Identity Access Management(IAM)

&

Threats, vulnerabilities and risks. Risk analysis.

October 2019

Bucharest

Agenda

Identity Access Management (IAM)

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

Threats, vulnerabilities and risks

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

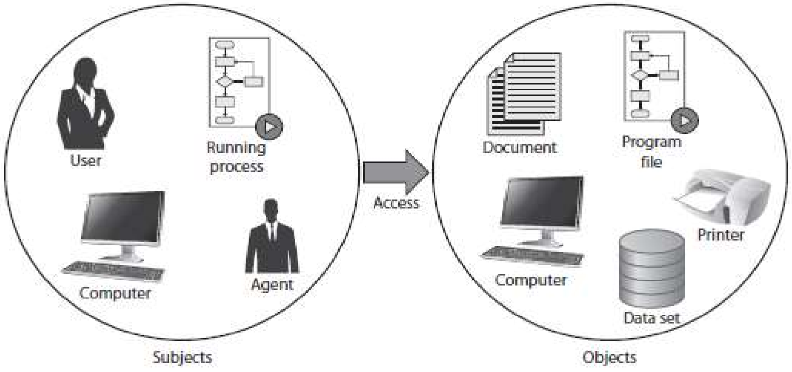
Lab – risk assessment simulation

Identity Access Management (IAM)

Access Control Overview

Access controls: security features that control how users and systems communicate and interact with other systems and resources.

Access controls give tor and
Protect resource ava ality.



Identity Access Management (IAM)

Access Control Overview

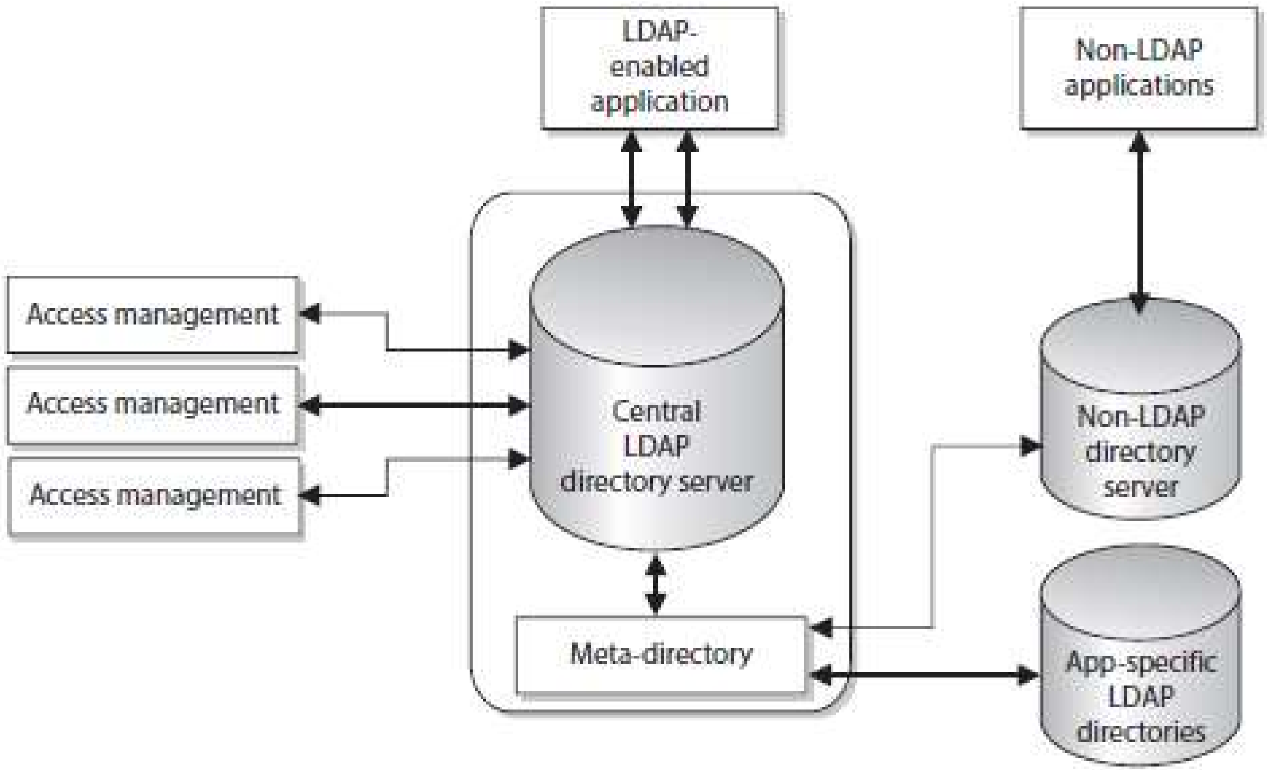
- Identification: username, user ID, account number
- AAA Principle
  - Authentication - passphrase, PIN value, thumbprint, smart card, OTP
  - Authorization - I know who you are, now what am I going to allow you to do?
  - Accountability - Audit logs and monitoring to track subject activities with objects

- Identity management
  - Directories – X.500, LDAP
  - Web access management (WAM)

Identity Access Management (IAM)

Access Control Overview

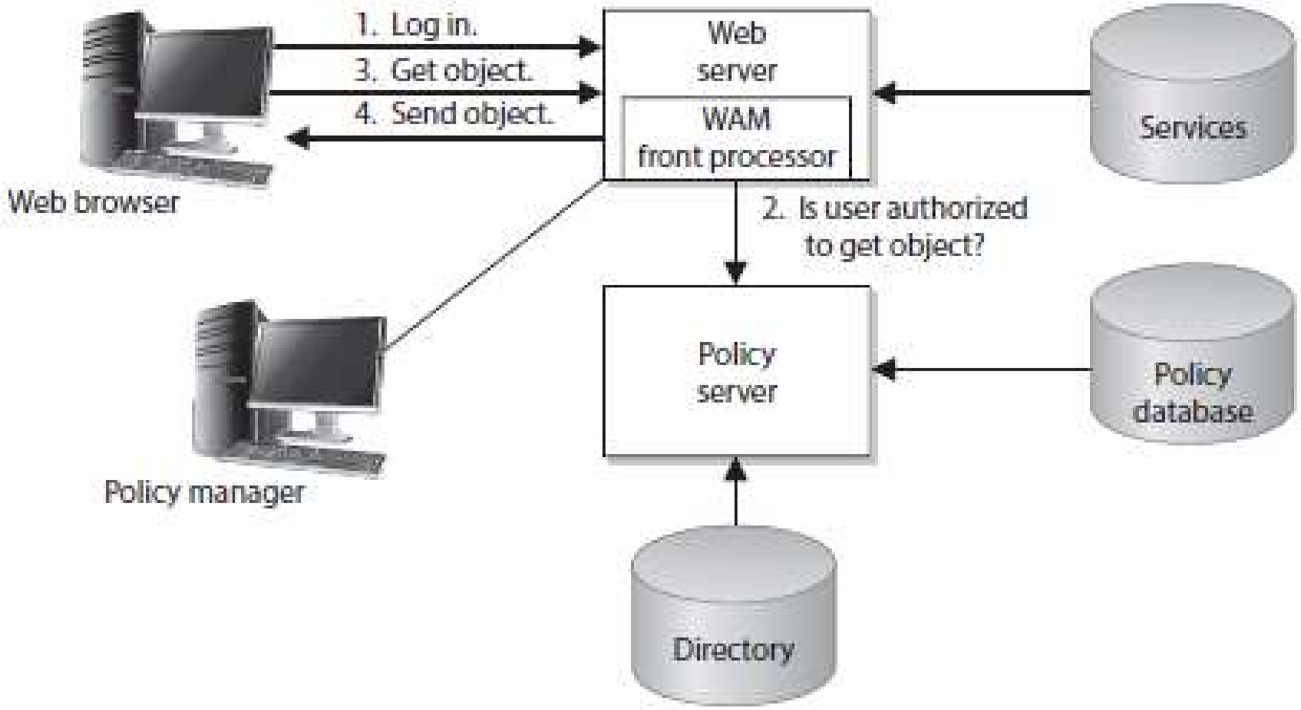
Directories:



Identity Access Management (IAM)

Access Control Overview

Web Access Management:



Identity Access Management (IAM)

Access Control Overview

Golden rule: **Default access to NO ACCESS**

Identity Access Management (IAM)

Access Control Models

- **Discretionary Access Control (DAC)** - the owner of the resource specify which subjects can access specific resources (most OS systems or ACLs)

  Issues: too extensive access, risk of malware spreading around
- **Mandatory Access Control** – users are given security clearance (secret, top secret, confidential, etc.) and data is classified in the same way (security labels for each object)
- **Role Based Access Control** - access to resources be based on the role the user holds within the company
- **Rule Based Access Control** - uses specific rules 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
- **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 Technologies

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

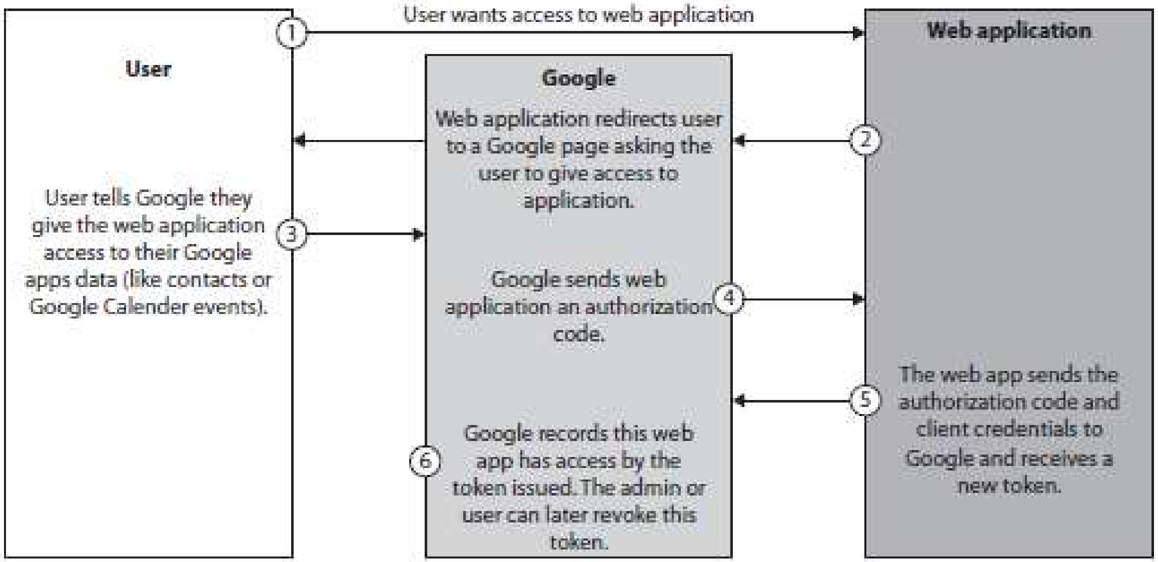
- TACACS (Terminal Access Controller Access Control System) – CISCO proprietary protocol developed in multiple formats like XTACACS, TACACS+

- 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


User wants access to web application
1
User
Google
Web application
Web application redirects user to a Google page asking the user to give access to application.
2
User tells Google they give the web application access to their Google apps data (like contacts or Google Calender events).
3
Google sends web application an authorization code.
4
The web app sends the authorization code and client credentials to Google and receives a new token.
5
6
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

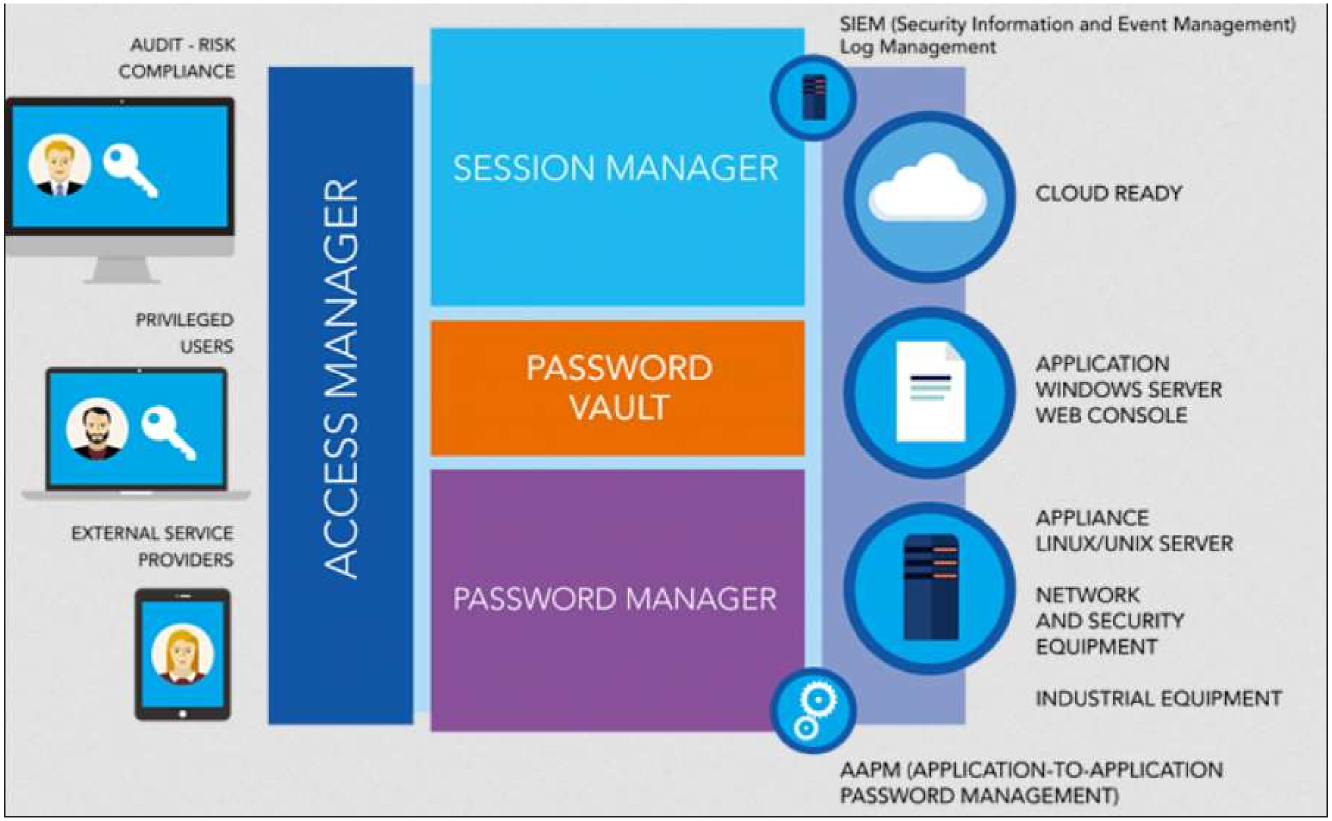
Top providers:

- 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)

Threats to access control

- Dictionary attacks
- Brute-force attacks
- Rainbow table
- 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.

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.

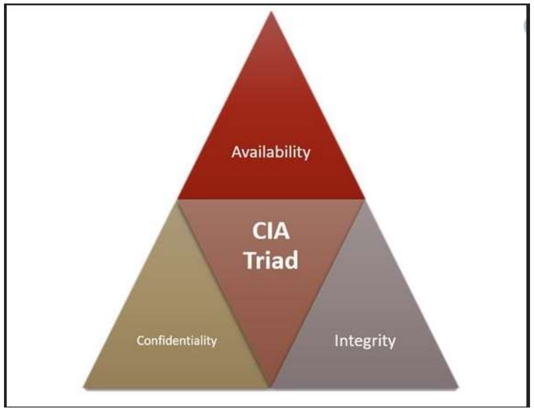
- Capability: the degree to which the adversary can succeed in accomplishing objectives;
- Opportunity: conditions(technical, logistical, legal, etc.) necessary to threat actor to accomplish objectives;
- Intent: what the threat actor seeks to achieve;

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 - vulnerability

Vulnerabilities in software.

e.g.

the software does not properly 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 designed to have backup

Other

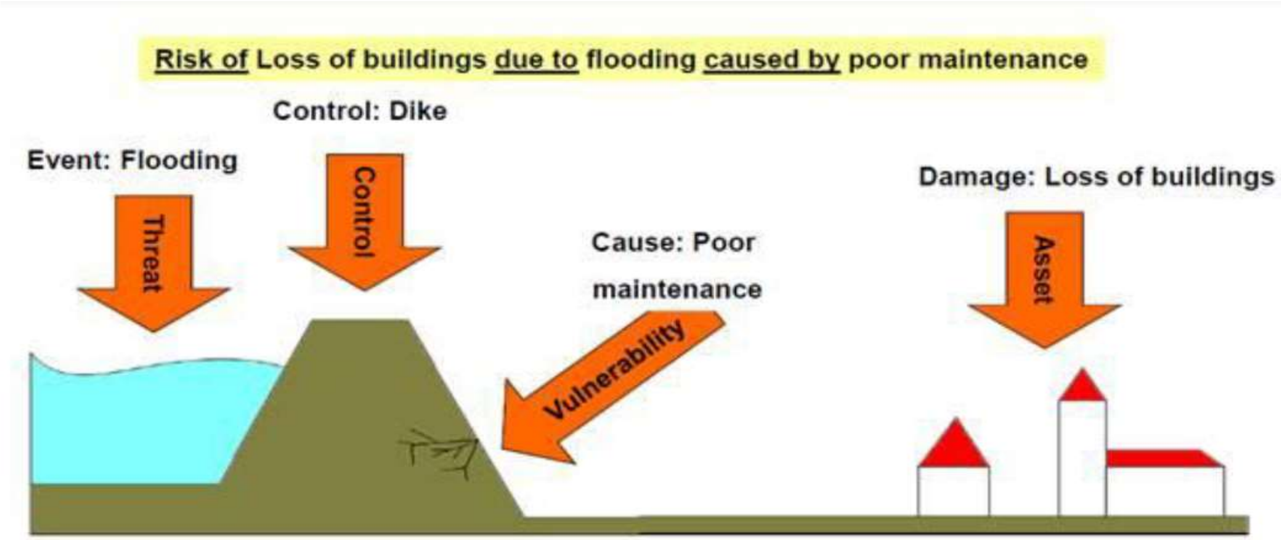
Example - threat

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.

Example - Risk

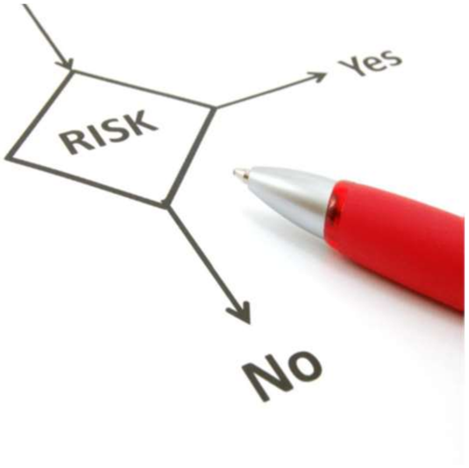
Risk of loss (financial or reputational) due to ransomware infections caused by lack of antivirus installed on the workstation.


Risk of Loss of buildings due to flooding caused by poor maintenance
Control: Dike
Event: Flooding
Threat
Control
Cause: Poor maintenance
Vulnerability
Damage: Loss of buildings
Asset

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

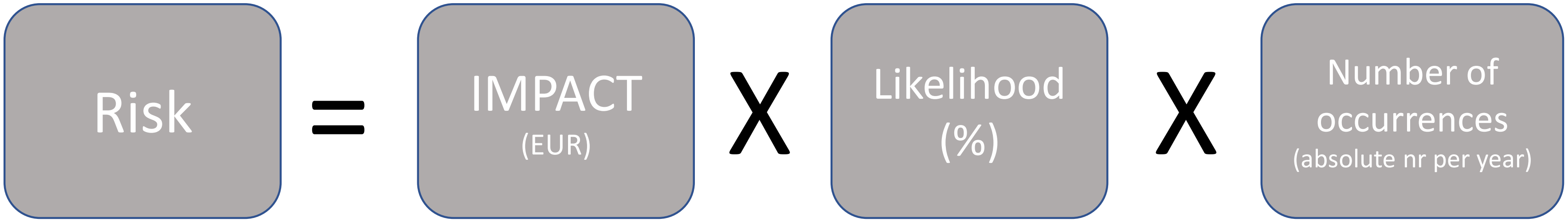


External assessments

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

Risk assessment and evaluation

Quantitative approach (financial impact)



Risk = IMPACT (EUR) X Likelihood (%) X Number of occurrences (absolute nr per year)

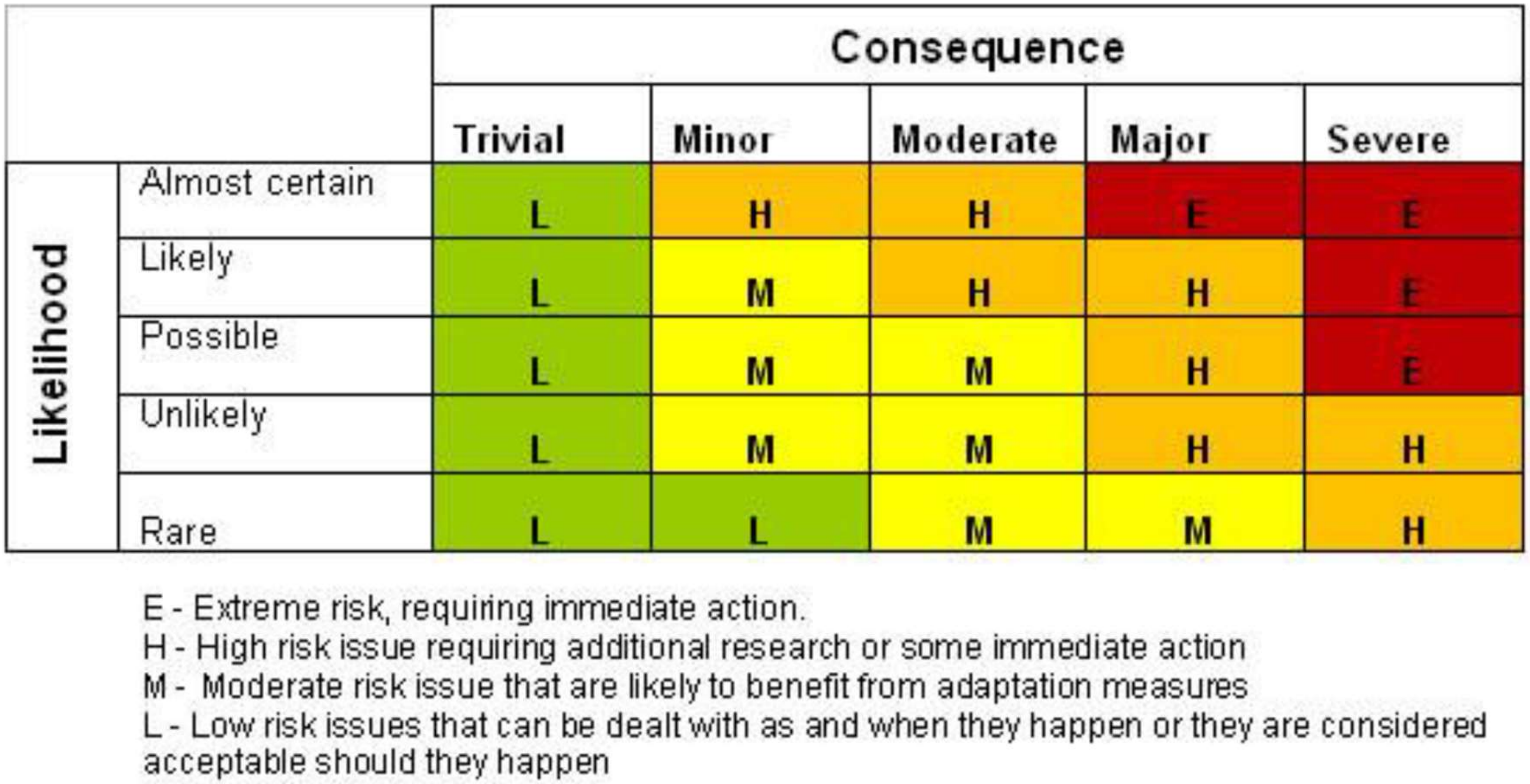
ALE: Annual Loss Expectancy - The expected annual loss as a result of a risk to a specific asset

Factors may include:

- ✓ Range and severity of issue
- ✓ Perceived importance
- ✓ Budget involved
- ✓ Etc.

Risk assessment and evaluation

Qualitative approach (non-financial impact) – risk rating table



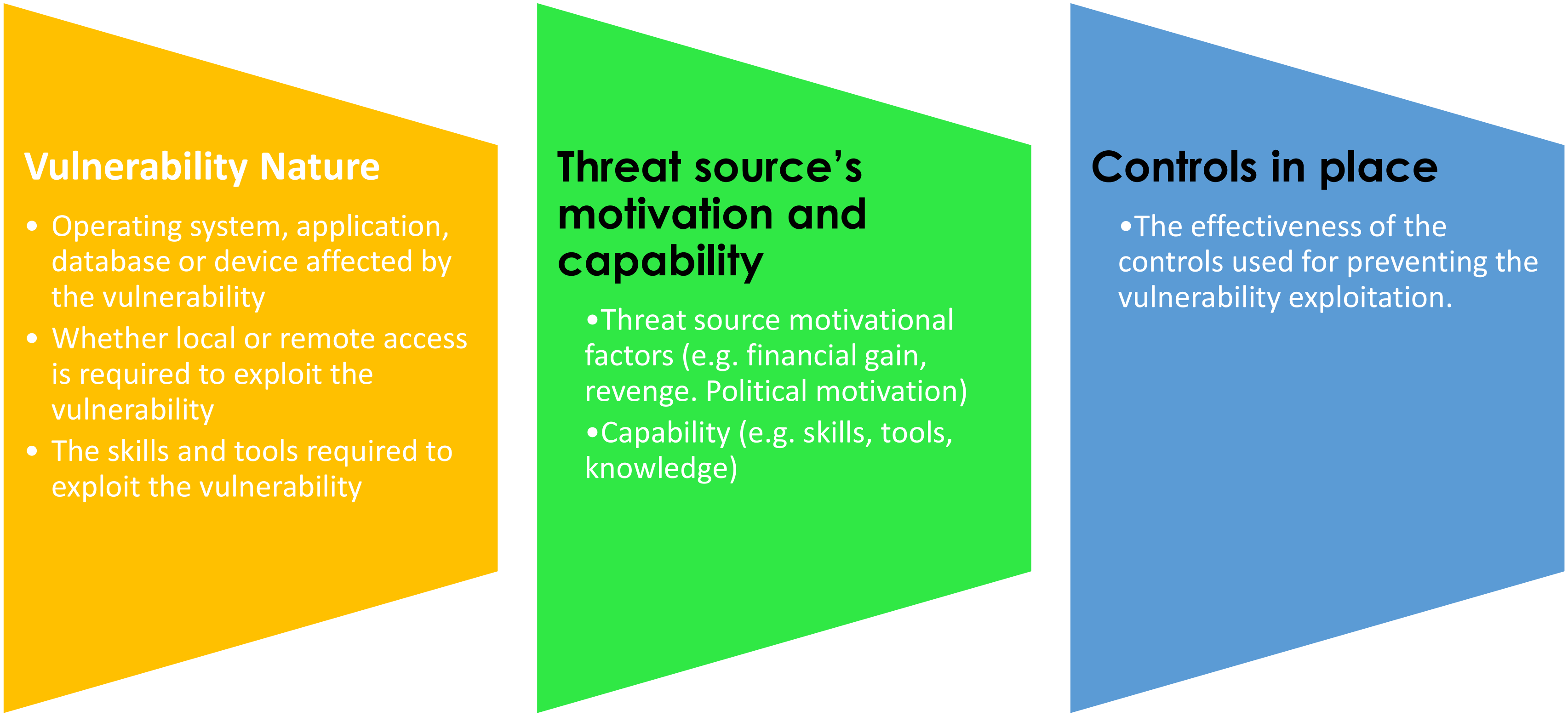
		Consequence				
		Trivial	Minor	Moderate	Major	Severe
Likelihood	Almost certain	L	H	H	E	E
	Likely	L	M	H	H	E
	Possible	L	M	M	H	E
	Unlikely	L	M	M	H	H
	Rare	L	L	M	M	H

E - Extreme risk, requiring immediate action.
H - High risk issue requiring additional research or some immediate action
M - Moderate risk issue that are likely to benefit from adaptation measures
L - Low risk issues that can be dealt with as and when they happen or they are considered acceptable should they happen

Source:
https://ischool2013.wikispaces.com/file/view/risk-table.jpg/472497818/risk-table.jpg

Risk Assessment – likelihood determination

Likelihood determination. Based on the**:**



Vulnerability Nature

- Operating system, application, database or device affected by the vulnerability
- Whether local or remote access is required to exploit the vulnerability
- The skills and tools required to exploit the vulnerability

Threat source's motivation and capability

- Threat source motivational factors (e.g. financial gain, revenge. Political motivation)
- Capability (e.g. skills, tools, knowledge)

Controls in place

- The effectiveness of the controls used for preventing the vulnerability exploitation.

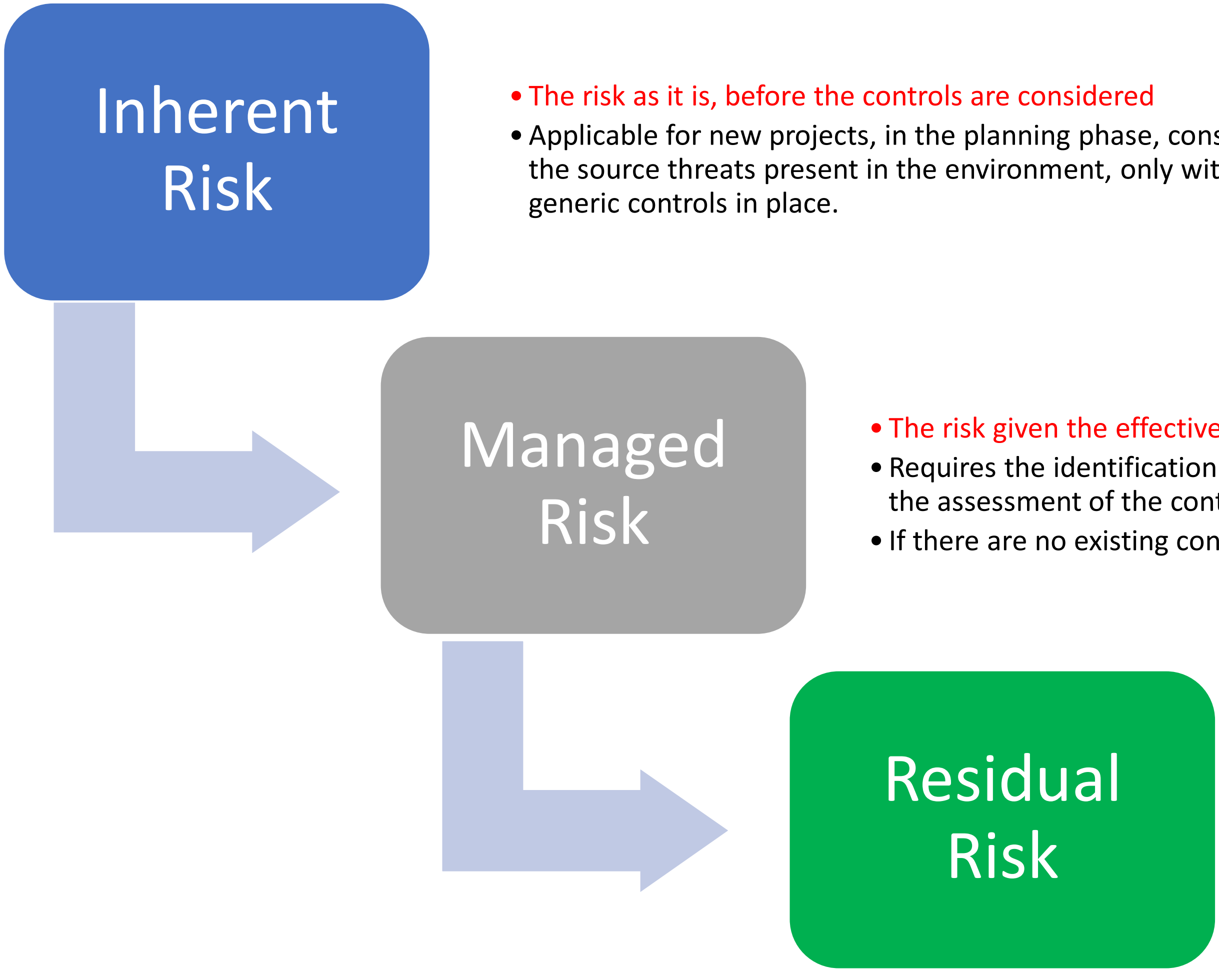
Risk mitigation - controls

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

- **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.)

- **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

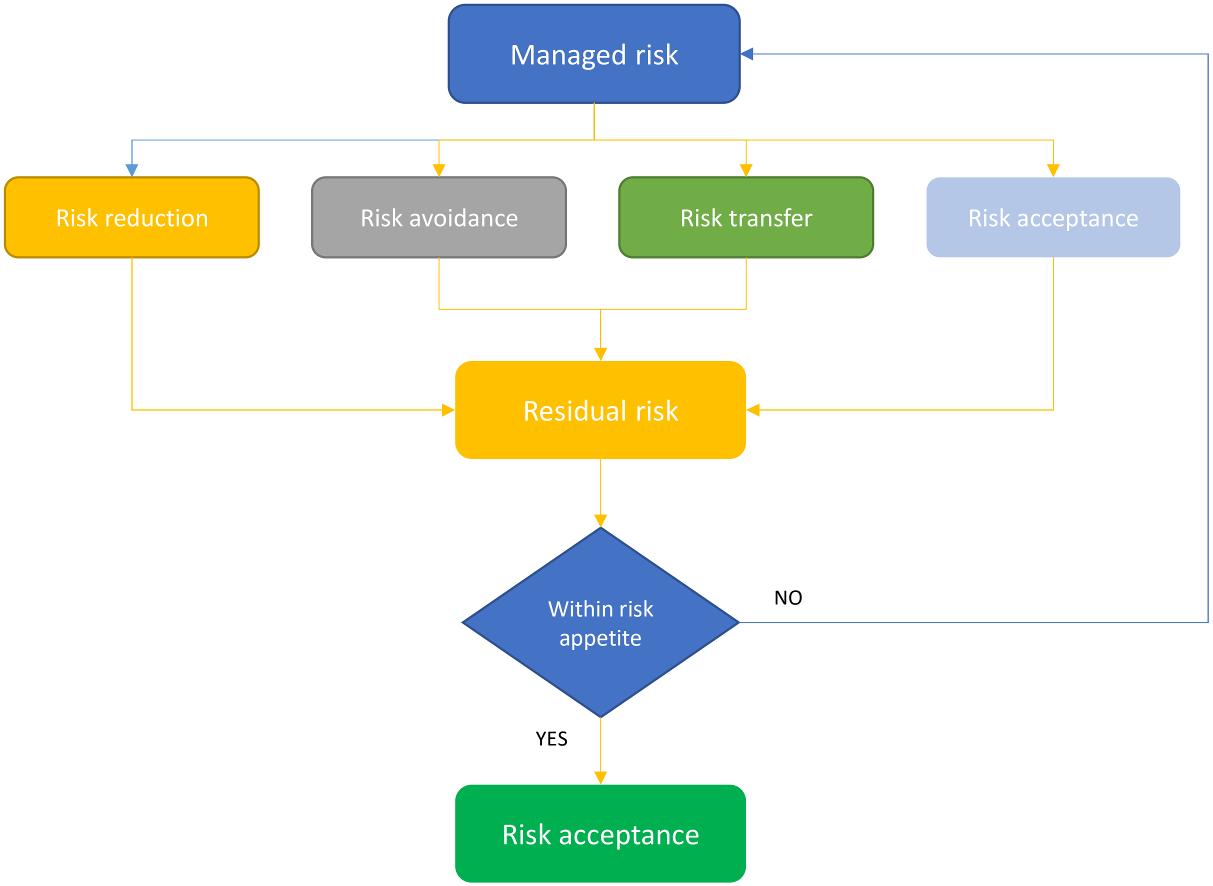
- The risk given the effectiveness of the current control environment
- Requires the identification of all relevant existing specific controls and the assessment of the controls’ effectiveness
- If there are no existing controls, the managed risk is the inherent risk

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 mitigation

Risk mitigation strategies



Managed risk

Risk reduction

Risk avoidance

Risk transfer

Risk acceptance

Residual risk

Within risk appetite

NO

YES

Risk acceptance

Risk reduction
- Reduce the likelihood
- Reduce the impact

Risk avoidance
- Stop the activity that generate the risk

Risk transfer
- Insurance

Risk acceptance
- Deviation
- Acceptance

Lab - risk assessment simulation

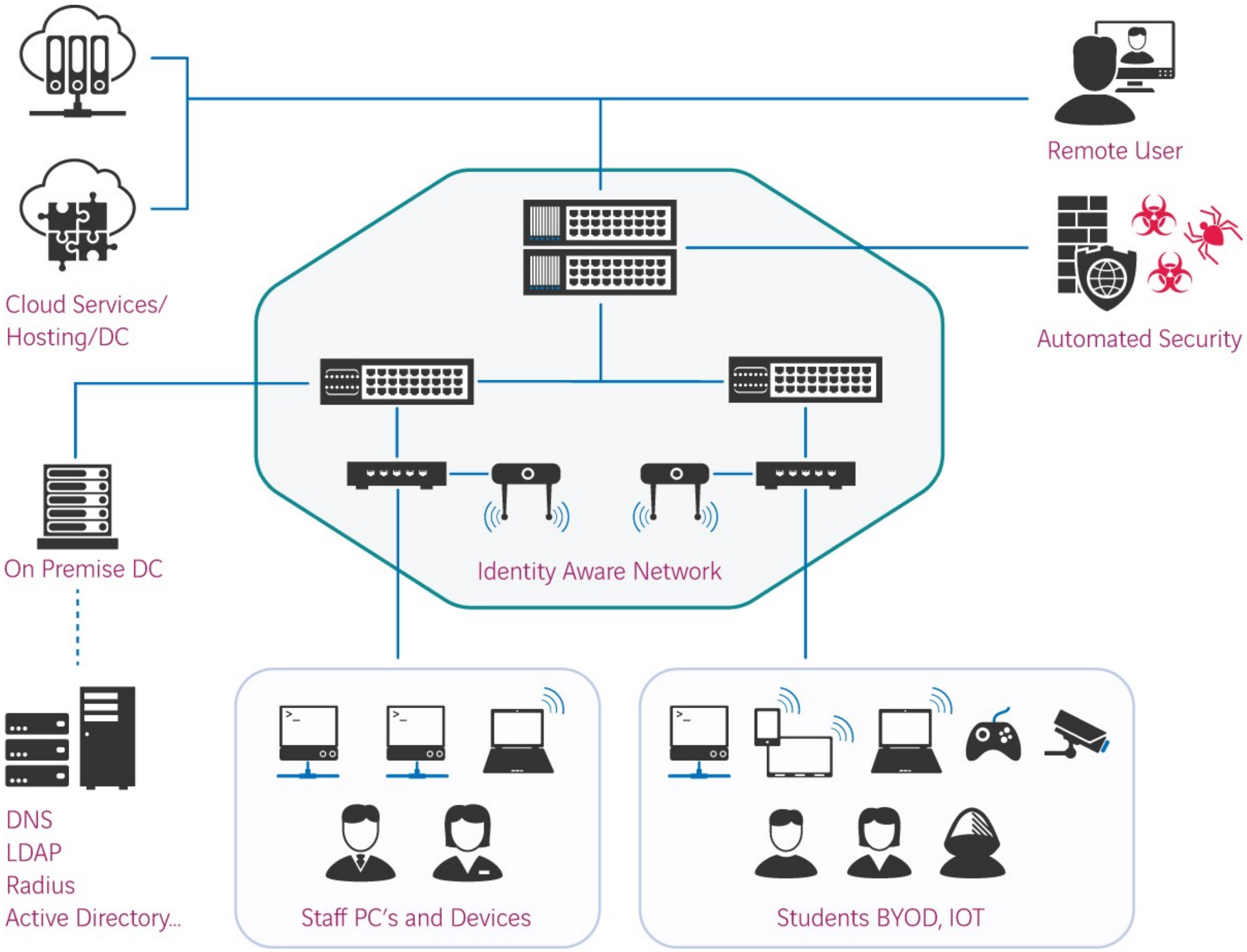
Input data

- You are working for UniBuc organization as an information risk analyst, in the first line
- A new project is considered for implementation – TBA
- 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.

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

Lab - risk assessment simulation


Remote User
Cloud Services/
Hosting/DC
Automated Security
On Premise DC
Identity Aware Network
DNS
LDAP
Radius
Active Directory...
Staff PC's and Devices
Students BYOD, IOT