Chapter Two: Security Risk Management

Presented by:

Malek Ahmad AL Zebn
B.Sc. STUDENT AT THE UNIVERSITY OF JORDAN

Definition and Importance of Risk Management

- **Risk Management** involves identifying, assessing, controlling, and mitigating risks, with the goal of minimizing potential losses while accepting that complete elimination of risks is impractical.
- Key drivers of risk are **threats** (external or internal events with potential harm) and **vulnerabilities** (weaknesses that threats can exploit).
- risk management isn't intended to be risk elimination
- risks that can be minimized and implement controls

Elements of Risk Management

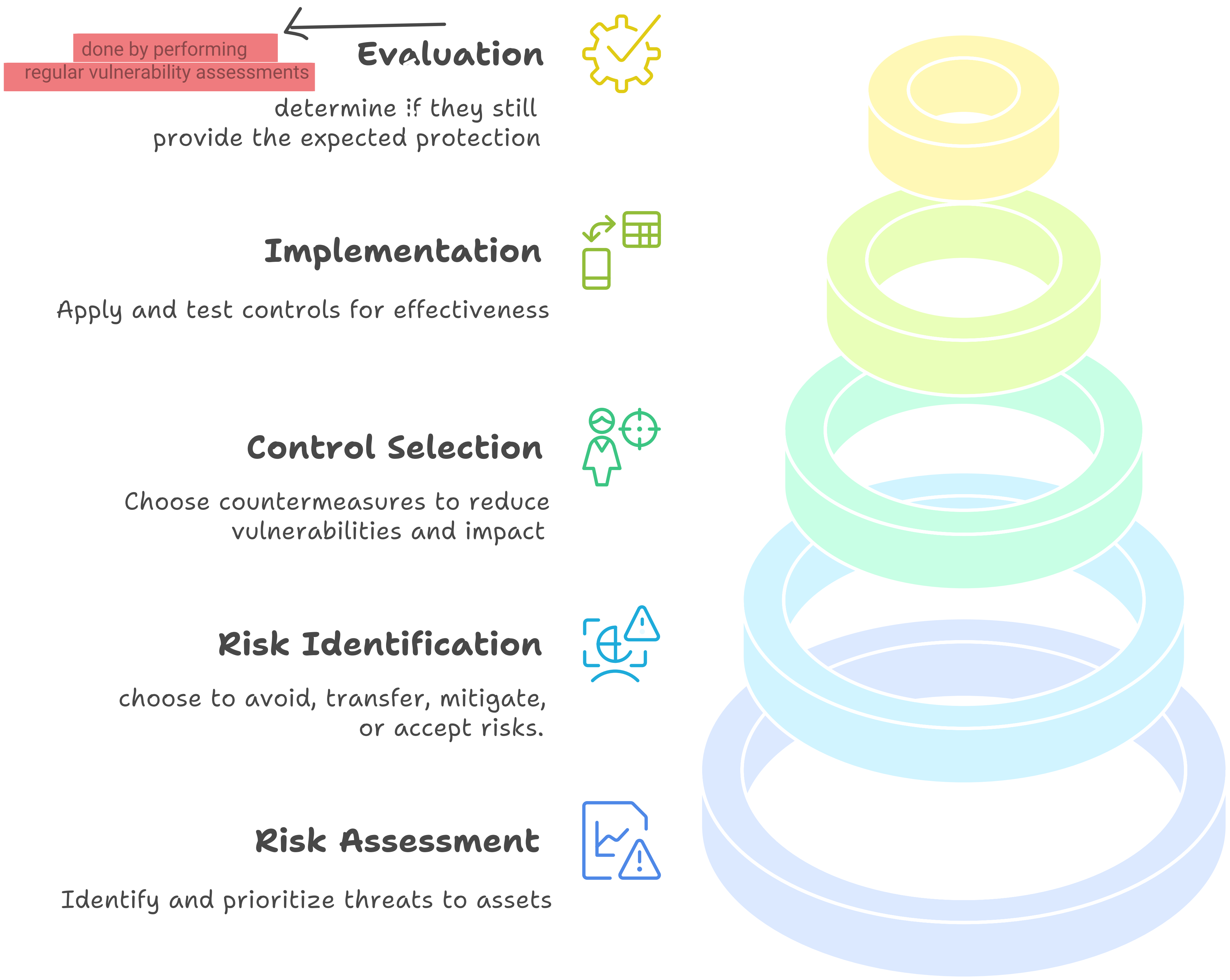
1. **Risk Assessment**:
   - Identify IT assets (etc , data, hardware) and their value.
   - Identify threats and vulnerabilities to these assets. Prioritize the threats and vulnerabilities.
   - Identify the likelihood a vulnerability will be exploited by a threat. These are your risks.
   - Identify the impact of a risk. Risks with higher impacts should be addressed first
2. **Risk Identification**:
   1. Risks can be managed by **avoiding**, **transferring**, **mitigating**, or **accepting** them.

Selecting appropriate controls (countermeasures) focuses on reducing vulnerabilities The decision is often based on the likelihood of the risk occurring, and the impact it will have if it occurs.

3. **Selection of controls**

   Control methods are also referred to as countermeasures. Controls are primarily focused on reducing vulnerabilities and impact
4. **Implementation and Testing**:Implementation and testing of controls—Once the controls are implemented, you can test them to ensure they provide the expected protection.
5. **Evaluation**:Risk management is an ongoing process. You should regularly evaluate implemented controls to determine if they still provide the expected protection. Evaluation is often done by performing regular vulnerability assessments.

IT Risk Management Hierarchy



done by performing regular vulnerability assessments

Evaluation

determine if they still provide the expected protection

Implementation

Apply and test controls for effectiveness

Control Selection

Choose countermeasures to reduce vulnerabilities and impact

Risk Identification

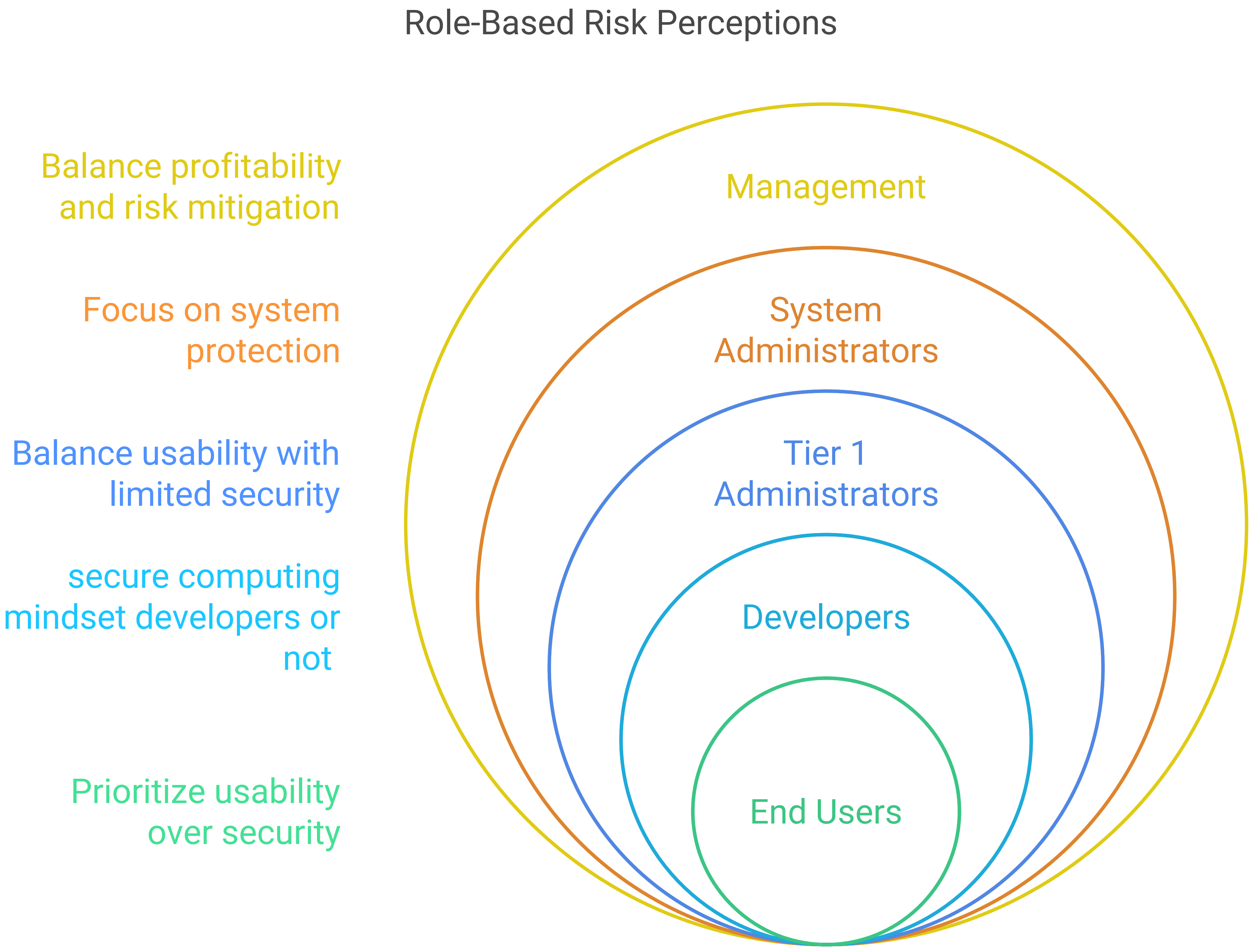
choose to avoid, transfer, mitigate, or accept risks.

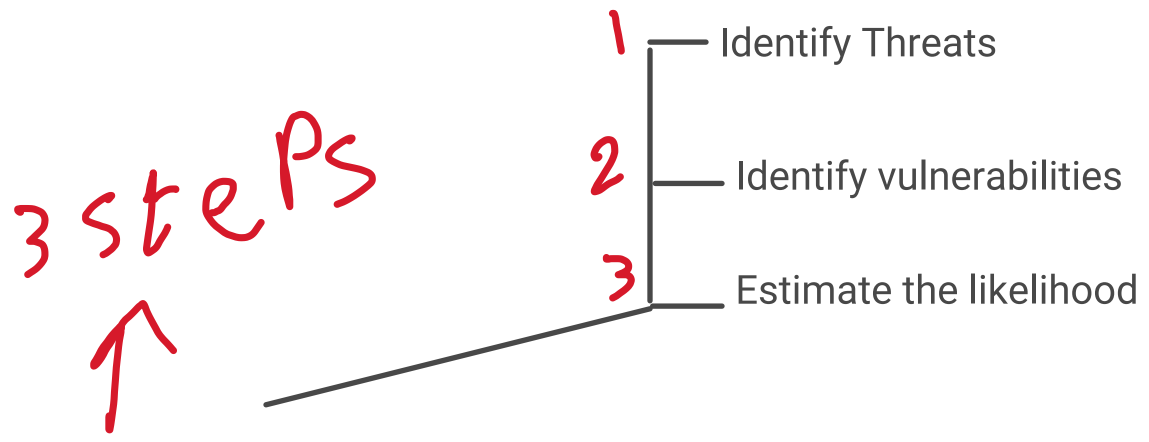
Risk Assessment

Identify and prioritize threats to assets

Role-Based Risk Perceptions

5. One of the challenges with effective risk management is achieving a proper balance between security and usability.
    - Risk perspectives by role:
        - **Management**: Balances profitability and survivability and risk mitigation costs Management needs accurate facts to make decisions on which controls to implement to protect company assets
        - **System Administrators**: responsible for protecting the IT systems Focuses on locking down systems but may overlook usability.
        - **Tier 1 administrator:** first line of defense for IT support , more concerned with usability than security or profitability they have limited administrative permissions.
        - **Developers**: a secure computing mindset developers They realize that security needs to be included from the design stage all the way to the release stage , developers haven't a security mindset, they try to patch security holes at the end of the development cycle. This patching mindset rarely addresses all problems, resulting in the release of vulnerable software
        - **End Users**: most concerned with usability , don't understand the reason for the security controls , try to break controls so they can complete their job.


Role-Based Risk Perceptions
Balance profitability and risk mitigation
Management
Focus on system protection
System Administrators
Balance usability with limited security
Tier 1 Administrators
secure computing mindset developers or not
Developers
Prioritize usability over security
End Users



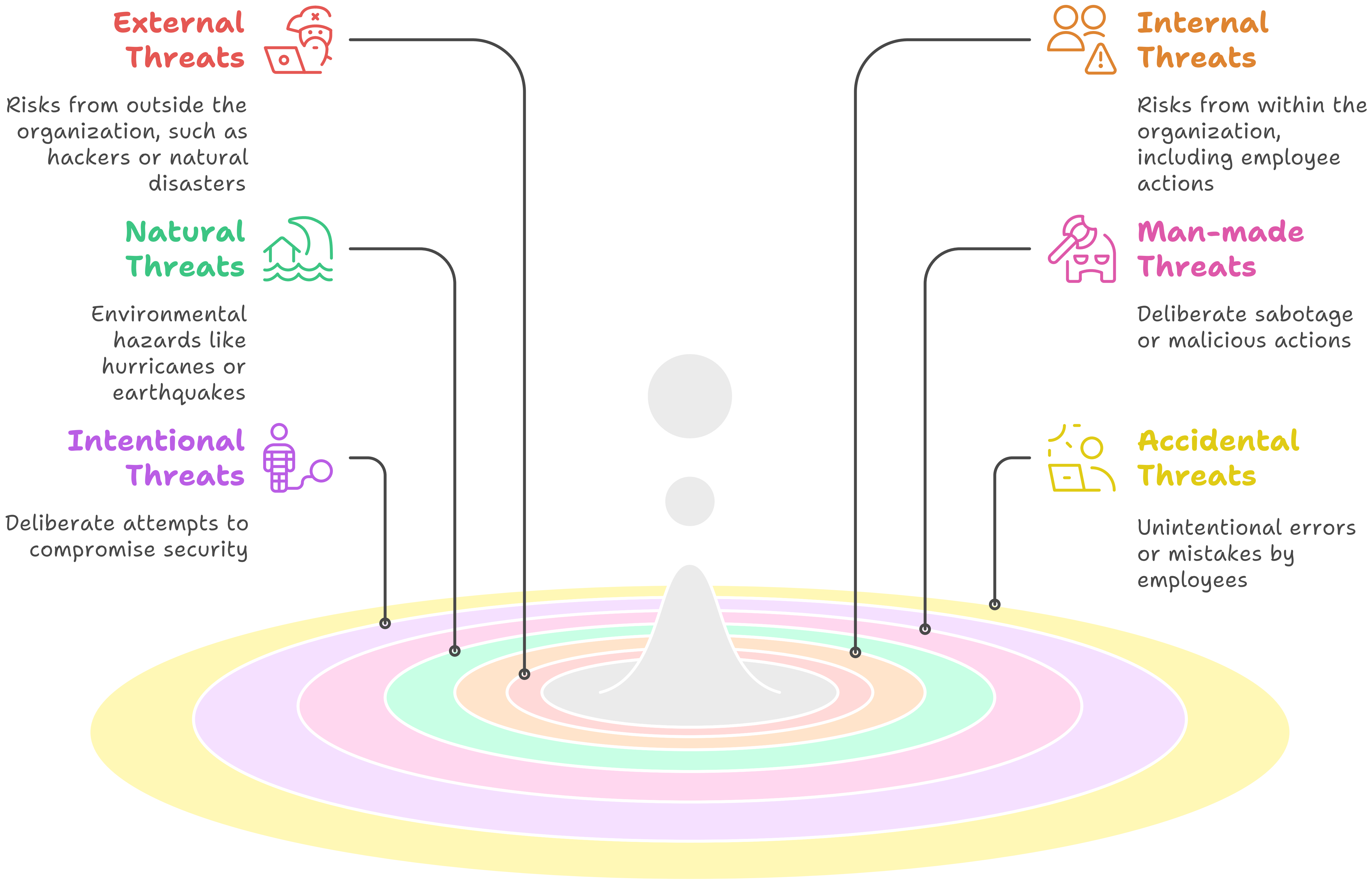
Risk Identification Techniques

step1 **Threat identification** : process of creating a list of threats. This list attempts to identify all the possible threats to an organization. This is no small task. The list can be extensive.

Categories of threats:

- **External/Internal**: External attackers outside the boundary of the organization can be risks that outside the control of the organization
- Internal threats are within the boundary of the organization related to employees or other personnel who have access to company resources
- **Natural/Man-made**: related to weather such as hurricane etc ,
- .manmade threat is any threat from a person any attempt to sabotage resources
- **Intentional/Accidental**: intentional is Any deliberate attempt to compromise → CIA confidentiality, integrity, or availability accidental threats are Employee mistakes or user error , brainstorming session is method used to identify threats

Risk Identification Techniques



External Threats

Risks from outside the organization, such as hackers or natural disasters

Natural Threats

Environmental hazards like hurricanes or earthquakes

Intentional Threats

Deliberate attempts to compromise security

Internal Threats

Risks from within the organization, including employee actions

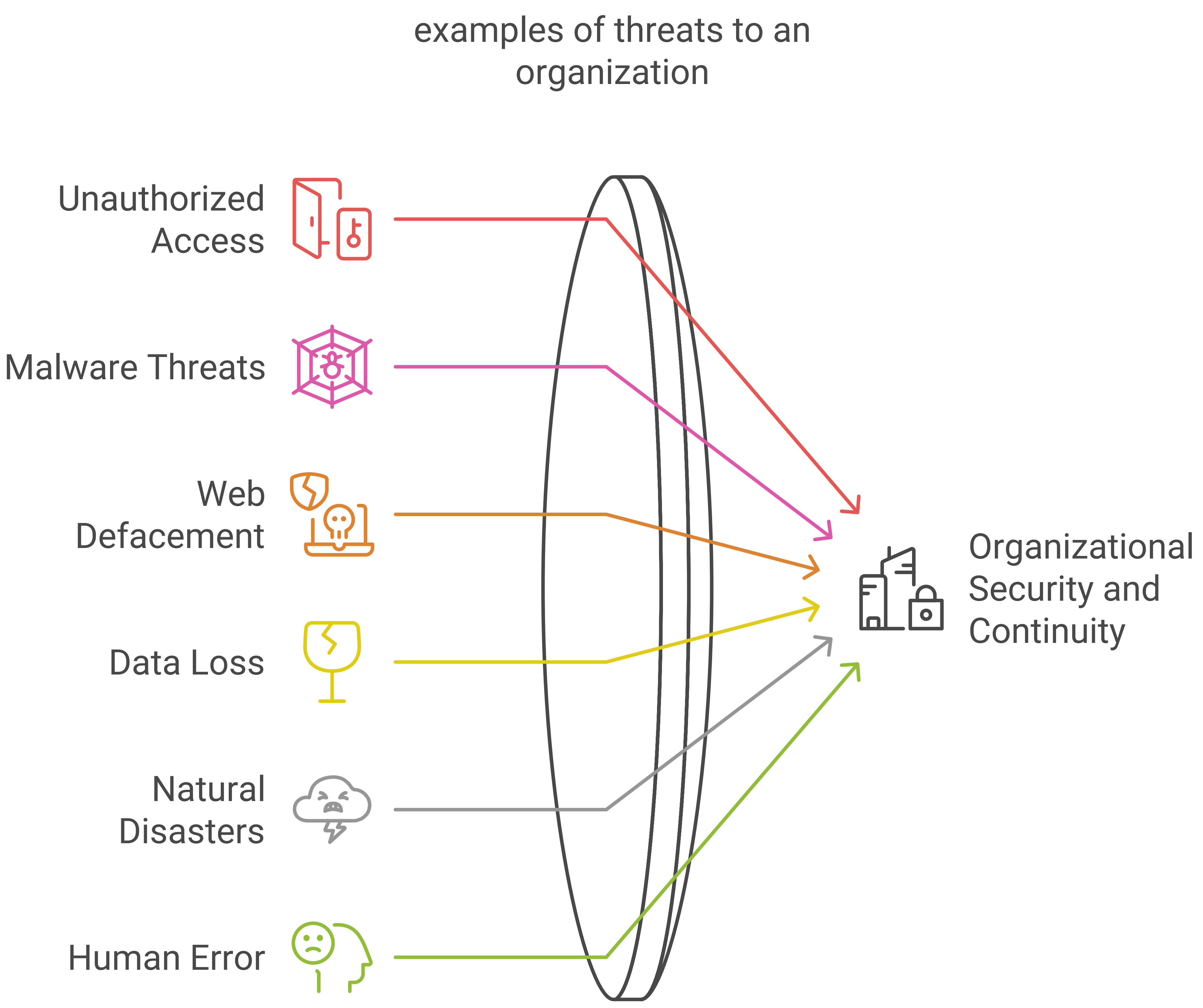
Man-made Threats

Deliberate sabotage or malicious actions

Accidental Threats

Unintentional errors or mistakes by employees

- Some examples of threats to an organization include



step 2

- **Identifying Vulnerabilities :** before threats occur, you'll have to dig a little to identify the weaknesses. Luckily, most organizations have a lot of sources which can help you.
    1. **System logs**—Audit logs can determine if users are accessing sensitive data.
    1. Firewall logs can identify traffic that is trying to breach the network and identify computers taken over by malware and acting as zombies.
    1. DNS logs can identify unauthorized transfer of data.

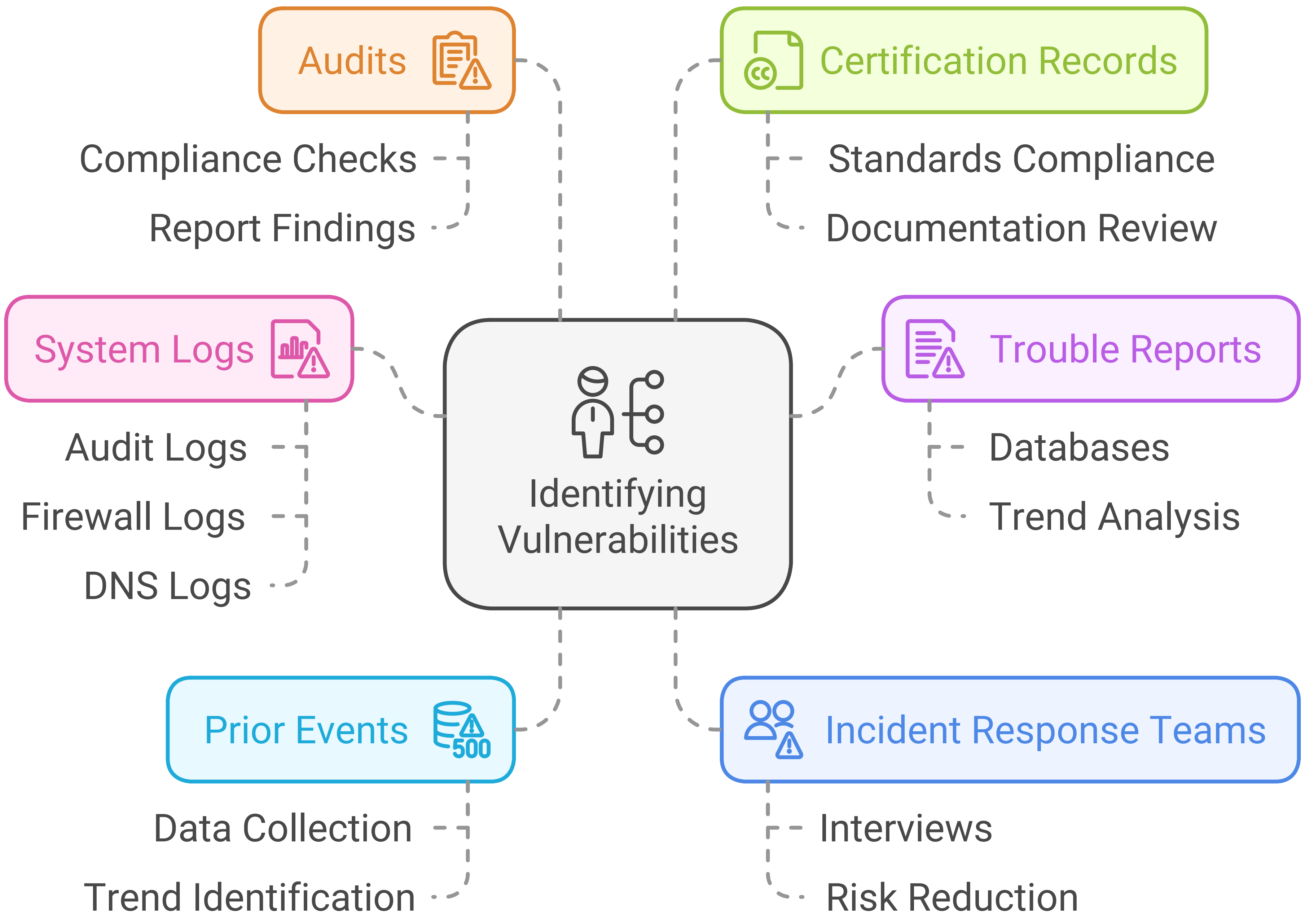
- 2.**Trouble reports**— use databases to document trouble calls. These databases can contain a wealth of information. With analysis, you can use them to identify trends and weaknesses

- 3. **Prior events**—Previous security incidents are excellent sources of data , they help justify controls. They show the problems that have occurred and can show trends.

4. **Incident response teams**— These teams will investigate all the security incidents within the company. These teams are often eager to help reduce risks. by interview team members and get a wealth of information

5.**Audits**— Systems and processes are checked to verify a company complies with existing rules and laws. At the completion of an audit, a report is created. These reports list findings which directly relate to weaknesses.

6. **Certification and accreditation records**— If the system meets the standards, the IT system can be accredited. The entire process includes detailed documentation. This documentation can be reviewed to identify existing and potential weaknesses.



step3

Estimate the likelihood of a threat exploiting a vulnerability Using the Seven Domains of a Typical IT Infrastructure

[1] User Domain—Social engineering represents a big vulnerability.

[2] Workstation Domain—Computers that aren't patched can be exploited.

[3] LaN Domain—Any data on the network that is not secured with right 'appropriate' access controls is vulnerable.

[4] LaN-to-WaN Domain— Firewalls with unnecessary ports open allow access to the internal network from the Internet that leads to make unneeded vulnerability to visit malicious Web sites

[5] WaN Domain—Any public-facing server is susceptible to DoS and DDoS attacks. A File Transfer Protocol (FTP) server that allows anonymous uploads can host malware "Warez" from black-hat hackers

[6] Remote access Domain—Remote users may be infected with a virus but not know it. When they connect to the internal network via remote access, the virus can infect the network.

[7] System/application Domain—Database servers can be subject to SQL injection attacks. In a SQL injection attack, the attacker can read the entire database. SQL injection attacks can also modify data in the database.

- **Pairing Threats with Vulnerabilities**

Threats are matched to existing vulnerabilities to determine the likelihood of a risk

Risk = Threat X Vulnerability

Risk Management Techniques

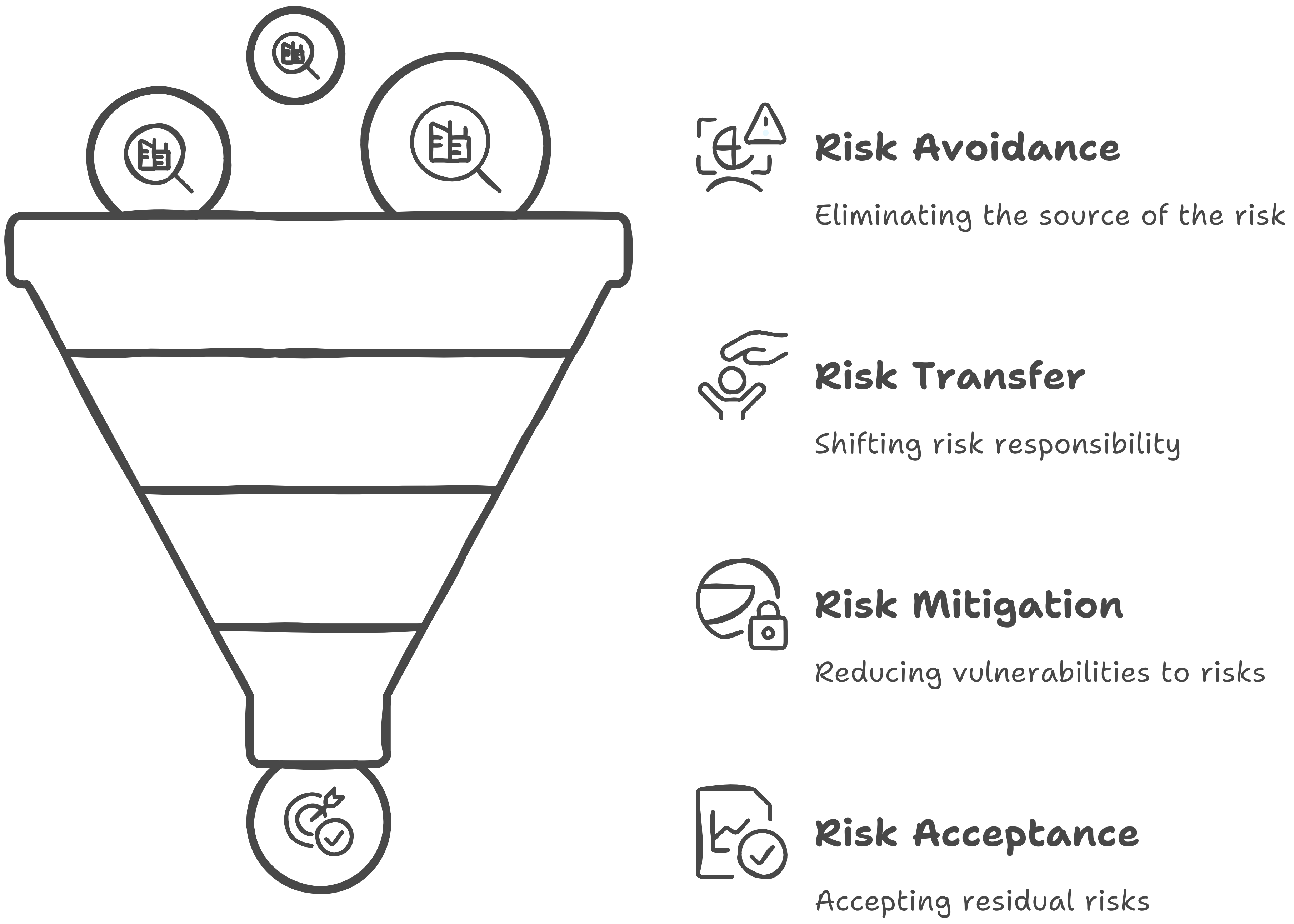
important to realize that risk management is not risk elimination.
The ultimate goal of risk management is to protect the organization
helps ensure a business can continue to operate and earn a profit

- **Avoidance**: Eliminating the source of the risk—The company can stop the risky activity.,Eliminating the exposure of assets to the risk—The company can move the asset

- **Transfer**: Shift risk responsibility, e.g., via insurance or outsourcing.

- **Mitigation**: reduce risk by reducing vulnerabilities the goal is not to eliminate the risk but instead, to make it too expensive for the attacker.
- physical environment—Replace hubs with switches.
- Change procedures—Implement a backup plan
- Add fault tolerance Use failover clusters to protect servers
- Modify the technical environment Use “IDS“
- Train employees
- **Acceptance**: Accept residual risks when mitigation costs exceed potential loss.This is commonly done when the cost of the control outweighs the potential loss.
- The decision to accept a loss by evaluate the cost Using CBA

Risk Management Process Funnel


Risk Avoidance
Eliminating the source of the risk
Risk Transfer
Shifting risk responsibility
Risk Mitigation
Reducing vulnerabilities to risks
Risk Acceptance
Accepting residual risks

Cost-Benefit Analysis (CBA)

CBA starts by gathering data to identify the costs of the controls and benefits gained if they are implemented.

Cost of the control—This includes the purchase costs plus the operational costs over the lifetime of the control.

Projected benefits—This includes the potential benefits gained from implementing the control

hidden costs may be:-

Costs to train employees-

Costs for ongoing maintenance-

Software and hardware renewal costs

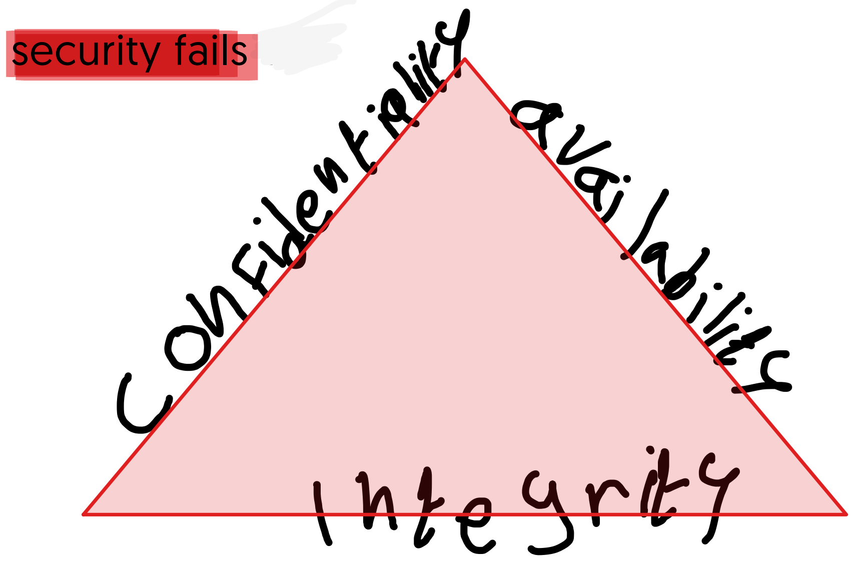
Evaluates the viability of risk controls by comparing their costs and benefits.

Helps in decisions like whether to implement, avoid, or transfer risks.

- **best practices to protect protect servers** : Remove unneeded services and protocols. Change default passwords. • Regularly patch and update the server systems. Enable local firewalls.

Note :If any side of the triangle is breached or fails, security fails

CIA



Impact of Threat

- Risks to **confidentiality**, **integrity**, and **availability** represent potential losses.
- Impacts categorized as:
  - **High**: Major resource loss, harm to mission or reputation.
  - **Medium**: Costly resource loss or mission impediments.
  - **Low**: Minor resource loss or minor mission impact.

OUR WEBSITE: https://errorcatchers.odoo.com