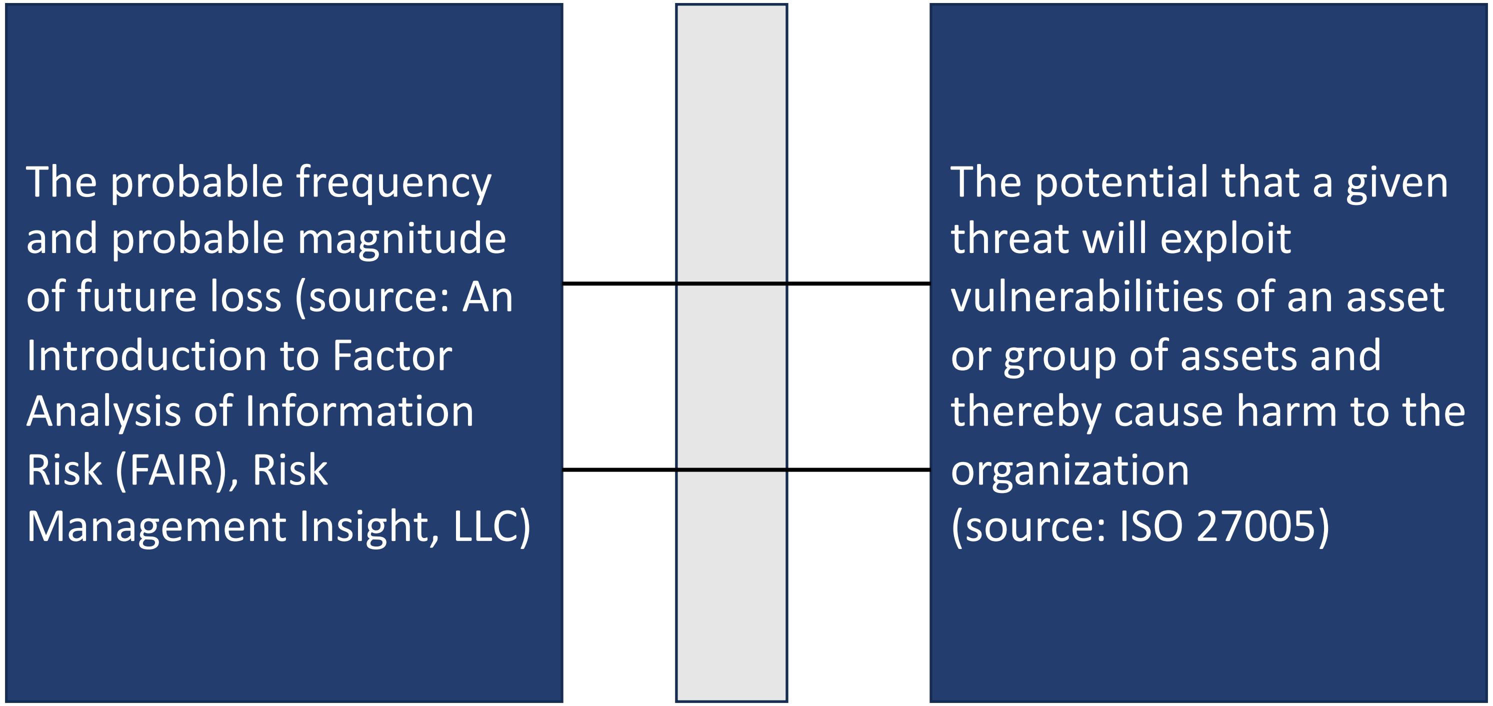
Vulnerability categorization

Vulnerabilities of IT systems fall into two distinct categories – general vulnerabilities and information-specific vulnerabilities.

General vulnerabilities include basic weaknesses in software (including poor design), hardware, buildings or facilities, people, processes and procedures.

Information-specific vulnerabilities include unsecured computers, including personal computers, hand-held devices and memory sticks, servers, un-patched operating systems and applications, unsecured network boundary devices, unsecured wireless systems, unsecured web servers, unsecured email systems, unlocked filing cabinets and the like.

Definitions of Risk



The probable frequency and probable magnitude of future loss (source: An Introduction to Factor Analysis of Information Risk (FAIR), Risk Management Insight, LLC)

The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization (source: ISO 27005)

When written as a conceptual formula, risk can be defined as follows:

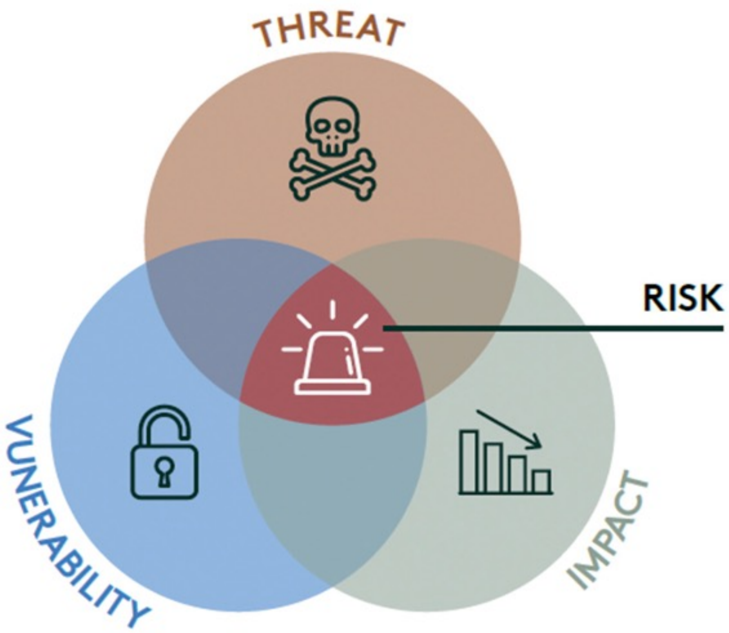
risk = threat * vulnerability
or
risk = probability of harm * severity of harm

Risk Management Process

- Risk Management

A proactive attempt to recognize and manage internal events and external threats.

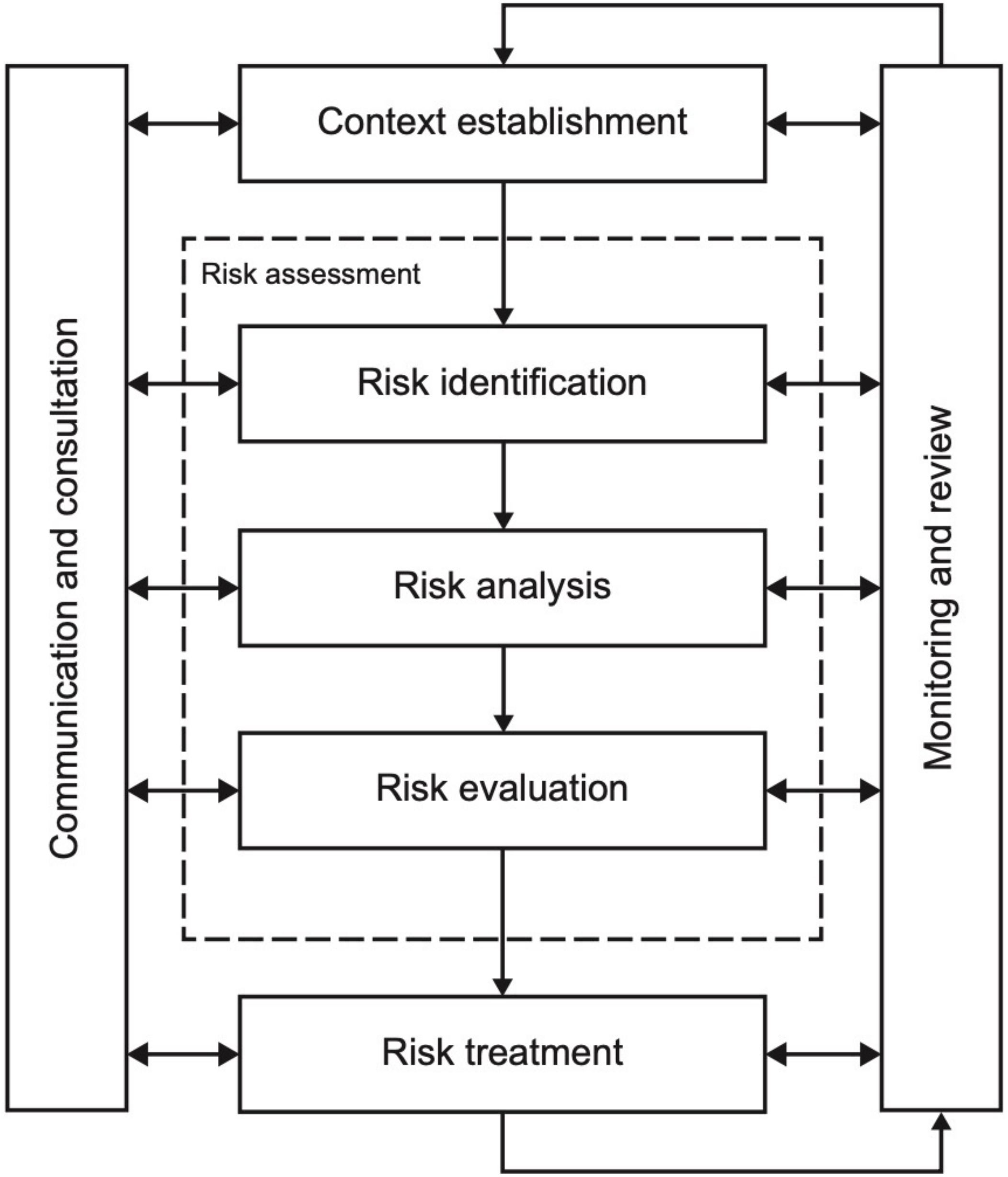
- What can go wrong (risk event)
- How to minimize the risk event’s impact (consequences)
- What can be done before an event occurs (anticipation)
- What to do when an event occurs (contingency plans)



Frequently, risk is defined as a combination of threat, vulnerability and impact

Risk management process

Risk management consists of distinct areas: context establishment; risk assessment (the combination of risk identification, risk analysis and risk evaluation); risk treatment; communication and consultation; and ongoing monitoring and review.



The risk management life cycle

Managing Risk

- Step 1: Context establishment

involves understanding an organization's information assets, business model, objectives, and position within the overall scheme, which is essential for a valuable risk assessment.

- Step 2: Risk Identification

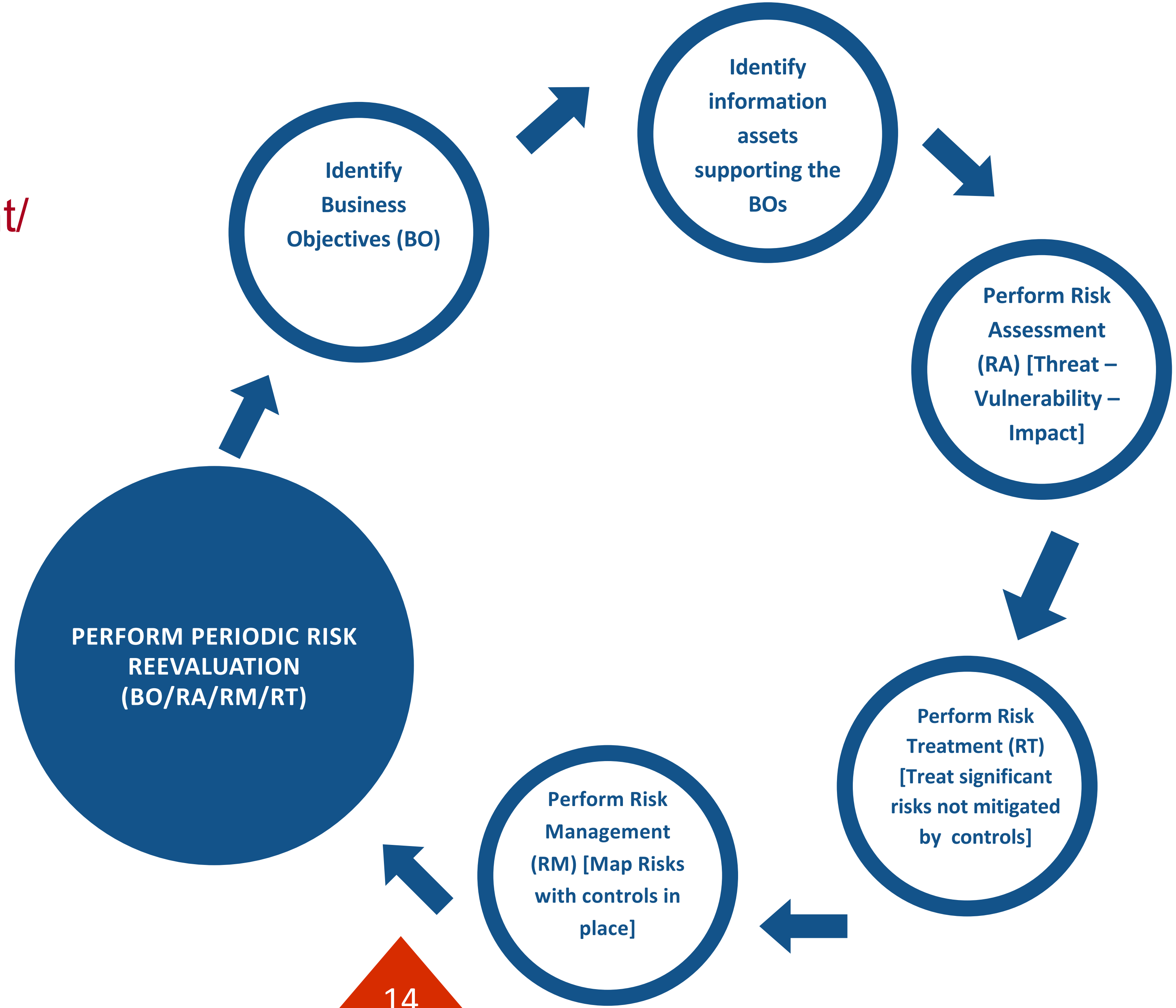
involving identifying threats and vulnerabilities. Each threat should be considered based on its impact on the asset, An alternative approach involves identifying critical assets and determining potential threats. This information is then used in the next analysis step.

Generate a list of possible risks through brainstorming, problem identification and risk profiling. Macro risks first, then specific events.

several tools and techniques for identifying risks:

- **Brainstorming :** Generate a list of all possible project risks.
- **Checklists :** Developed based on historical information from similar organization.
- **SWOT Analysis :** Identify opportunities that are result of organization strength as well as threats that are result of organization weakness.

Step 3: Risk Assessment/ Analysis



Identify Business Objectives (BO)

Identify information assets supporting the BOs

Perform Risk Assessment (RA) [Threat – Vulnerability – Impact]

Perform Risk Treatment (RT) [Treat significant risks not mitigated by controls]

Perform Risk Management (RM) [Map Risks with controls in place]

PERFORM PERIODIC RISK REEVALUATION (BO/RA/RM/RT)

Risk Assessment/Analysis

- Risk management is primarily the responsibility of upper management. However, upper management typically assigns the actual task of risk analyses and risk response modeling to a team from the IT and security departments. The results of their work will be submitted as a proposal to upper management, who will make the final decisions as to which responses are implemented by the organization

- All IT systems and organizations have risk, and upper management must decide which risks are acceptable. This requires detailed asset and risk assessments, understanding of the organization's budget, internal expertise, and business conditions. Risk is personal and specific to an organization based on its assets, threats, and risk tolerance.

Risk Assessment Tools

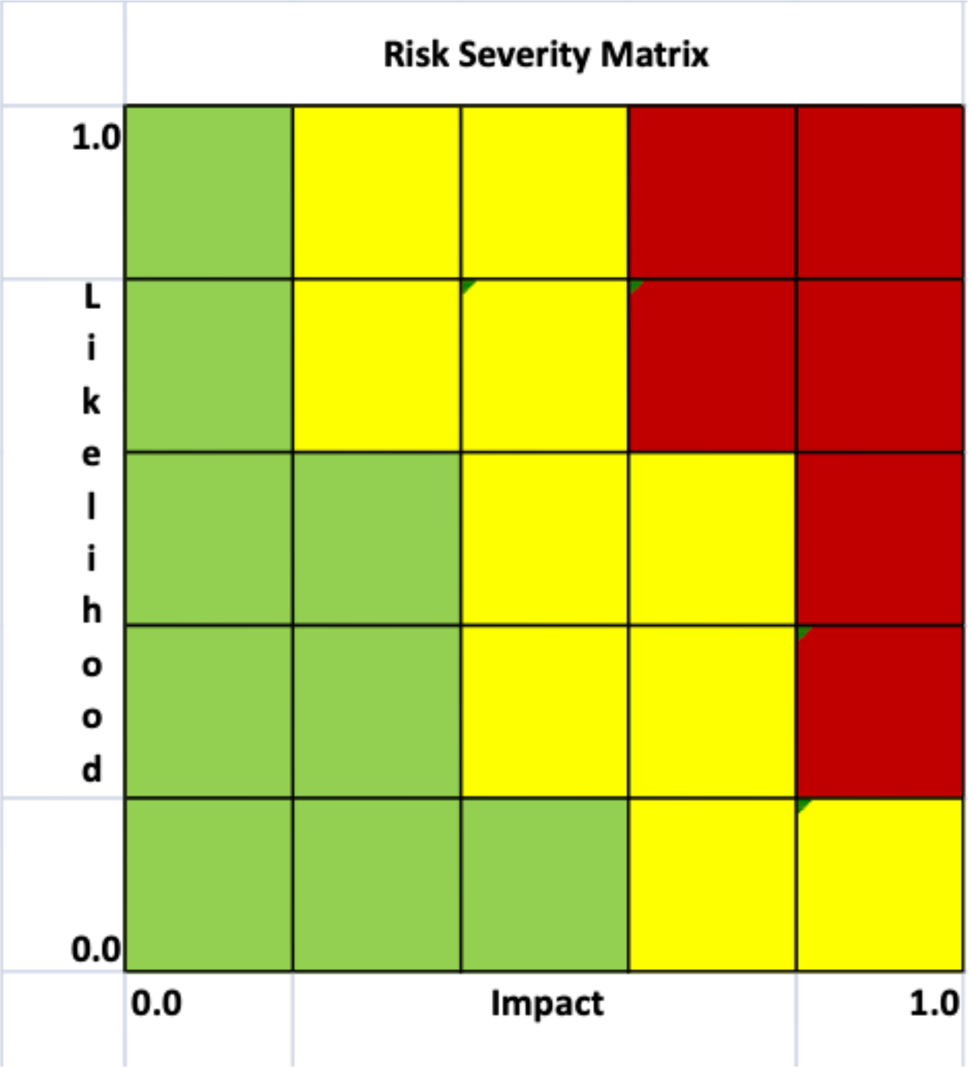
Risk Assessment Tools :

- Scenario analysis for event probability and impact
- Risk assessment matrix
- Failure Mode and Effects Analysis (FMEA)
- Probability analysis
  - Decision trees, NPV, and PERT
- Semiquantitative scenario analysis

Risk Severity Matrix
Probability/Impact Matrix

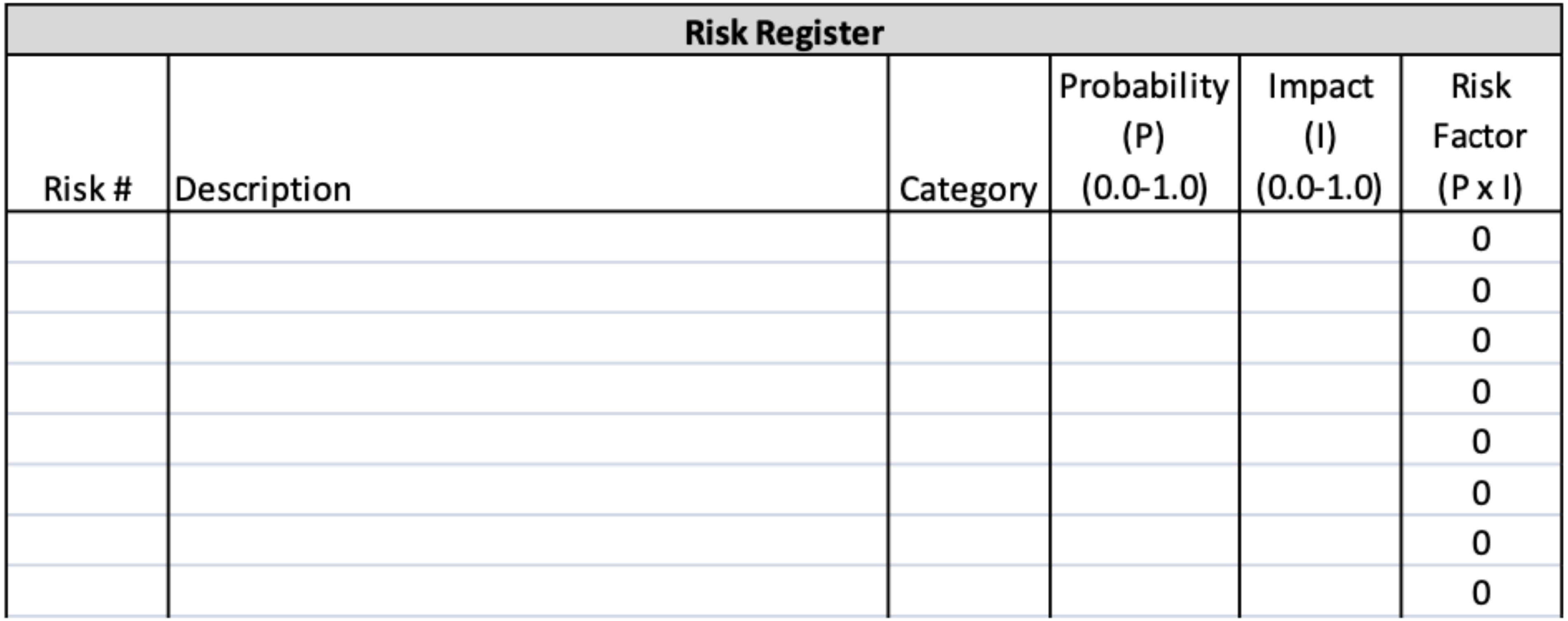
Risk Severity Matrix (Probability/Impact Matrix)

lists the relative probability of a risk occurring on one side of a matrix or axis on a chart and the relative impact of the risk occurring on the other.



🟩	🟨	🟨	🟥	🟥
🟩	🟨	🟨	🟥	🟥
🟩	🟩	🟨	🟨	🟥
🟩	🟩	🟨	🟨	🟥
🟩	🟩	🟩	🟨	🟨

Risk Register



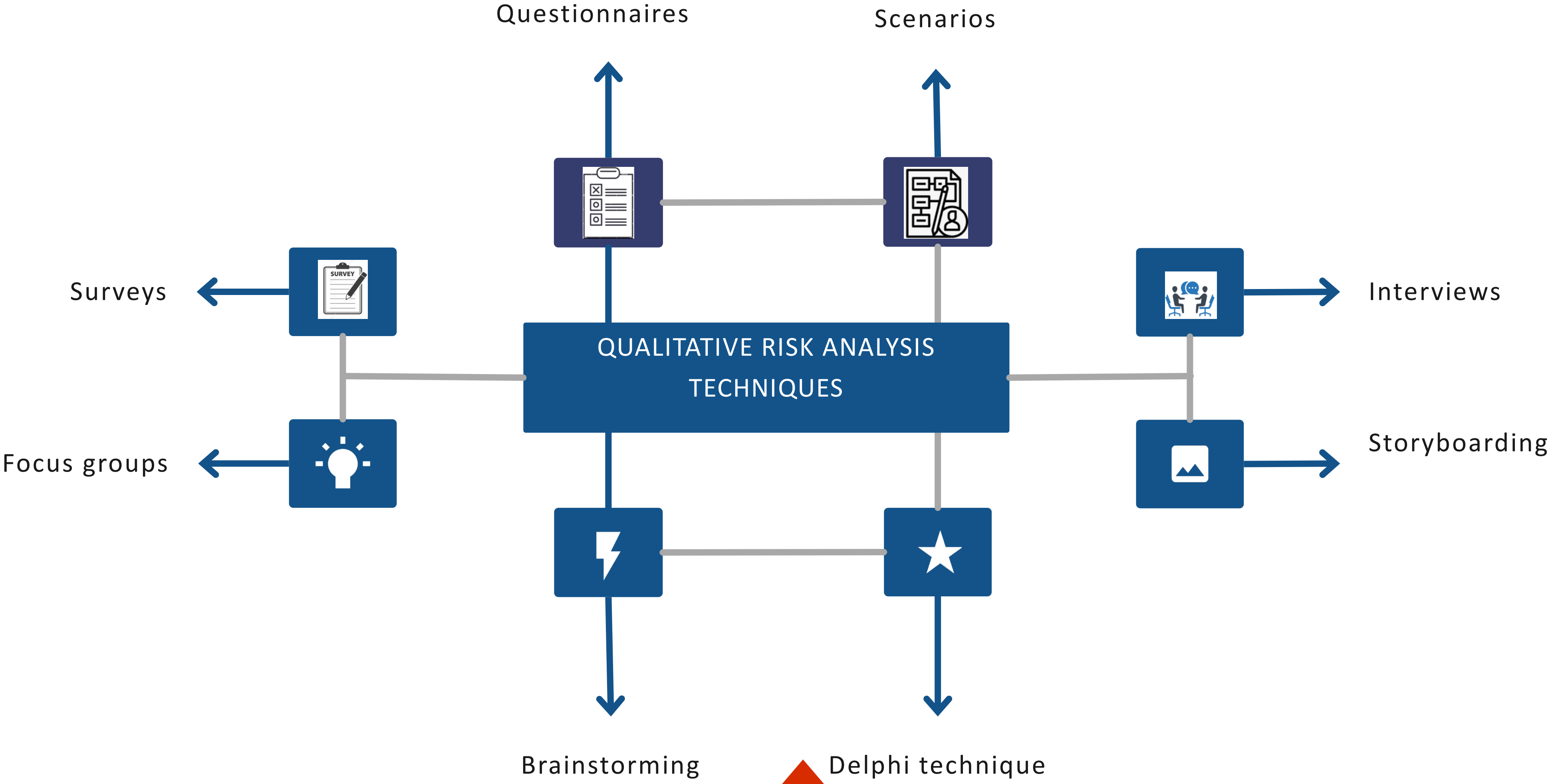
Risk Register

Risk #	Description	Category	Probability (P) (0.0-1.0)	Impact (I) (0.0-1.0)	Risk Factor (P x I)
					0
					0
					0
					0
					0
					0
					0
					0

Output of Risk Identification is : Risk Register.
List of individual identified risks. Potential risk owners.

QUALITATIVE RISK ANALYSIS

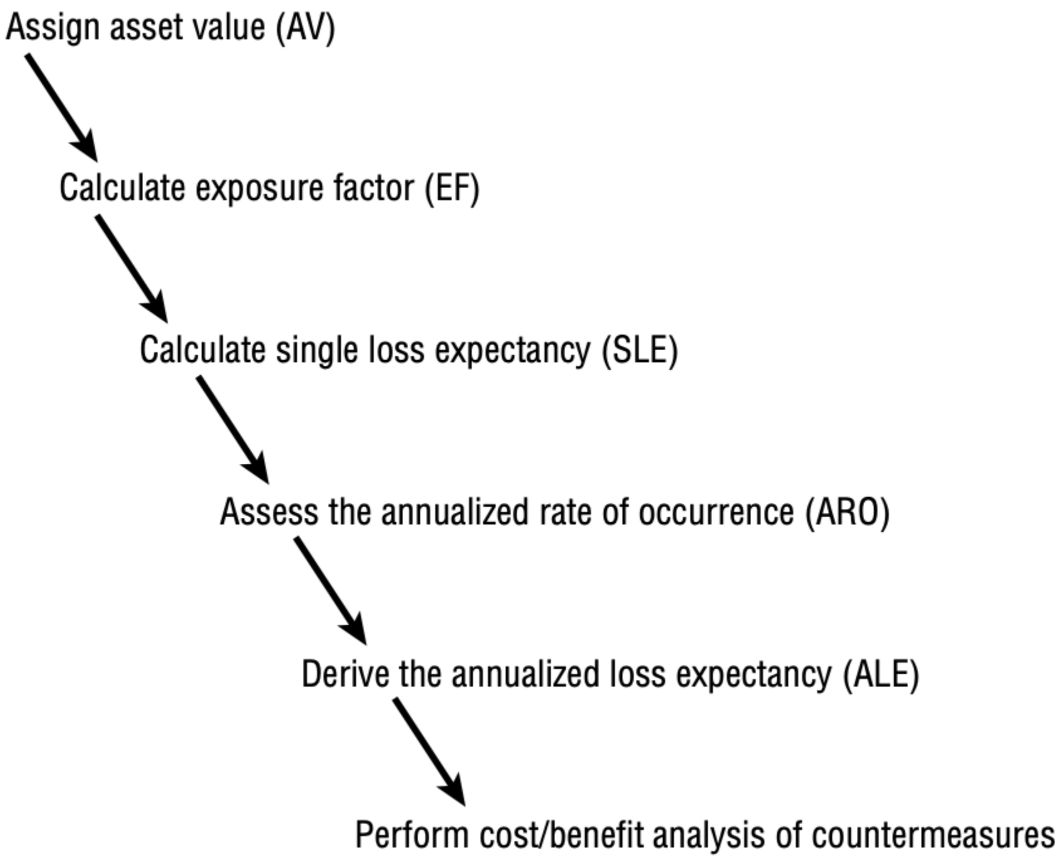
It is more scenario-based than it is calculator-based. Rather than assigning exact dollar figures to possible losses, you rank threats on a relative scale to evaluate their risks, costs, and effects.



QUANTATIVE RISK ANALYSIS

The quantitative method results in concrete probability indications or a numeric indication of relative risk potential. That means the end result is a report that has dollar figures for levels of risk, potential loss, cost of countermeasures, and value of safeguards.

The major steps or phases in quantitative risk analysis are as follows :



Assign asset value (AV)

Calculate exposure factor (EF)

Calculate single loss expectancy (SLE)

Assess the annualized rate of occurrence (ARO)

Derive the annualized loss expectancy (ALE)

Perform cost/benefit analysis of countermeasures

QUANTATIVE RISK ANALYSIS CON.

The Exposure Factor (EF)

is the percentage of value an asset lost due to an incident

The Single Loss Expectancy (SLE)

is the cost of a single loss.
SLE is the Asset Value (AV) times the Exposure Factor (EF)

The Annual Rate of Occurrence (ARO)

is the number of losses you suffer per year

The Annualized Loss Expectancy (ALE)

is your yearly cost due to a risk. It is calculated by multiplying the Single Loss Expectancy (SLE) times the Annual Rate of Occurrence (ARO)

QUANTATIVE RISK ANALYSIS CON.

SLE = Asset Value (AV) × Exposure Factor (EF)

Risk = Probability of the Risk × Cost of the Eventuality

ALE = single Loss Expectancy (SLE) × Annual Rate of Occurrence (ARO

Comparison of quantitative and qualitative risk analysis

Characteristic	**Qualitative**	**Quantitative**
Employs math functions	No	Yes
Uses cost/benefit analysis	May	Yes
Requires estimation	Yes	Some
Supports automation	No	yes
Involves a high volume of information	No	yes
Is objective	Less so	More So
Relies substantially on opinion	Yes	No
Requires significant time and effort	Sometimes	Yes
Offers useful and meaningful results	Yes	Yes

Managing Risk (cont’d)

Step 4: Risk treatment

- **Risk Mitigation**

Applying adequate controls to lower the risks

- **Risk acceptance**

Objectively and knowingly not taking action

- **Risk avoidance**

Evading risks by ensuring actions that cause the risk are prevented

- **Risk transfer/sharing**

Sharing the risk with third parties such as suppliers or insurance companies

Managing Risk (cont’d)

- **Inherent risk,** is the level of natural, native, or default risk that exists in an environment, system, or product prior to any risk management efforts being performed.

- **Residual risk,** Once safeguards, security controls, and countermeasures are implemented, the risk that remains is known as residual risk.

In other words, residual risk is the risk that management has chosen to accept rather than mitigate. In most cases, the presence of residual risk indicates that the cost/benefit analysis showed that the available safeguards were not cost-effective deterrents.

- Total risk is the amount of risk an organization would face if no safeguards were implemented.

threats * vulnerabilities * asset value = **total risk**

- The difference between total risk and residual risk is known as the controls gap. The controls gap is the amount of risk that is reduced by implementing safeguards.

total risk – controls gap = **residual risk**

Cost vs. Benefit of Security Controls

To determine whether the safeguard is financially equitable, use the following **cost/benefit formula** :
[ALE pre-safeguard – ALE post-safeguard] – annual cost of safeguard (ACS) = value of the safeguard to the company

In The review, to perform the cost/benefit analysis of a safeguard, you must calculate the following three elements:

- pre-safeguard ALE for an asset-threat pairing
- The potential post-safeguard ALE for an asset-threat pairing
- The ACS (annual cost of the safeguard)

Several common factors affect ACS:

- Cost of purchase, development, and licensing
- Cost of implementation and customization
- Cost of annual operation, maintenance, administration, and so on Cost of annual repairs and upgrades
- Productivity improvement or loss
- Changes to environment
- Cost of testing and evaluation

Security Controls Selection and Implementation

Selecting a countermeasure, safeguard, or control (short for security control) within the realm of risk management relies heavily on the cost/benefit analysis results. However, you should consider several other factors when assessing the value or pertinence of a security control:

- The cost of the countermeasure should be less than the value of the asset.
- The cost of the countermeasure should be less than the benefit of the countermeasure.
- The result of the applied countermeasure should make the cost of an attack greater for the perpetrator than the derived benefit from an attack.
- The countermeasure should provide a solution to a real and identified problem
- The benefit of the countermeasure should be testable and verifiable.
- The countermeasure should provide consistent and uniform protection across all users, systems, protocols, and so on.
- The countermeasure should require minimal human intervention after initial deployment and configuration.

Types of Controls

Preventive

- Predict and prevent problems before they occur
- Monitor input controls and events as a preventive measure • Examples:
  - Segregation of duties
  - Maker-checker/four-eyes principle
  - Input and access controls (physical and logical)
  - Encryption of data at rest and in transit

Corrective

- Minimize the impact of a threat and rectify the cause of a problem
- Correct detected errors
- Root cause analysis, followed by changes to minimize future occurrences
- Examples:
  - Disaster recovery and business continuity planning
  - Incident response
  - Backups, to ensure recovery by restoring data
  - Reruns of failed processes

Detective

- Controls to detect and report intentional and unintentional errors after they occur
- Report incidence of errors, attacks, and omissions as they occur • Examples:
  - Logs
  - Error messages
  - Hash totals
  - Code review
  - Logical and physical access logging, such as server room access control, and door logging

Gap analysis

A gap analysis is the process that companies use to compare their current performance with their desired, expected performance. This analysis is used to determine whether a company is meeting expectations and using its resources effectively.

reality is that most organizations that embark on ISO27001 already have a number of information security measures in place; ISO27001 necessitates ensuring that those controls that are in place are adequate and appropriate and that additional required controls are implemented as quickly as possible. In other words, **an analysis of the gap between what is in place and what might be required might be carried out**

could be a useful point of reference when carrying out the risk assessment;

Threat Modelling

- A process where potential threats are identified, categorized, and analysed
- Can be performed both pro-actively as well as reactively
- Two goals of threat modelling
  - Reduce the number of security related coding and design defects
  - Reduce the severity of remaining defects

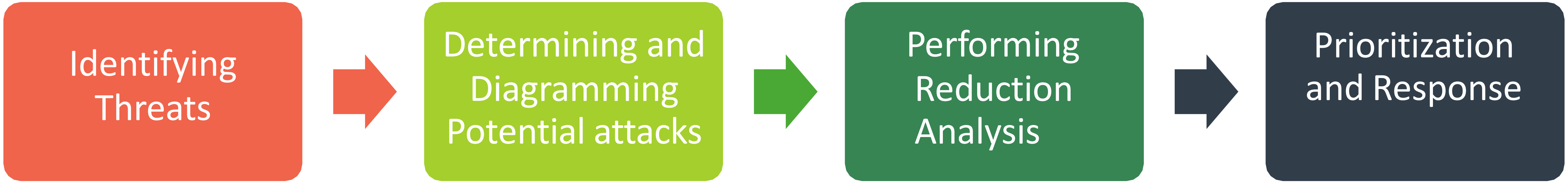
- **Proactive Approach**

- Also known as defensive approach
- Takes place during early stages of systems development
- Based on predicting threats and design specific counter measures during the coding and crafting process

- **Reactive Approach**

- Also known as adversarial approach
- Takes place after a product has been created and deployed
- This is the core concept behind ethical hacking, PT, source code review and Fuzz testing

Threat Modelling Steps



Identifying Threats

Determining and Diagramming Potential attacks

Performing Reduction Analysis

Prioritization and Response

Identifying Threats – STRIDE approach

Microsoft Threat categorization scheme:

- **S**POOFING
- **T**AMPERING
- **R**EPUDIATION
- **I**NFORMAITON DISCLOSURE
- **D**ENIAL OF SERICE
- **E**LEVATION OF PRIVILEGES

Determining and Diagramming Potential Attacks

- Post identifying threats, the next step is to determine the potential attack concepts that could materialize
- Often accomplished by data flow diagrams, privilege boundaries, and elements involved
- Once diagram has been crafted, identify all the technologies involved.
- Identify attacks that could be targeted at each element of the diagram
- Attacks should include all forms – logical, physical, social

Perform Reduction Analysis

- Involves decomposing the application, system or environment
- Purpose of this process is to get a greater understanding on the purpose of the product and its interactions with external entities
- Each element should be evaluated to understand inputs, processing, security, data management, storage and output
- 5 key concepts to be aware of
  - Trust Boundaries – location where the level of trust changes
  - Data flow paths – movement of data between locations
  - Input points – locations where external input is received
  - Privilege Operations – Activity that requires greater privileges
  - Security stance and approach – Declaration of the security policy, security foundation and security assumptions

Prioritization and Response

- Document the threat – define the means, target and consequences of a threat
- After documentation, rank or rate the threats
- **DREAD** Rating System
    - **D**amage potential
    - **R**eproducibility
    - **E**xploitability
    - **A**ffected Users
    - **D**iscoverability

THREAT INTELLIGENCE

The definition of threat intelligence is sometimes confused with other cybersecurity terms. Most commonly, people confuse ‘threat data’ with ‘threat intelligence’ – but the two are not the same:

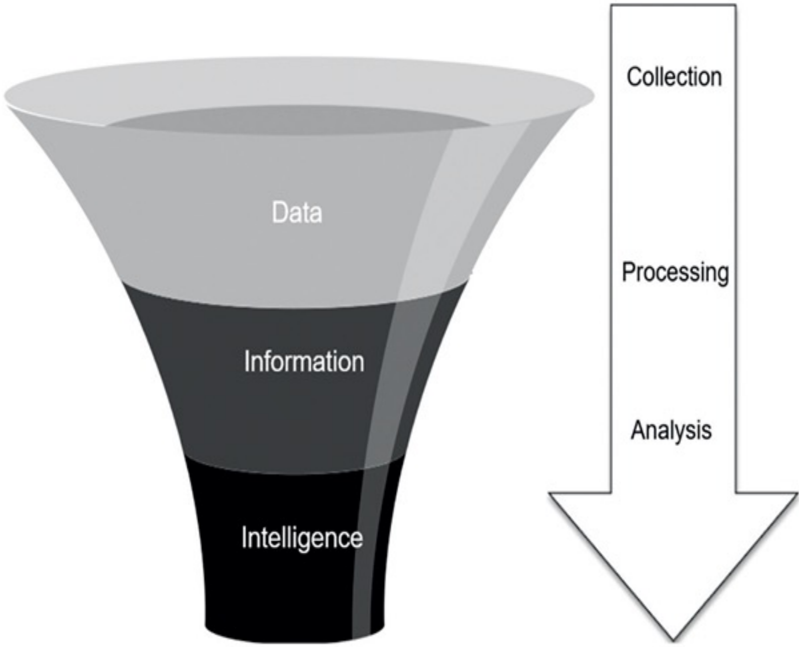
•Threat data is a list of possible threats.
•Threat intelligence looks at the bigger picture – by interrogating the data and the broader context to construct a narrative that can inform decision-making.

In essence, threat intelligence enables organizations to make faster and more informed security decisions. It encourages proactive, rather than reactive, behaviors in the fight against cyber attacks

Why is threat intelligence important?
Threat intelligence is a crucial part of any cybersecurity ecosystem. A cyber threat intelligence program, sometimes called CTI, can:

- Prevent data loss
- Provide direction on safety measures
- Inform others

Data vs information vs intelligence



The terms data, information and intelligence are often incorrectly used interchangeably.

Data refers to simple facts that tend to be available in large volumes. In the context of cyber security, IP addresses or logs are typical examples. By itself, raw data is of limited utility.

Information is produced when this data is collated to provide a useful output – for example, a collated series of logs showing a spike in suspicious activity.

Intelligence comes from the processing and analysis of this information and can be used to inform decision making. For example, the collated log data is contextualised with prior incident reports regarding similar activity, which also allows for the development of a strategy to mitigate the incident.

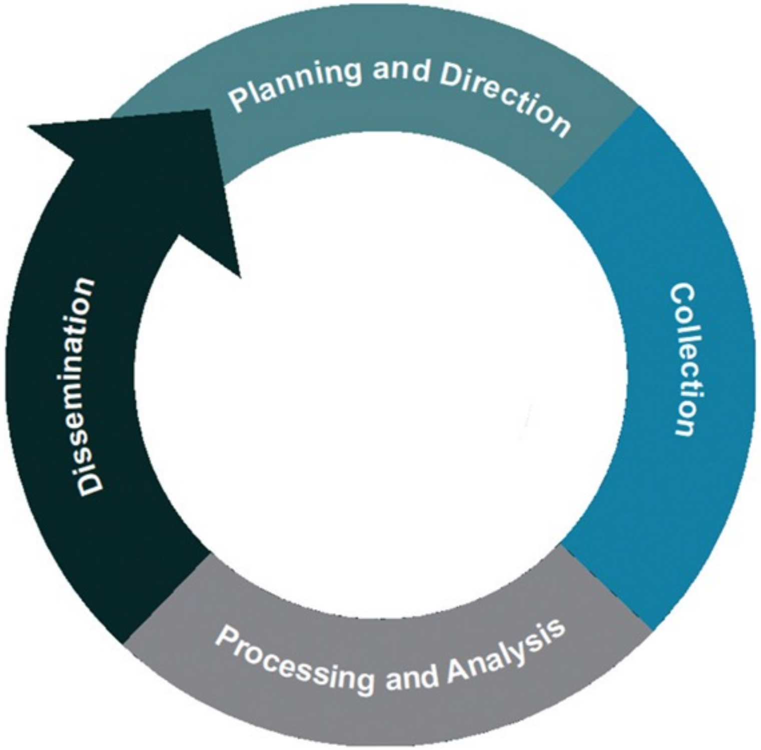
The intelligence cycle

Planning and direction, should determine the exact requirements of the consumer - often called intelligence requirements (IRs) or priority intelligence requirements (PIRs). From these IRs and PIRs, one can establish what data and information is required and how it should be collected.

Collection, involves gathering the data and information that is likely to meet the identified requirements.

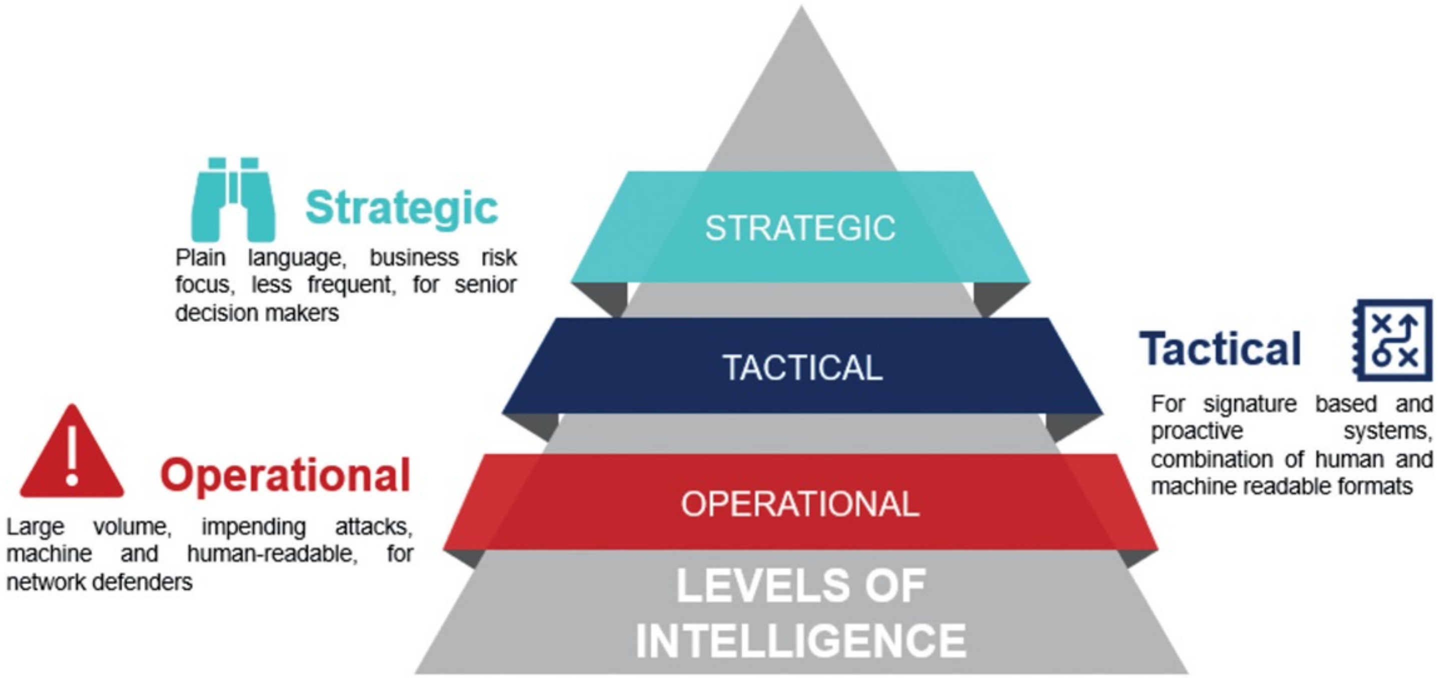
Processing and analysis, of raw data and information. Analysts use various techniques to assess the importance and implications of processed information, identify patterns, and interpret new knowledge.

Dissemination, involves timely delivery of completed intelligence products, in an appropriate format to the intended consumers. Feedback and refining of existing intelligence products can restart the cycle.



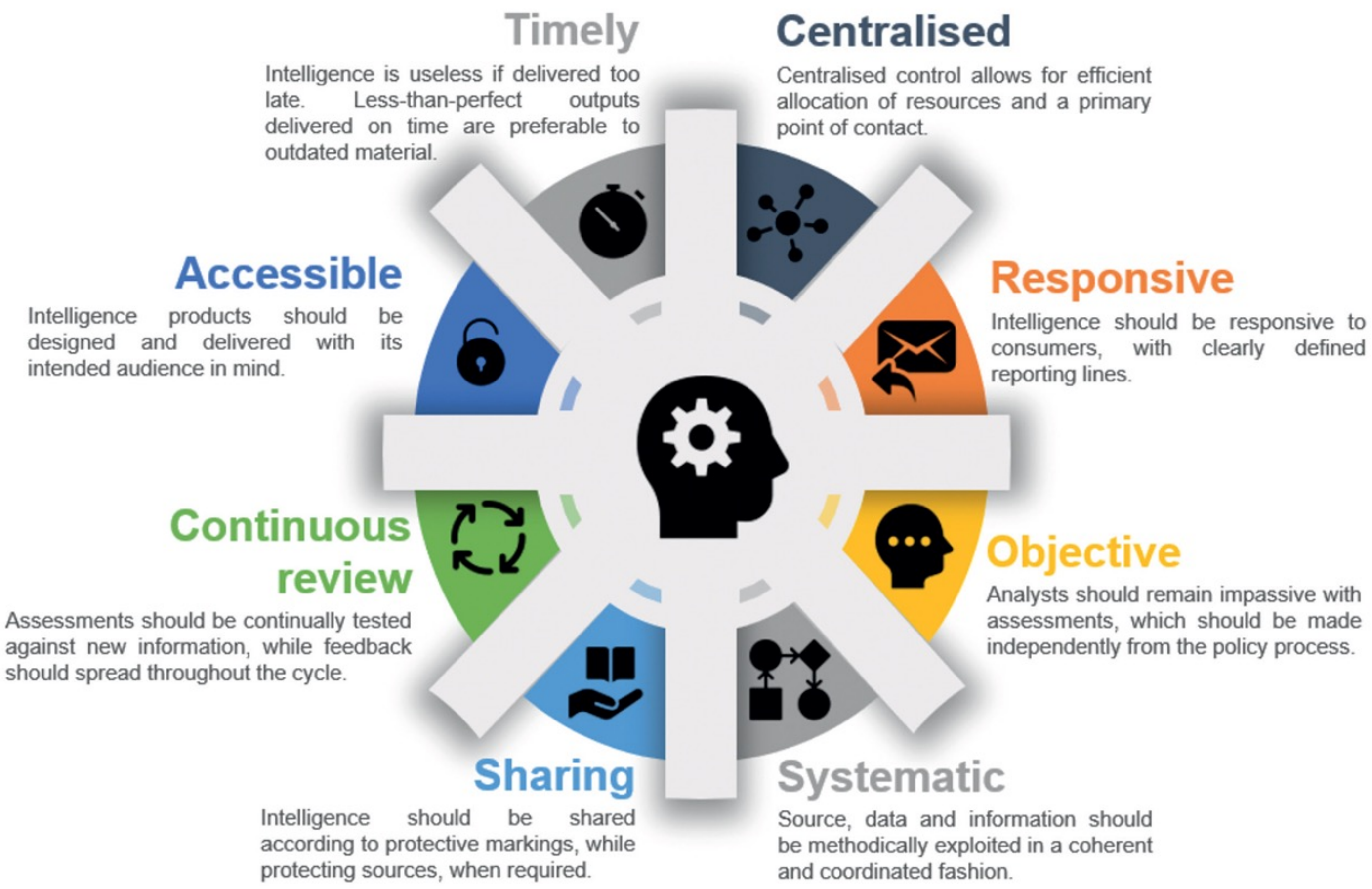
Levels of cyber threat intelligence

The different levels of cyber threat intelligence As with conventional intelligence, there are different levels of cyber threat intelligence: operational, tactical, and strategic. Each level differs in the nature and format of the material conveyed, its intended audience and its application. These are summarised in the infographic below.


Strategic
Plain language, business risk focus, less frequent, for senior decision makers
STRATEGIC
TACTICAL
Tactical
For signature based and proactive systems, combination of human and machine readable formats
Operational
Large volume, impending attacks, machine and human-readable, for network defenders
OPERATIONAL
LEVELS OF INTELLIGENCE

The principles of intelligence

The infographic beside summarises the principles that intelligence processes and products should adhere to. These principles are often known by the mnemonic CROSSCAT



Timely

Intelligence is useless if delivered too late. Less-than-perfect outputs delivered on time are preferable to outdated material.

Centralised

Centralised control allows for efficient allocation of resources and a primary point of contact.

Accessible

Intelligence products should be designed and delivered with its intended audience in mind.

Responsive

Intelligence should be responsive to consumers, with clearly defined reporting lines.

Continuous review

Assessments should be continually tested against new information, while feedback should spread throughout the cycle.

Objective

Analysts should remain impassive with assessments, which should be made independently from the policy process.

Sharing

Intelligence should be shared according to protective markings, while protecting sources, when required.

Systematic

Source, data and information should be methodically exploited in a coherent and coordinated fashion.

sources of Cyber threat intelligence

Commonly used sources by cyber threat intelligence providers include:

Indicators of compromise (IoCs) associated with malicious activity. Hashes of malware samples, IP addresses and domain names can all be used to update firewalls and detection systems, as well as contribute to an understanding of threat actors’ TTPs. IOCs are their own are more akin to data than processed intelligence, though are still included within the spectrum of cyber threat intelligence.

Client-derived data, such as that regarding its infrastructure or extracted from a security information and event management (SIEM) tool or other logs can be correlated with other sources, or for pro-active measures such as threat hunting.

Deep web, such as information from member-only hacking forums frequented by cybercriminals. These sources can provide valuable insight into the tools and services advertised and requested by cybercriminals, as well as identifying which exploits are being discussed to enable patch prioritisation.

Dark web will include marketplaces and shops that are hosted on anonymity-focused networks such as Tor or I2P which criminals use to purchase goods and services. This will enable consumers to identify if their data – ranging from login credentials to valuable intellectual property – is available or being advertised for sale, or if infrastructure they use may be targeted.

Threat Intelligence and Horizon Scanning: How to identify emerging threats

Horizon Scanning

- Horizon scanning is a strategic and systematic process used to detect and evaluate possible future risks and opportunities that may impact an organization or particular field. It involves actively monitoring and analyzing emerging trends, technologies, events, and developments on the horizon, typically over a longer time frame. The goal of horizon scanning is not to predict the future with certainty but to gain insights into potential scenarios and challenges that may arise.

- Essentially, horizon scanning helps organizations prepare for and navigate the uncertainties of the future.

- Integrating threat intelligence into horizon scanning processes can help organizations identify emerging threats and build operational readiness. By monitoring historical patterns and incidents, organizations can understand ongoing developments and assess potential threats.

Reference

- Alexander, D., Finch, A., Sutton, D. and Taylor, A. (2020) Information Security Management Principles BCS. 3rd edn. BCS The Chartered Institute for IT.

- Calder, A. and Watkins, S. (2019) IT Governance: An International Guide to Data Security and ISO27001/ISO27002. 7th edn. Kogan Page.

- Chapple, Mike - CISSP Official Study Guide (2021, Sybex). 9th edn.

- http://www.crest-approved.org