IDENTITY ACCESS MANAGEMENT(IAM)

&

THREATS, VULNERABILITIES AND RISKS. RISK ANALYSIS.

Bucharest

October 2021

AGENDA

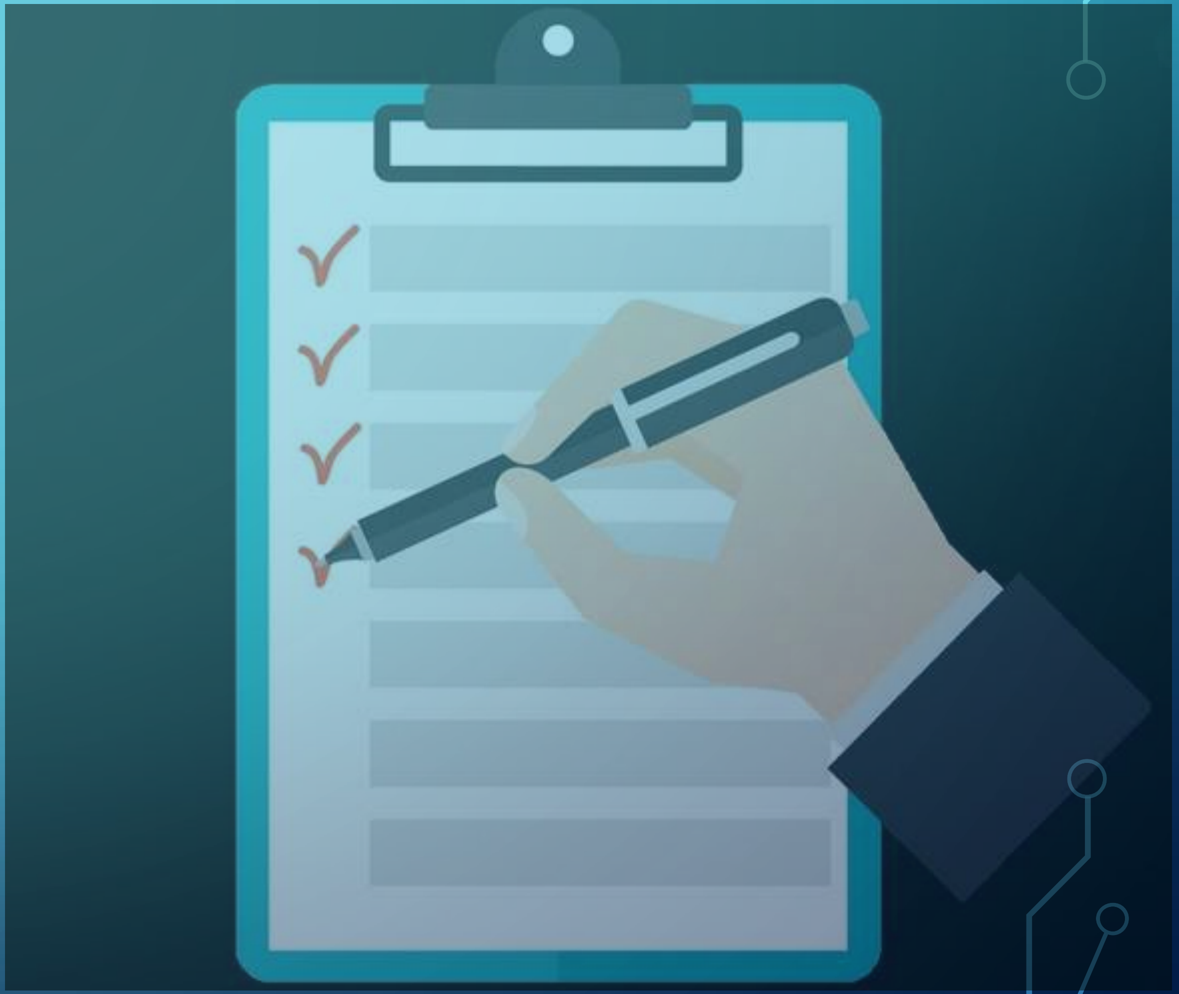
Identity Access Management (IAM)

- ✓ Access Control Overview
- ✓ Access Control Models
- ✓ Access Control Technologies
- ✓ Identity as a Service
- ✓ User Provisioning Lifecycle
- ✓ Threats to access control

Threats, vulnerabilities and risks

- ✓ Introduction
- ✓ Definitions
- ✓ Risk identification
- ✓ Risk assessment
- ✓ Risk mitigation

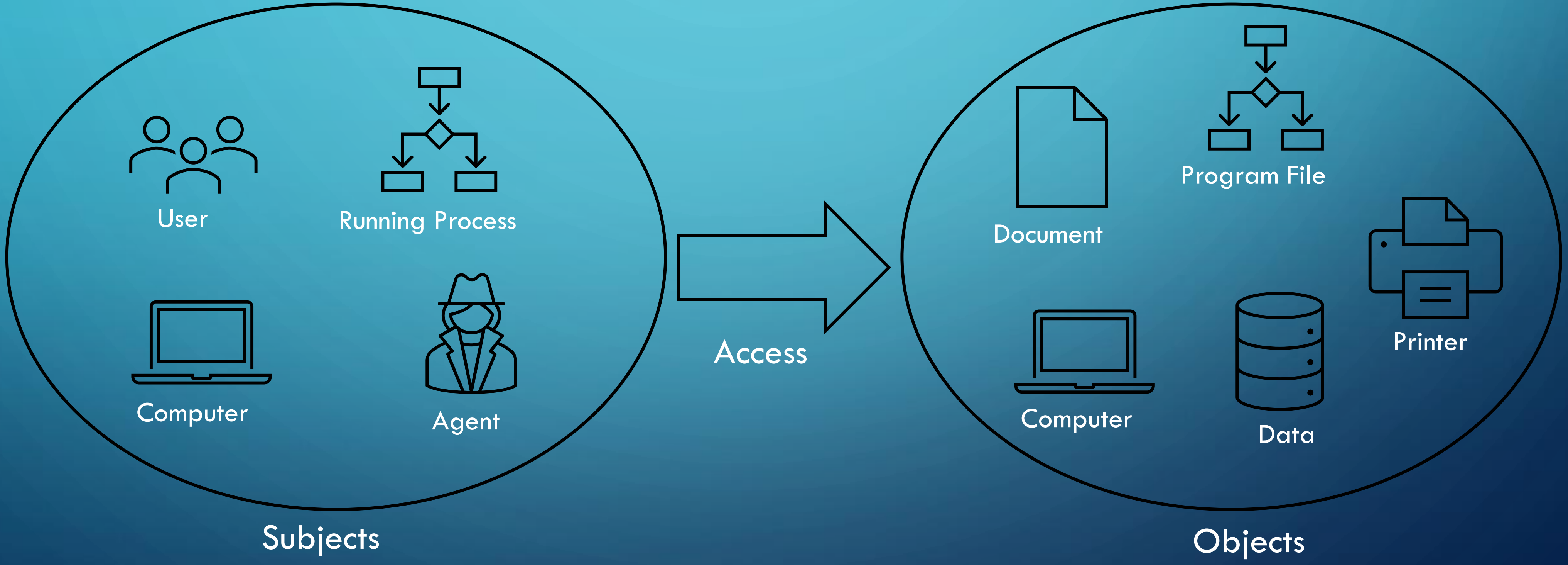
Lab – risk assessment



IDENTITY ACCESS MANAGEMENT (IAM)

Access Control Overview

What is **Access Control**?



IDENTITY ACCESS MANAGEMENT (IAM)

Access Control Overview

Access control:

- ✓ Restricted access to a resource or a place.
- ✓ Security feature that control how users and systems communicate and interact with other systems and resources.

Access control give ability to Control, Restrict, Monitor and Protect resource **availability, integrity and confidentiality**.

IDENTITY ACCESS MANAGEMENT (IAM)

Access Control Overview

Access Control Phases:

- Identification - username, user ID, account number
- Authentication - passphrase, PIN value, thumbprint, smart card, OTP
- Authorization - I know who you are, now what am I going to allow you to do?
- Accountability - Audit logs and monitoring to track subject activities with objects

The last three phases are known as AAA Principle (triple A).

IDENTITY ACCESS MANAGEMENT (IAM)

Access Control Overview

Account Privilege Principles:

- Least privilege
- Separation of duties
- Job rotation
- Account lifecycle.

Golden Principle

- **Implicit Deny**

IDENTITY ACCESS MANAGEMENT (IAM)

Access Control Models

- **Mandatory Access Control (MAC)** – users are given security clearance (labels): secret, top secret, confidential, etc. and data is classified in the same way (security labels for each object). System is hard to maintain, all changes can be done only by administrators. Usually used in government and military institutions.
- **Discretionary Access Control (DAC)** – permissions can be set by the owner of the resource (file, computer, other), specifying which subjects can access specific resources (ACLs). Example: Windows New Technology File System permissions (full control, read/write, read only)
- **Role Based Access Control (RBAC)** – access to resources be based on the role the user holds within the company. Administrators group permissions into functional roles and users are assigned to those roles.
- **Rule Based Access Control (RBAC)** – uses specific rules (security policies) that indicate what can and cannot happen between a subject and an object

IDENTITY ACCESS MANAGEMENT (IAM)

Access Control Models

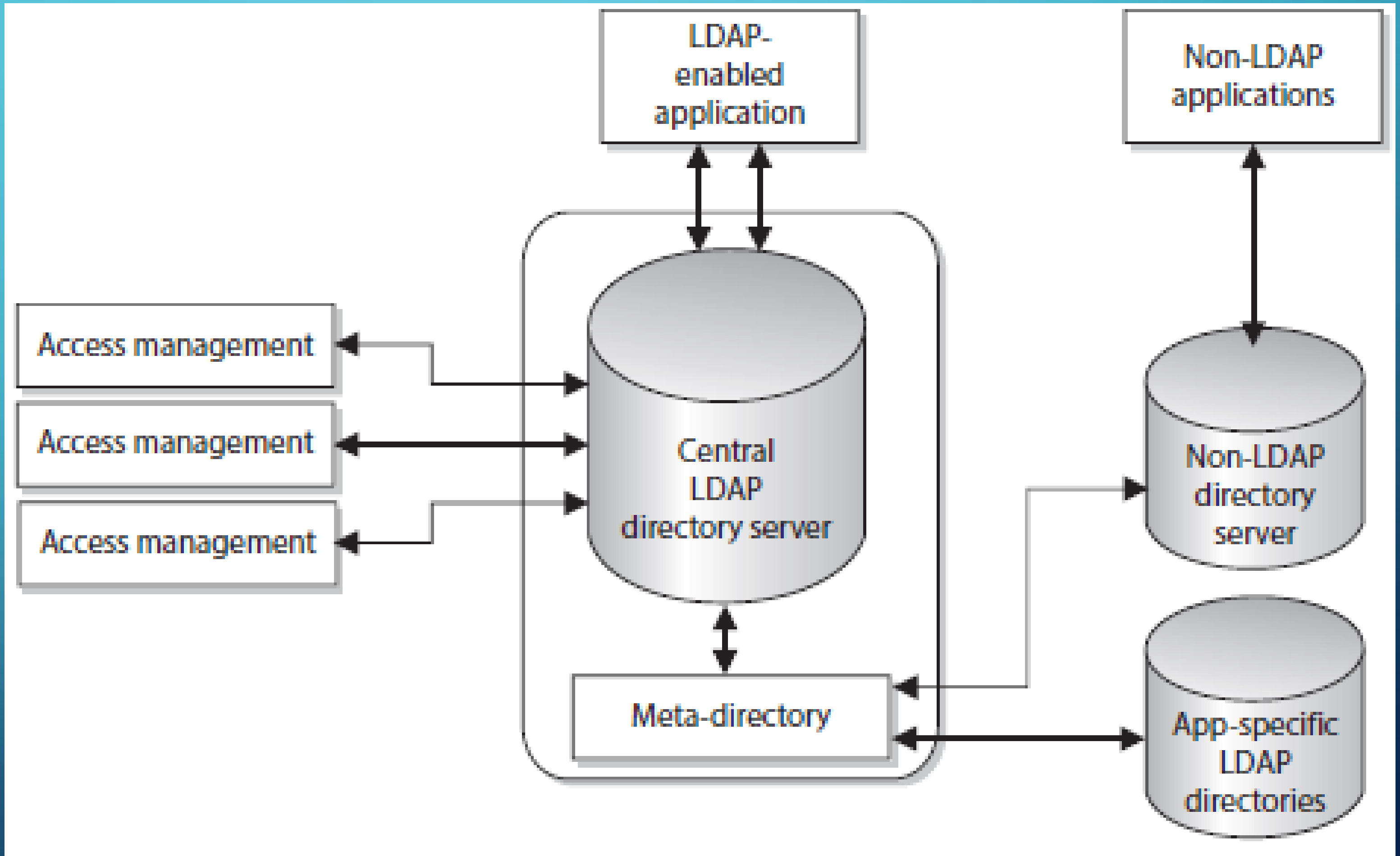
Access control techniques are used to support the access control models.

- **Access control matrix** - Table of **subjects and objects** that outlines their access relationships (No Access, Read Only, Read/Write, Execute)
- **Access control list** - Bound to an **object** and indicates what subjects can access it and what operations they can carry out
- **Capability table** - Bound to a **subject** and indicates what objects that subject can access and what operations it can carry out
- **Content-based access** - Bases access decisions on the sensitivity of the data, not solely on subject identity
- **Context-based access** - Bases access decisions on the state of the situation, not solely on identity or content sensitivity
- **Restricted interface** - Limits the user's environment within the system, thus limiting access to objects

IDENTITY ACCESS MANAGEMENT (IAM)

Access Control Overview

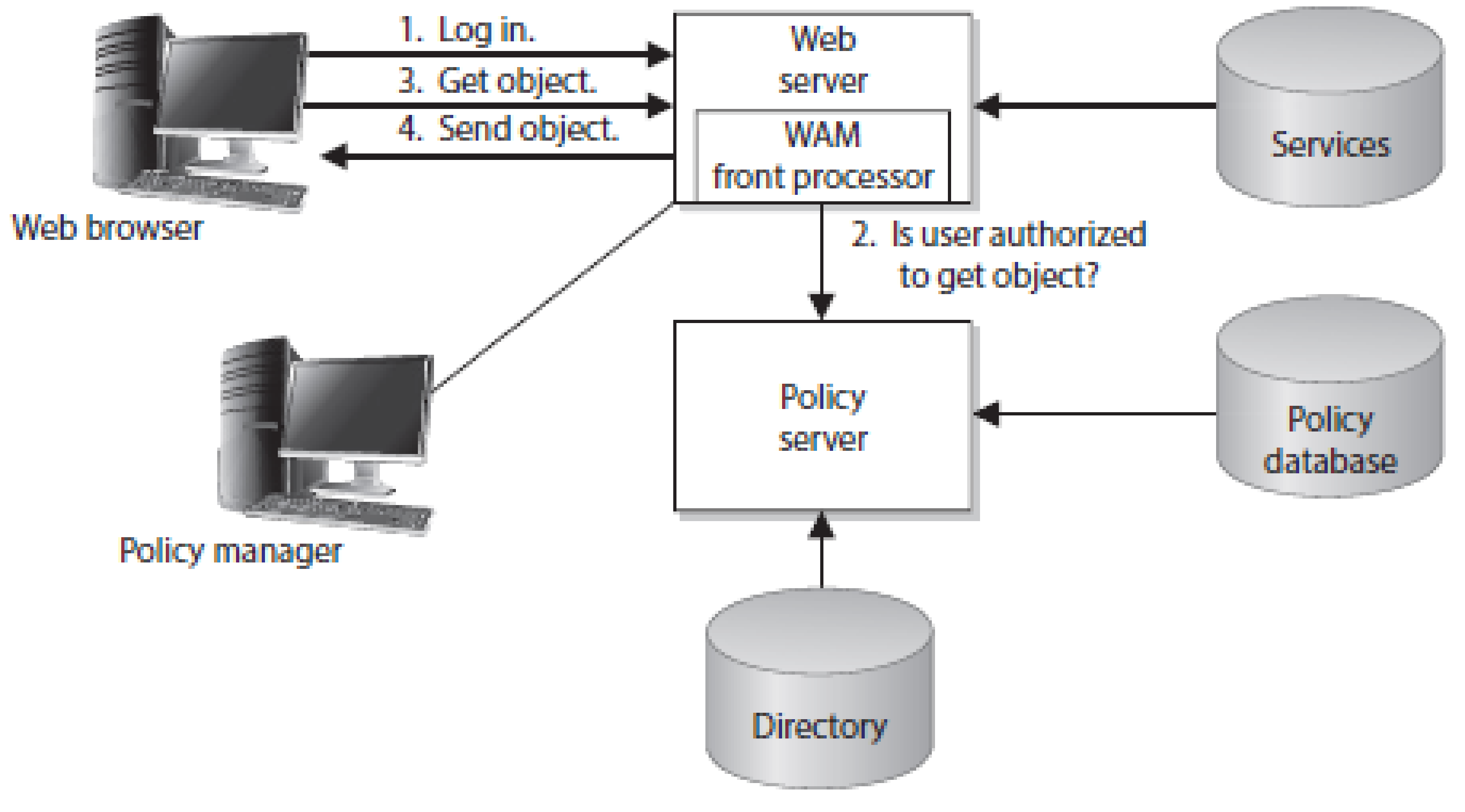
Directory Services:



IDENTITY ACCESS MANAGEMENT (IAM)

Access Control Overview

Web Access Management:



IDENTITY ACCESS MANAGEMENT (IAM)

Access Control Technologies

- Radius (Remote Authentication Dial-In User Service) - network protocol that provide client/server combined authentication, authorization and audit.

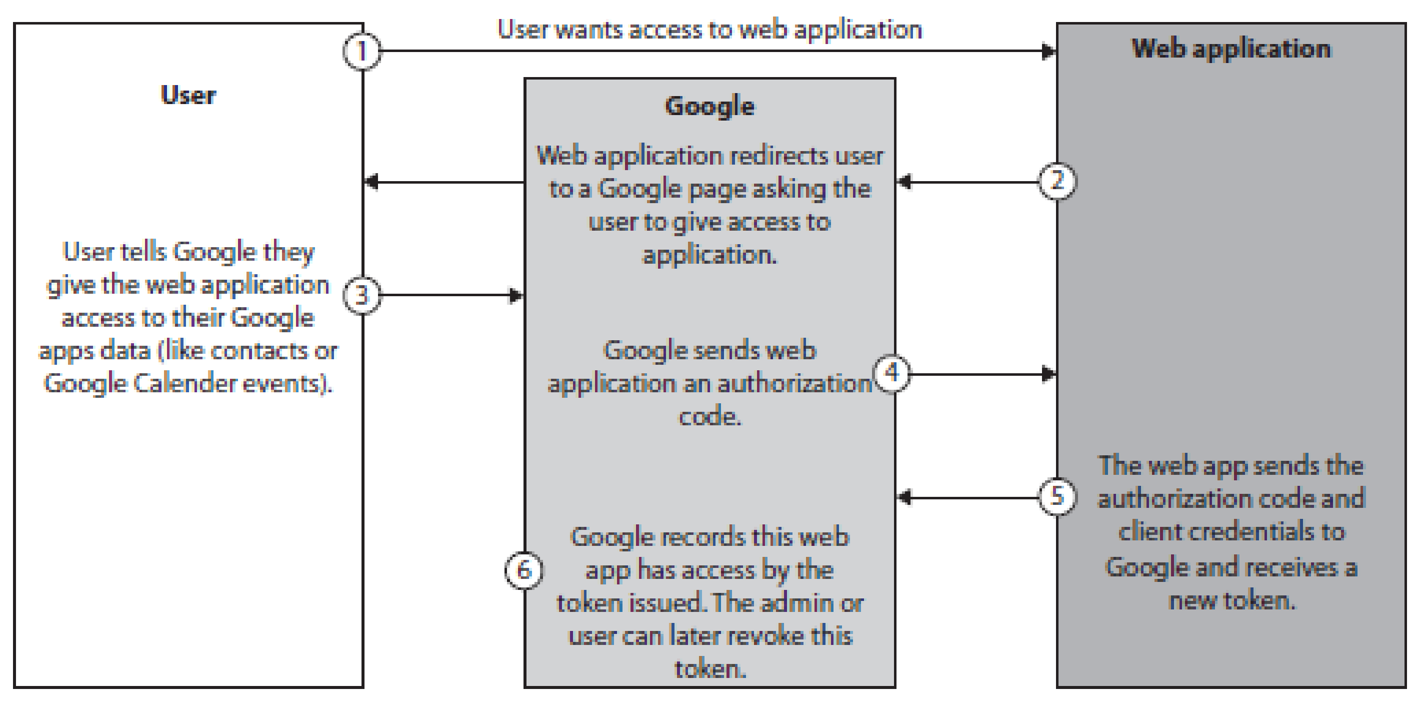
- TACACS (Terminal Access Controller Access Control System) – CISCO proprietary protocol developed in multiple formats like XTACACS, TACACS+

- Diameter - build upon the functionality of RADIUS and overcome many of its limitations

IDENTITY ACCESS MANAGEMENT (IAM)

Identity as a Service

Identity as a Service (IDaaS) is a type of Software as a Service (SaaS) offering that is normally configured to provide SSO, federated IdM, and password management services



Web application redirects user to a Google page asking the user to give access to application.

User tells Google they give the web application access to their Google apps data (like contacts or Google Calender events).

Google sends web application an authorization code.

The web app sends the authorization code and client credentials to Google and receives a new token.

Google records this web app has access by the token issued. The admin or user can later revoke this token.

IDENTITY ACCESS MANAGEMENT (IAM)

Identity as a Service

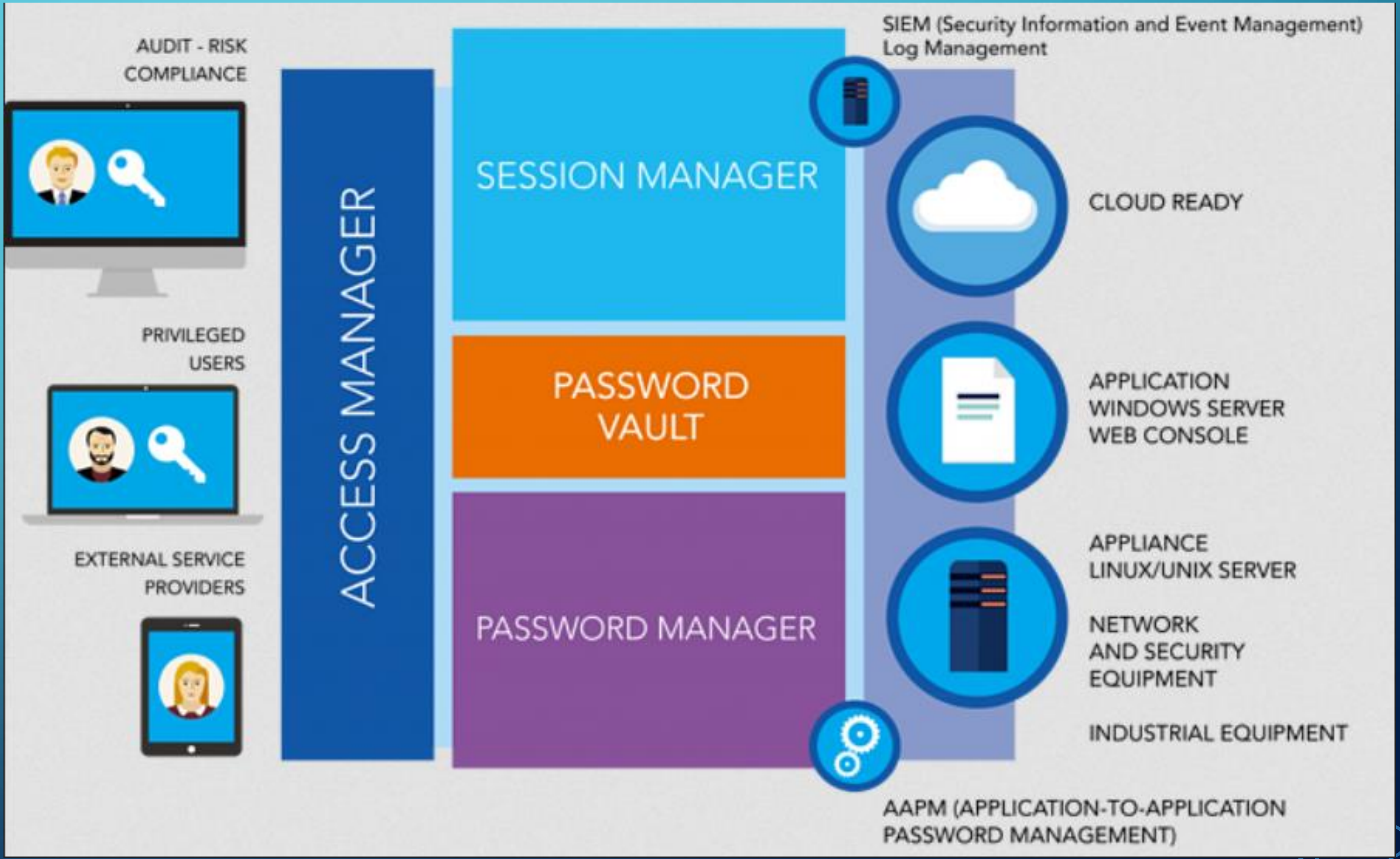
Top providers:

- Azure Active Directory
- IBM Security Identity and Access Assurance
- Oracle Identity Cloud Service
- Okta
- Centrify
- RSA SecurID Access

IDENTITY ACCESS MANAGEMENT (IAM)

Identity as a Service

Privilege Access Management



IDENTITY ACCESS MANAGEMENT (IAM)

User Provisioning Lifecycle

- ✓ Onboarding (Provisioning user)
  - ✓ Documentation / Change Control
  - ✓ User Agreement / NDA
  - ✓ Account Creation
  - ✓ Orientation + Trainings
- ✓ Authorization & Assignment
  - ✓ No by default,
  - ✓ Add to group,
  - ✓ Assign privileges
  - ✓ Other security awareness trainings
- ✓ Access Review (Audit & Maintain)
  - ✓ Disable inactive accounts
  - ✓ Audit permissions
  - ✓ Audit activity
  - ✓ Recertification
- ✓ Offboarding
  - ✓ Reclaim of assets (tokens)
  - ✓ Disable accounts (time of disabling)
  - ✓ Signs documents

IDENTITY ACCESS MANAGEMENT (IAM)

Threats to access control

- Social engineering
- Impersonation attack
- Dictionary attacks
- Brute-force attacks
- Watering hole attacks
- Spoofing at Logon
- Phishing and Pharming
- Network sniffers

Threats, vulnerabilities and risks

THREATS, VULNERABILITIES AND RISKS

How does a regular organization look like

An organization can be structured on:

- Horizontal: meaning peer departments/teams
- Vertical: meaning that there is a hierarchy
- Depth: meaning same field of activity but different purpose

INTRODUCTION

Vulnerability ≠ Threat ≠ Risk

Vulnerability (& patching) Management

Threat Management

Threat Intelligence

Threat Hunting

Risk Management

Information Risk Management

Audit

DEFINITIONS

- **Vulnerability =** a weakness or a flaw that would expose an asset to intentional or unintentional harm or perturbation.

Vulnerabilities are classified according to the asset class they are related to:

Hardware

- susceptibility to humidity, dust, temperature
- susceptibility to unprotected storage
- age-based wear that causes failure

Software

- insufficient testing
- insecure coding
- lack of audit trail

Network

- unprotected communication lines
- insecure network architecture

- Personnel
  - inadequate recruiting process
  - inadequate security awareness
  - insider threat
- Physical site
  - area subject to natural disasters (e.g. flood, earthquake)
  - interruption of power source
- Organizational
  - lack of regular audits
  - lack of continuity plans
  - lack of security

EXAMPLE - VULNERABILITY

Vulnerabilities in software.

e.g.

- the software does not properly handle user input
- the software does not properly handle the user access

Vulnerabilities in processes.

e.g.

- one user have the responsibility of initiating and approving payments
- a critical system is not implemented to have backup

Other

DEFINITIONS

- **Threat =** anything that is capable and have the intent and the opportunity to act against an asset in a manner that can result harm or perturbation.
  - **Capability:** the degree to which the adversary can succeed in accomplishing objectives;
  - **Opportunity:** conditions(technical, logistical, legal, etc.) necessary to threat actor to accomplish objectives;
  - **Intent:** what the threat actor seeks to achieve;

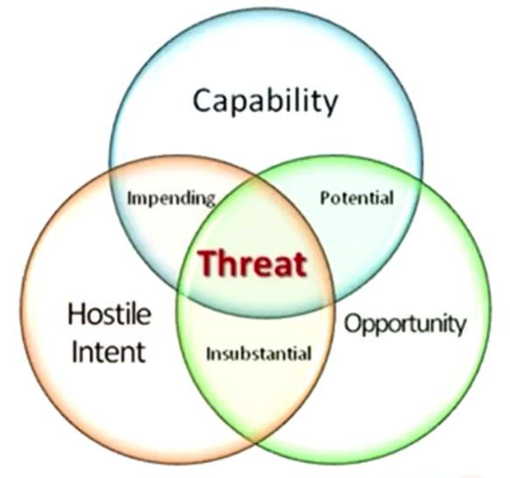
- Threat types:
  - Environmental (floods, tornados, hurricane, earthquake)
  - Manmade
  - Internal vs External
- A threat can belong to one or more of above categories.

- A threat vector == method used by attacker to get to the target

EXAMPLE - THREAT

A cyber criminal group using private infrastructure to target banks clients via phishing attacks.

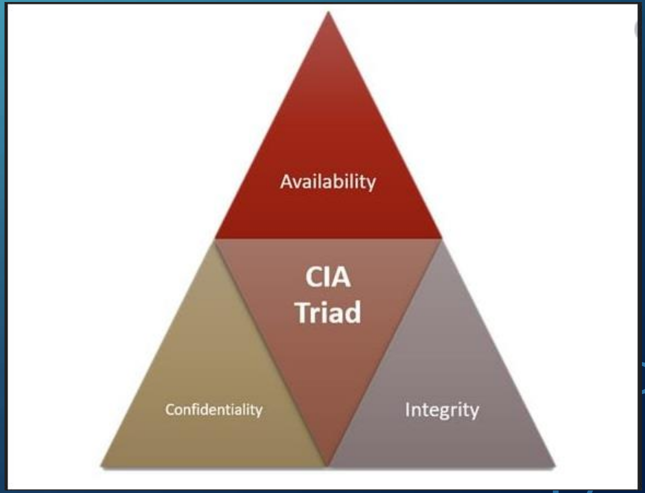
A nation state sponsored group that leverage 0-day exploits to compromise high profile organizations to steal intellectual property.



DEFINITIONS

Risk

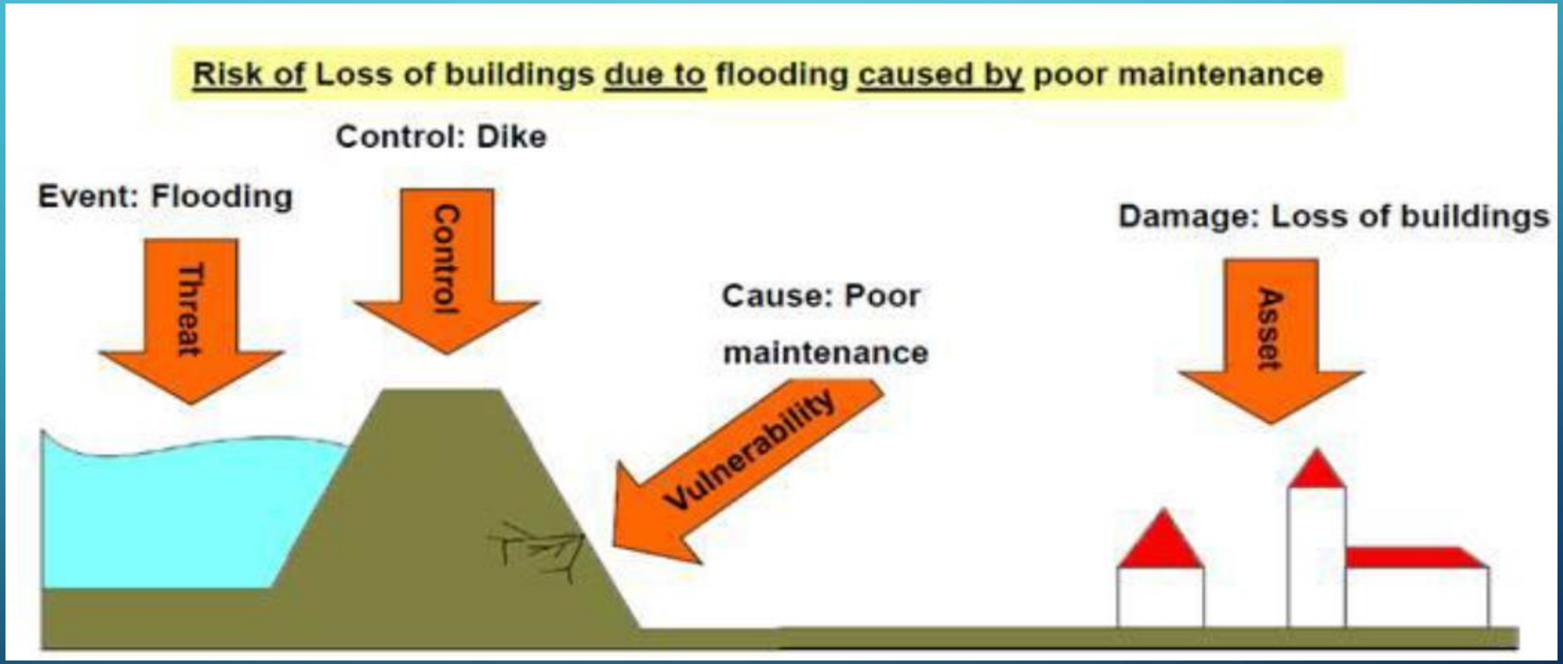
IT Risk = The risk of financial and reputational loss due to events leading to breaches of **confidentiality, integrity and availability** of business processes or information caused by inadequate information and IT security.



Operational Risk = The risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems, or from external events

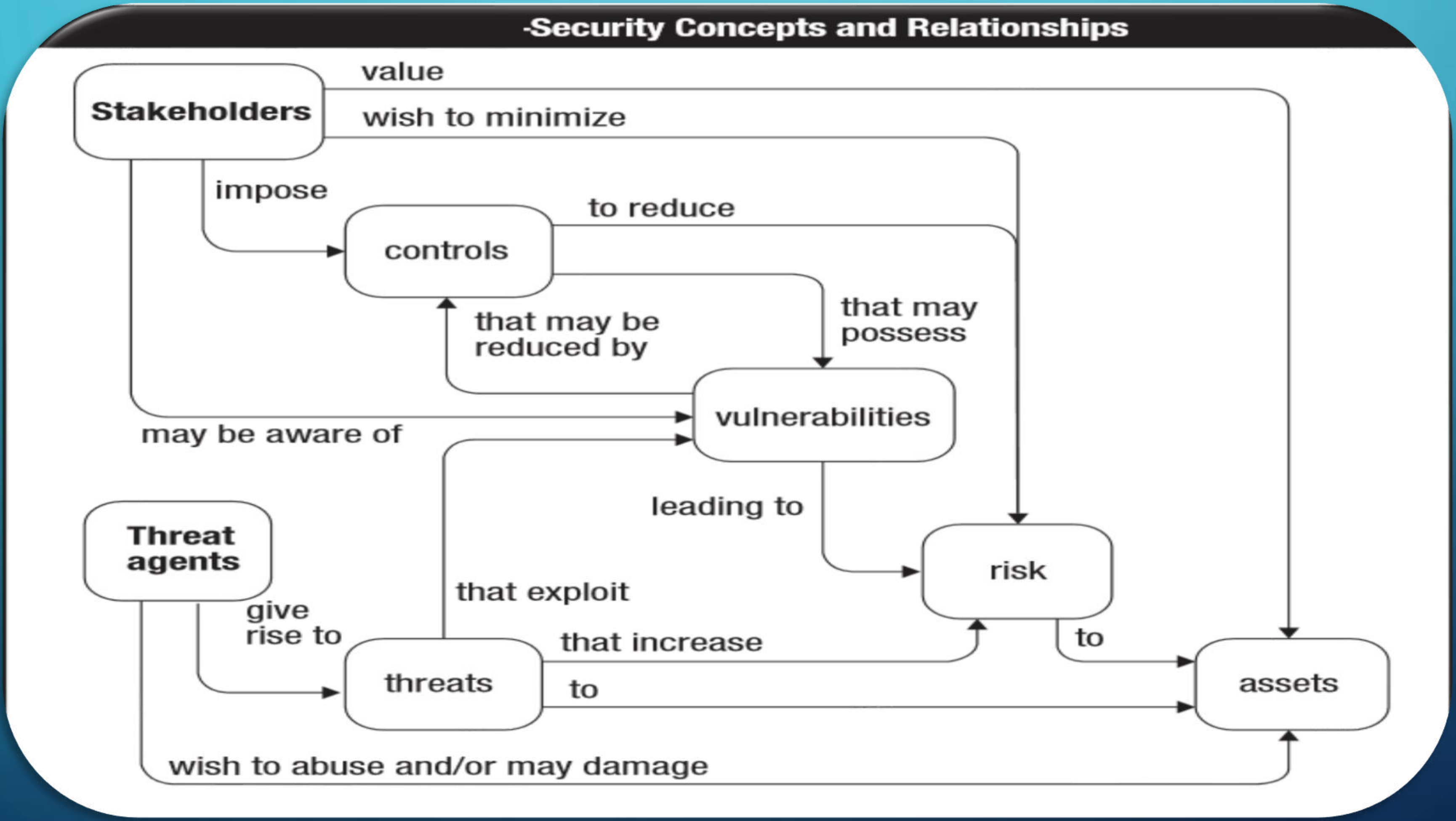
EXAMPLE - RISK

Risk of loss (financial or reputational) due to ransomware infections caused by lack of antivirus installed on the workstation.



Risk of Loss of buildings due to flooding caused by poor maintenance

BRINGING IT ALL TOGETHER



-Security Concepts and Relationships

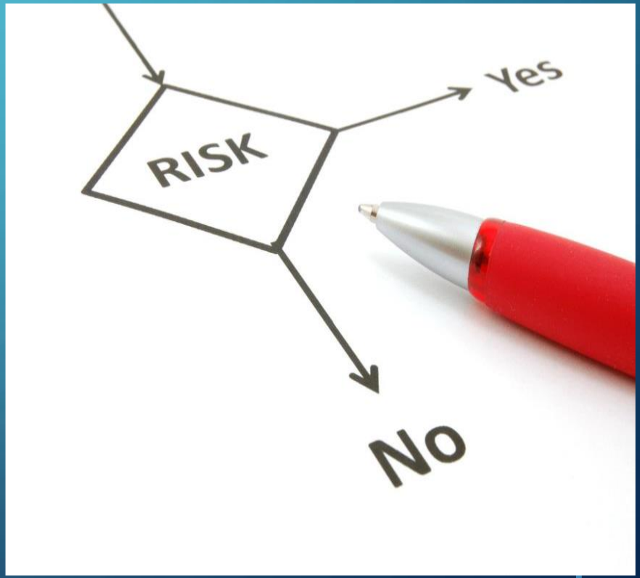
RISK IDENTIFICATION

Internal Assessments

- ✓ Business environment assessments
- ✓ Risk and control self assessments
- ✓ IT risk assessments
- ✓ Vulnerability assessments (e.g. scans)
- ✓ Internal control missions/verifications
- ✓ Scenario analysis

External assessments

- ✓ External audit reports;
- ✓ External penetration tests;
- ✓ Responsible disclosure programs;
- ✓ Emerging external trends/factors, sourced from reputable external sources;



RISK ASSESSMENT AND EVALUATION

Quantitative approach

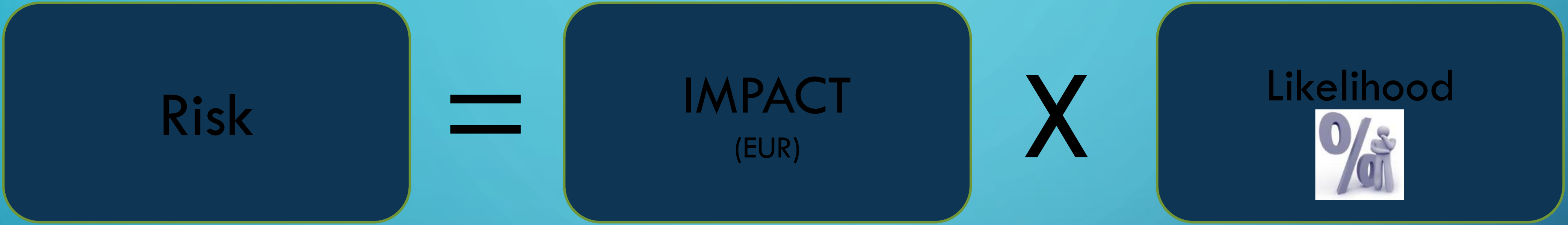
based on numbers and financial impact

Qualitative approach

based on opinion and experience

RISK ASSESSMENT AND EVALUATION

Quantitative approach (financial impact)



Risk = IMPACT (EUR) X Likelihood

Annual Loss Expectancy (ALE) The expected annual loss as a result of a risk to a specific asset

Single Loss Expectancy (SLE) Asset Value (AV) x Exposure Factor (EF)

Annualized rate of occurrence (ARO) Likelihood drawn from historical data

RISK ASSESSMENT AND EVALUATION

Qualitative approach (non-financial impact) – Risk Rating Matrix

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

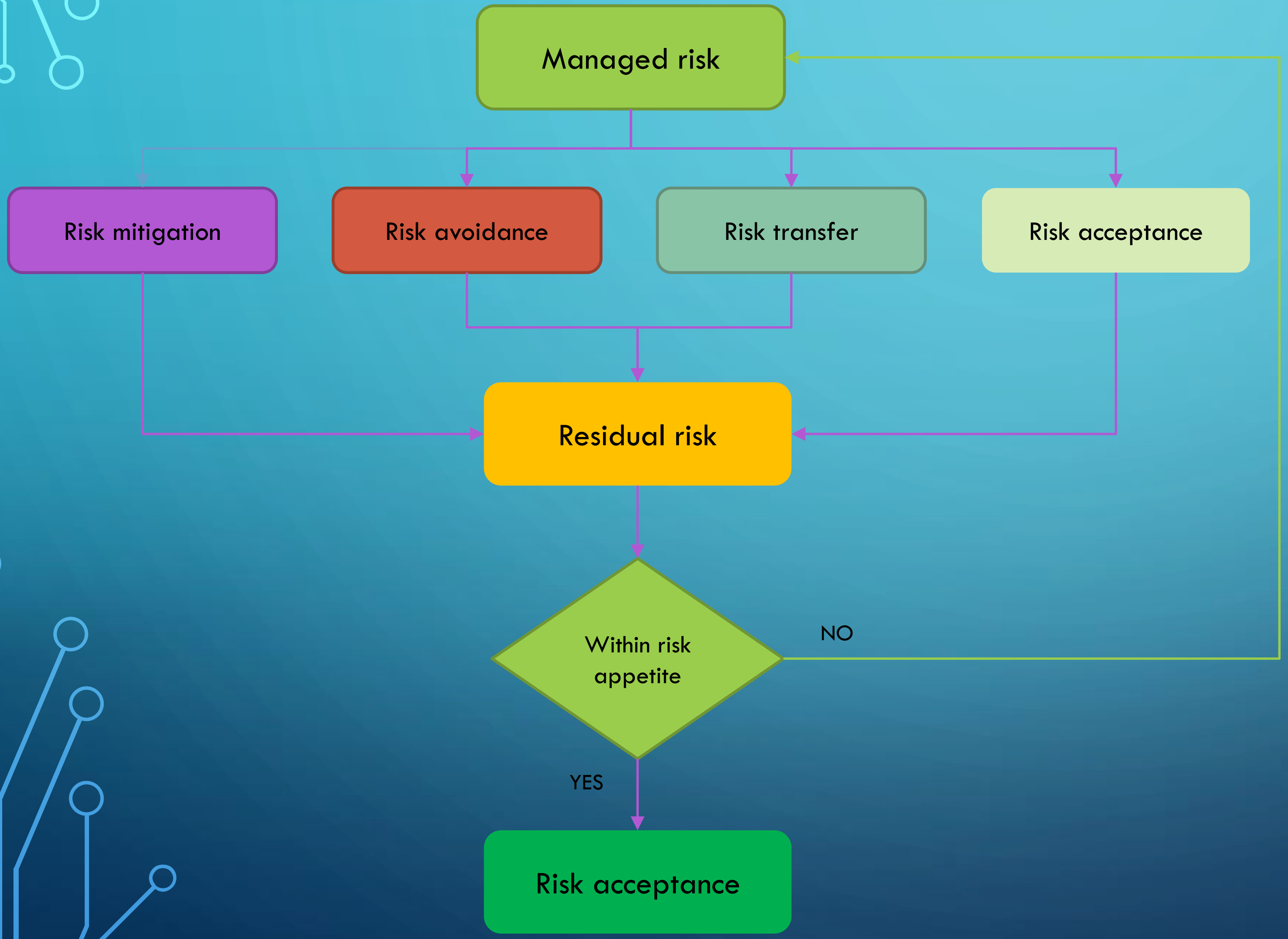
RISK ASSESSMENT AND EVALUATION

Qualitative approach (non-financial impact) – Impact Matrix

IMPACT	Description
Very High	The threat event could be expected to have multiple severe or catastrophic adverse effects on organizational operations, organizational assets, individuals, other organizations.
High	High The threat event could be expected to have a severe or catastrophic adverse effects.
Moderate	Moderate The threat event could be expected to have a serious adverse effects.
Low	Low The threat event could be expected to have a limited adverse effects.
Very Low	Very Low The threat event could be expected to have a negligible adverse effect.

RISK

Risk response strategies



Managed risk

Risk mitigation

Risk avoidance

Risk transfer

Risk acceptance

Residual risk

Within risk appetite

NO

YES

Risk acceptance

Risk mitigation
- Reduce the likelihood
- Reduce the impact

Risk avoidance
- Stop the activity that generate the risk

Risk transfer
- Insurance

Risk acceptance
- Deviation
- Acceptance

RISK MITIGATION - CONTROLS

A control is a measure, an action, a process, a requirement, etc. that has the final scope to mitigate a risk.

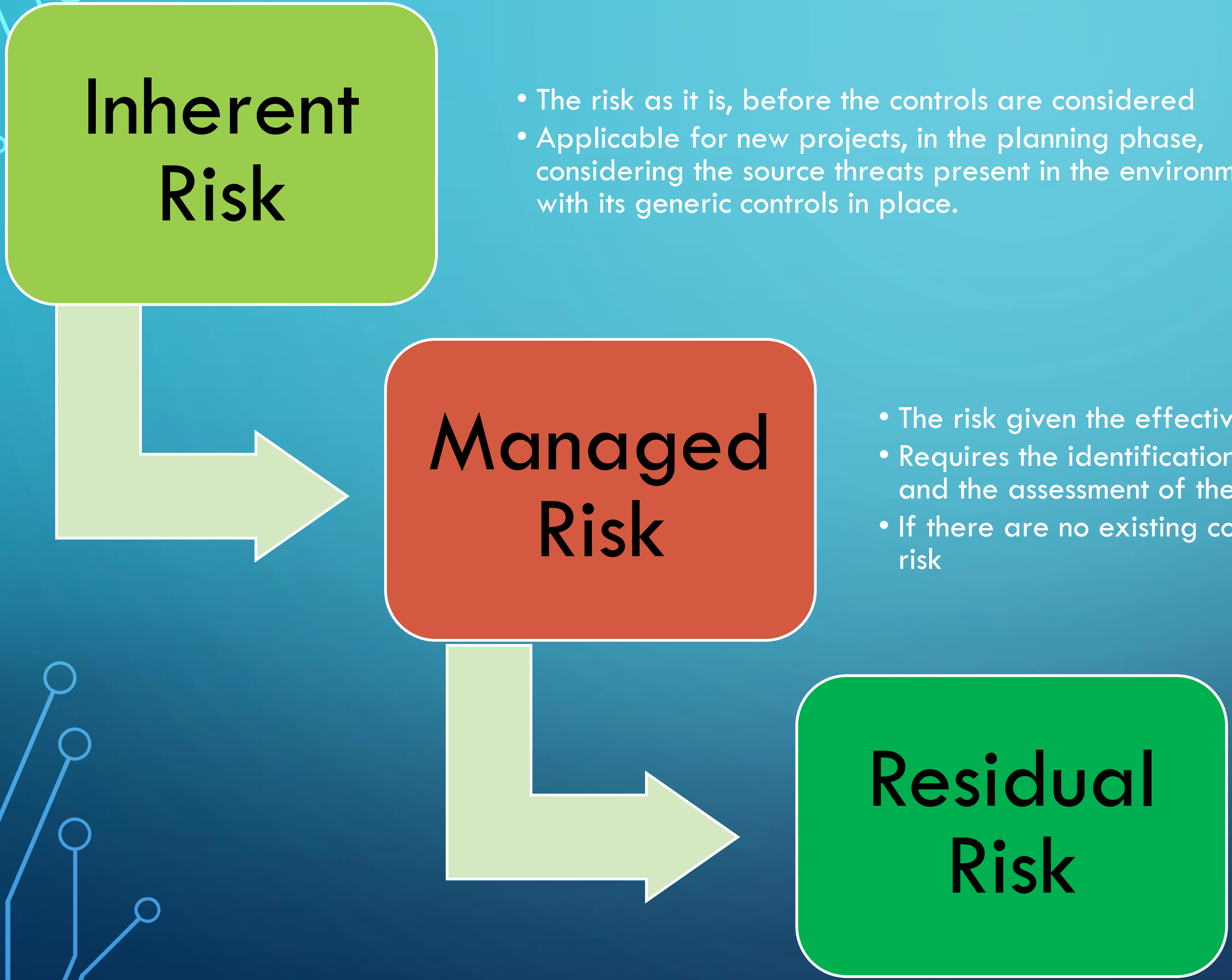
By mechanism of action:

- **Technical** (control end-user and system action; e.g. passwords constraints, access control lists, firewalls, data encryption, antivirus software, intrusion prevention software, etc.)
- **Administrative** (dictates how the activities should be performed; e.g. policies, procedures, guidelines, standards, etc.)
- **Operational** (e.g. configuration management, incident response, awareness, etc.)

By purpose:

- **Preventive** (attempt to prevent adverse behavior and actions from occurring; e.g. firewall, IPS, etc.)
- **Deterrent** (warn a would-be attacker that he should not attack; e.g. fence, dog sign, etc.)
- **Detective** (detect actual or attempted violations of system security; e.g. sensors IDS, etc.)
- **Compensating** (backup controls that come into play only when other controls have failed; e.g. backup generator)

RISK MITIGATION



Inherent Risk

- The risk as it is, before the controls are considered
- Applicable for new projects, in the planning phase, considering the source threats present in the environment, only with its generic controls in place.

Managed Risk

- The risk given the effectiveness of the current control environment
- Requires the identification of all relevant existing specific controls and the assessment of the controls' effectiveness
- If there are no existing controls, the managed risk is the inherent risk

Residual Risk

- The target risk level after mitigation actions have been put in place
- Assessment of the residual risks after planned mitigation actions and related to the target risk appetite of business management
- If there are no additional planned mitigation actions, the residual risk is the managed risk

RISK MANAGEMENT TOOLS – RISK REGISTER

One tool that it is frequently used to identify and track risks.

Risk				Risk Analysis			Risk Mitigation			Risk Status
ID	Date Raised	Risk Description	Owner	Likelihood	Impact	Severity	Control	Implementation Plan	Residual Risk	
	Date first identified	Brief summary of the risk	Responsible	Rate 1 (low) to 5 (high)	Rate 1 (low) to 5 (high)	Likelihood*Impact	What can be done to reduce or eliminate the likelihood or impact	How the control will be implemented	Risk remained after control is applied	Open (identified) / Closed (mitigated / resolved)

Q&A

LAB - RISK ASSESSMENT SIMULATION

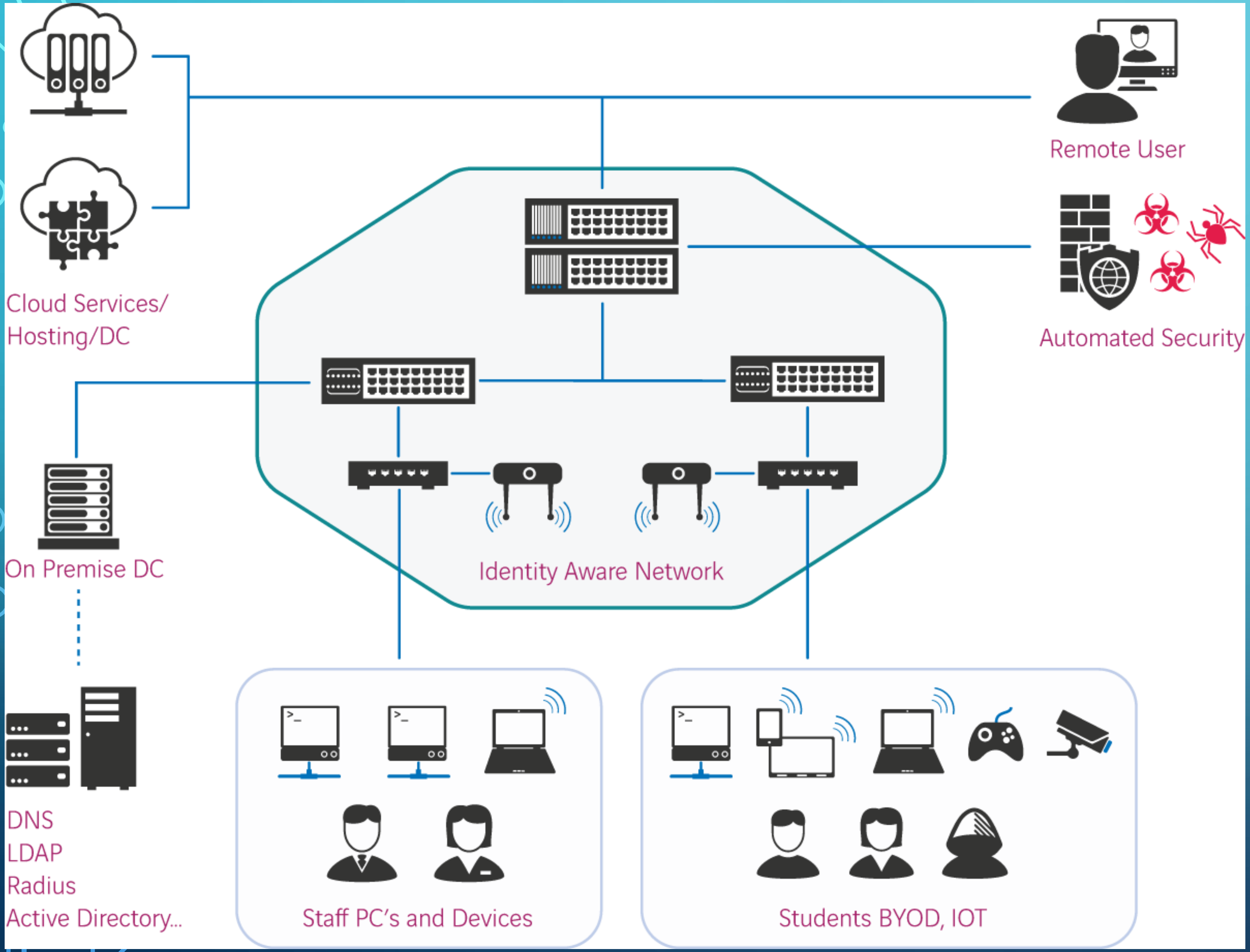
Input data

- ❖You are working for UniBuc organization as an information risk analyst, in the first line
- ❖A new project is considered for implementation
- ❖UniBuc's risk approach is to mitigate any moderate, high and extreme risks before production.
- ❖You are required to perform a risk assessment on the project and to support the project team to apply all the needed security measures so they can finalize the project without inducing risks into production.

Details on the project

UniBuc acquired a digital catalogue – a web application. The application is hosted on prem and will be exposed in internet as it needs to be accessed by teachers, students and parents.

LAB - RISK ASSESSMENT SIMULATION



Steps

1. Identify vulnerabilities, threats, risk applicable. Brainstorming.

2. Document the risks identified and estimate the likelihood and the impact for those.

3. Evaluate those using qualitative approach (non-financial impact) – risk rating table

4. Identify needed controls to mitigate the identified risks

5. Chose the most suitable mitigation strategy

THANK YOU!