Course: IT RISK MANAGEMENT AND CONTROL

Week 8

Topic: Access and Identity Management

Lecturer: Ninyikiriza Deborah Lynn

TODAYS outline

1. Review of week 7 Material
2. Principles of Access Control
3. Identity and Access Management (IAM) Systems
4. Best Practices for Access Control

Week 7 Review

Before we start looking at week 8 material, let's first do a quick review of our previous lecture material (week 7)

In week 7, we discussed the following;

1. IT control frameworks

- Structured methodologies used in IT risk management and control to help organizations manage risks and ens ure that IT processes and systems are reliable, secure, and are aligned with business objectives.

Week 7 Review

2. Purpose of IT Control Frameworks

- Aligning IT with Business Goals.
- Risk Mitigation.
- Regulatory Compliance.
- Operational Efficiency.
- Security Assurance.

Week 7 Review

3. Overview of Control Frameworks

1. COBIT (Control Objectives for Information and Related Technologies)

- A governance and management framework that helps orga nizations to align IT strategy with business goals.

2. NIST Cybersecurity Framework

- NIST was developed by the National Institute of Standards and Technology to help organizations identify, manage and mitigate cybersecurity risks.

3. ITIL (Information Technology Infrastructure Library)

- ITIL is a framework that provides a set of practices for IT se rvice management (ITSM) that focuses on aligning IT servic es with the needs of the business.

Week 7 Review

Overview of Control Frameworks cont..

4. ISO/IEC 27001

- An international standard which manages sensitive compan y information and ensures that it remains secure through im plementing a robust Information Security Management Syst em (ISMS).

5. COSO (Committee of Sponsoring Organizations of the Treadway Commission)

- COSO is an enterprise risk management.
- It is not specifically focused on IT, but it is widely used for in ternal control and risk management, thus integrating IT risks into overall organizational risk.

Week 7 Review

4. Designing effective control frameworks

Steps;

1. Understand the Organization's Risk Appetite and Strategy
2. Define a Risk Assessment Process
3. Select an Appropriate Control Framework
4. Develop Control Objectives for the Framework
5. Establish a Governance Structure
6. Implement Monitoring and Reporting Mechanisms
7. Ensure Compliance and Adaptability
8. Integrate IT Controls into Business Processes
9. Implement Continuous Improvement
10. Conduct Training and Awareness Programs
11. Make use of Technology and Automation
12. Test and Validate Controls

Week 7 Review

5. Key considerations of choosing the framework

1. Scalability
2. Cost Efficiency
3. Transparency

6. Steps for Implementing Control Frameworks

1. Assess and Identify Relevant Frameworks
2. Establish IT Governance
3. Perform a Risk Assessment
4. Map Controls to the Framework
5. Implement Controls
6. Testing and Validation
7. Perform monitoring and continuous Improvement
8. Reporting and Compliance
9. Training and Awareness

Week 7 Review

7. Control Frameworks Enhance Risk Management through;

- Implementing effective controls
- Ensuring compliance
- Identifying Risks

8. Benefits of implementing control frameworks

- Improved Risk Management
- Regulatory Compliance
- Better IT Governance
- Enhanced Security
- Operational Efficiency

Week 7 Review

9. Challenges faced in implementing control frameworks

- Complexity
- Integration with Other Systems
- Customization
- Continuous Change/ Evolving threats an technologies

Week 8: Access and Identity Management

QN. What is Access control and Identity Management (AIM)?

- Access control and Identity Management (AIM) is a critical component of IT risk management and control which focus es on managing and securing user identities, access rights, and permissions within an organization.
- AIM systems help to prevent unauthorized access to syste ms, applications, and data, thus ensuring that only authoriz ed users have access to sensitive information.

Access and Identity Management

The Access Control Framework

- organizations rely on access controls to grant and restrict user access to information, systems, and other resources.
- Access control systems, when properly designed can implement business rules and directly implement data policy.
- The policy is that individuals have access only to the information and resources they require to perform their job responsibilities.
- The consequences of weak or nonexistent access controls range from inconvenience to causing disaster, depending on the nature of the resources being protected.
- For the average user, it may be a personal invasion of privacy to have someone else reading your email.

Access and Identity Management

Terms: Access and Access Control.

- Before diving deep into the content for this lecture, Lets first understand these important concepts;

  What does “**Access**” and “**Access control**” mean?

- In the real world of Technology, there is a need to protec t precious data, systems, networks, and other assets fro m a variety of threats.

- These concepts therefore help us to lock the virtual door s and secure valuable information assets from unauthori zed access, modification, and disruption.

Access and Identity Management

“**Access**” and “**Access control**” **con’t…..**

Generally, Access refers to the ability of a subject and an object to interact.

Example: Consider a busy manager with an admin who decide s who will be allowed to interact with the manager or not.

In this scenario;

- The visitor is the subject.
- The Manager is the object.
- The admin is the access control system.

So in this case the admin(access control system) restricts which individuals (subjects) may access the manager (object).

Access" and "Access Control

QN: What Is "**Access**" and **"Access control"** in IT?

- Now think about what would happen if data were freely available?
- What if the data exposed is the company's payroll file, an unsecur ed file that anyone could open and obtain sensitive information su ch as employees Social Security numbers and their annual salary.
- Imagine what would happen if an annoyed employee manipulated/ reset the salaries.
- Therefore, data is one of the most valuable assets that organizatio ns possess, so IT professionals must invest time and energy to ap propriately secure it.

Access" and "Access Control

Access and "Access control" in IT con't…

- Information systems use formalized systems to grant or rest rict access to resources.
- Computers are not very good at making correct decisions, s o we have to lay out specific rules for them to follow when d eciding whether to grant or deny access.

Access Control

- Access control is the process of following rules to allow or d eny access to the computer user.

Access controls

- Access controls define the allowable interactions between s ubjects and objects ie users and computers.
- They are based on the granting of rights, or privileges, to a subject(user) with respect to an object (computer).

The Access Control Process

There are three steps in the access control process ie;

1. Identification—The process by which a subject identifies itself to the access control system.

2. Authentication—Verification of the subject's identity.

3. Authorization—The decision to allow or deny the subject to access an object.

- The second step usually happens behind the scenes, so the subject is really only aware of two stages; 1 and 3.
- He or she enters credentials and is either given or denie d access to a resource.

The Access Control Process (Example)

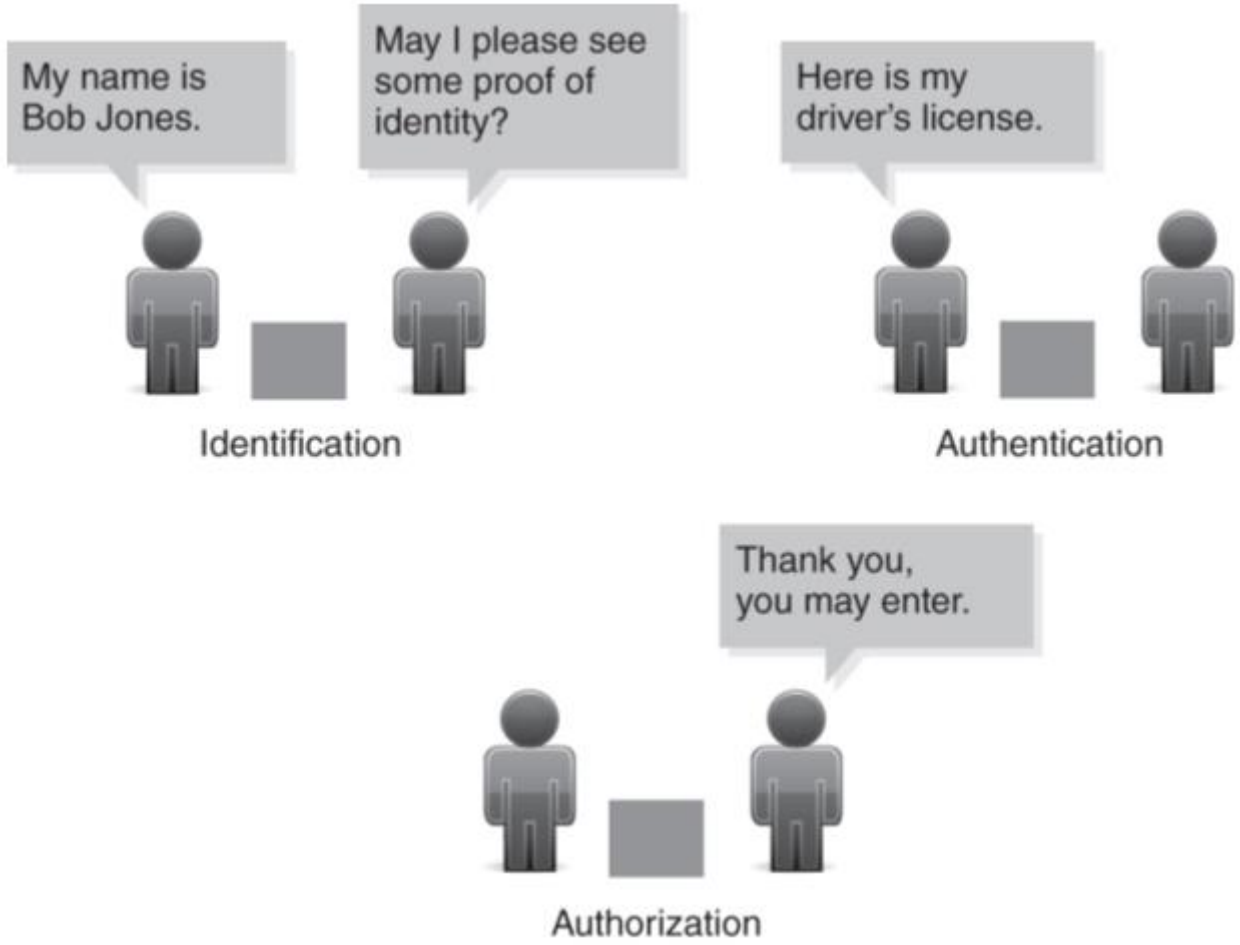

FIGURE 1: The access control process

The Access Control Process cont..

- As seen in figure 1, the first step in any access control proce ss is;

1. Identification;

- The system must trust that a subject has not falsified his or her credentials, but at the same time, the subject must be co nfident that the system will store those credentials securely.
- The system must be able to apply labels to the two parts of t he access equation; the subject and the object.
- In this case, a label is a purely logical description that is eas y for the computer to understand.
- A human might easily recognize that “Beth” and “Elizabeth” are the same individual, but a computer cannot necessarily make that logical connection.

The Access Control Process cont..

2. Authentication;

- As seen in the diagram, authentication builds upon identific ation by requiring that the subject provides proof of Identity.
- Authentication methods may include;

1. Password—A secret word or combination of characters tha t is known only to the subject.

2. Token—Something the subject has that no one else does, such as a smart card, driving license, passport etc.

3. Fingerprint scan—Involves optical analysis of a person's fin gerprint then compare the results with the recorded sample to verify his /her identity.

The Access Control Process cont..

Authentication factors,

- Most authentication systems require only a single authenticati on factor, but those protecting highly sensitive assets might us e multiple factors.

The three most common factors are;

- Something you know—Generally a password or shared secret
- Something you have—A token or smart card ID badge
- Something you are—Fingerprints or other biometric factor

SEE example on next slide;

The Access Control Process cont..

Authentication con't...

Figure 2: Iris scanning as an authentication technique
© United States Department of Defense

NOTE

Authentication techniques such as biometric authentication and iris scanning are more secure than a simple password because it is more difficult to copy or steal an eyeball than it is to guess or steal a password as shown in fig.2.

The Access Control Process cont..

- Using more than one authentication factor increa ses the security of the system. This is referred to as “two-factor authentication (2FA)

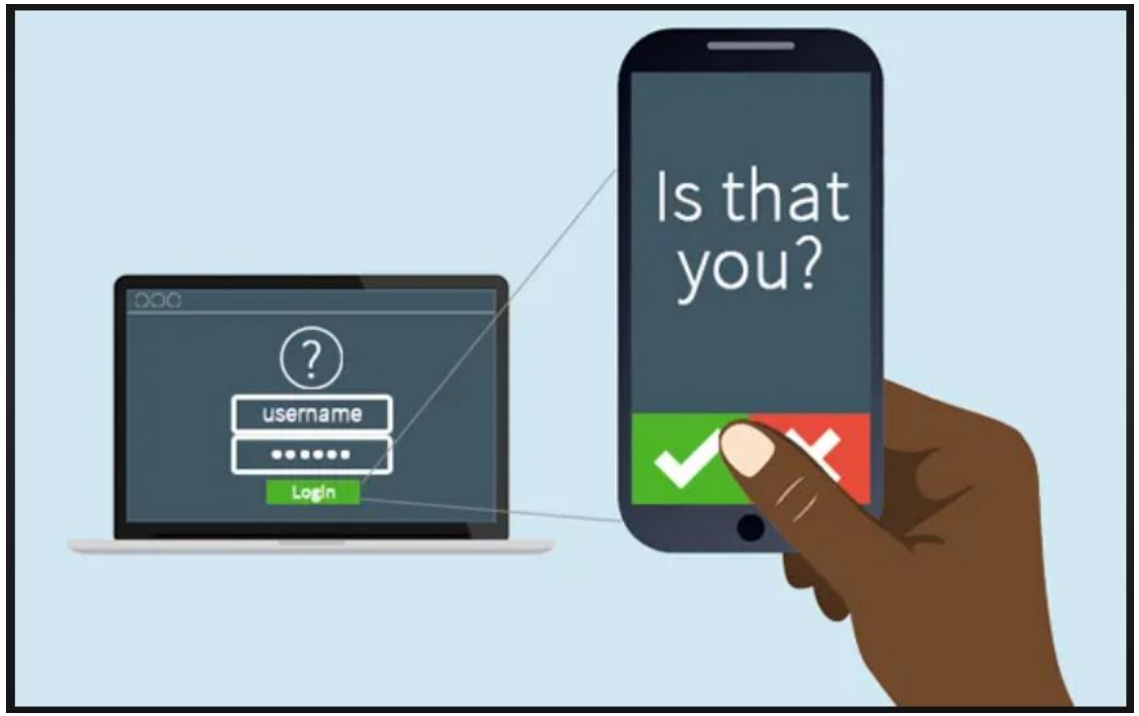

Figure 3. 2FA Example

Qn: Does 2FA increase security?

Yes, This is because if one stage of the aut hentication system is compromised, the sec ond stage can still restrict access to those w ho do not have the proper credentials.

The Access Control Process cont..

3. Authorization

- Once a subject has identified him or herself and the access control system authenticates the subject’s identity, the acces s control system must determine whether the subject is auth orized to access the requested resources or not.
- Authorization bases on identity to allow acess e.g a manage r in the human resources department might be authorized to view personnel records but not authorized to edit the year-e nd financial report.

The Access Control Process cont..

Authorization cont..

- Authorization rules can be simple. For example, a corporate e-mail directory might allow access to any employee with a valid user account.
- However, authorization rules can also be complex, dependi ng on the value of the resources being protected and the nu mber of people requesting access.
- For example, a file server might limit folder access by an e mployee’s role and membership in a particular department.

Principal Components of Access Control

There are three principal components of any access control sc enario ie;

- Policies—The rules that govern who gets access to which re sources.
- Subjects—The user, network, process, or application reques ting access to a resource.
- Objects—The resource which the subject desires to access (e.g, files, databases, printers, and physical facilities).

Access Control System

A well-defined access control system consists of three eleme nts ie;

- Policies—Clear statements of the business requirements r egarding access to resources.
- Procedures—Nontechnical methods, such as business pro cesses and background checks, used to enforce policies.
- Tools—Technical methods, such as file system access cont rols and network firewalls, used to enforce policies.
- Organizations typically use procedures and tools together t o enforce policies.

Access Control Subjects

- The subject in an access-control scenario is a person or another application requesting access to a resource such as the network, a file system, or a printer.
- There are three types of subjects when it comes to access control for a specific resource ie;
- Authorized—Those who have presented authenticated credentials and have been approved for access to the resource.
- Unauthorized—Those who have presented authenticated credentials but are not approved for access to the resource.
- Unknown—Those who have not presented authenticated credentials.

Note: Every individual who initially approaches an access control system is unknown until he or she attempts to authenticate.

Access Control Objects

- There are three main categories of objects to be protected by access controls;
- Information—Any type of data
- Technology—Applications, systems, and networks
- Physical location—Physical locations such as buildings and r ooms.
- Information is the most common asset in terms of IT access controls.
- Databases and applications need passwords to ensure that o nly authorized users can access the information they contain.

Access Control Objects

Continuation;

- The physical location is very important.
- Technology objects are very important because a malicious user can easily compromise the integrity of data by attackin g the technology that stores and uses it.
- If an unauthorized user gains access to a file server, that us er can easily steal, delete, or change the data stored on the file server.
- It is therefore very important to protect the physical location in order to have the data and technology safe.

Access Control Objects

Example 1;

- Consider an automated teller machine (ATM) in a mall.
- The ATM system deals with highly sensitive data, but in ord er to fulfill its purpose, it must be in an open and easily acc essed area.
- In this type of situation, information and technology-based a ccess controls become doubly important.
- Physical security is the process of ensuring that no one wit hout the proper credentials can access physical resources.

Access Control Objects

Example 2

- Consider a server. If all of the servers require a password to log o n, why bother restricting who can enter the server room?
- The answer is simple; if a malicious user's goal is to bring down a server, he or she doesn't need to log in.
- All the person needs to do is unplug it, steal it, or destroy it.
- Additionally, an individual who is able to gain physical access to a network router can almost always take control of that device, eve n without knowledge of the correct password.
- This because most server and network systems have "backdoors" that are available to anyone with physical access to the machine.
- These backdoors allow system administrators to take control of a server that has been corrupted.
- Some locations, such as a server rooms are controlled-access loc ations for the reasons just described above.

Principles of Access Control

- As earlier mentioned, access control is a fundamental aspect of IT risk management.
- This is because it helps to ensure that only authorized individuals have access to specific systems, data, and resources.
- The principles of access control are essential to safeguarding information and managing risk.
- Next slide, we discuss the detailed core principles;

1. Identification Principle

Identification is the process of recognizing and distinguishing an individual or entity in the system.

It ensures that the system can track which individuals are requesting access.

Example: Using a unique username, user ID, or biometrics to identify users in a system.

Principles of Access Control

2. Authentication Principle

- Authentication verifies the identity claimed during the id entification phase.
- It involves confirming the user’s identity through credent ials, such as passwords, tokens, or biometrics.
- It ensures that only legitimate users who possess the co rrect credentials can access the system.

Types of Authentication

- *Single-Factor Authentication (SFA)*: Uses one type of cr edential, such as a password.
- *Multi-Factor Authentication (MFA)*: Requires multiple for ms of verification, like a password plus a fingerprint.

Principles of Access Control

3. Authorization Principle

- Authorization determines what a user is allowed to acces s or perform within the system.
- Once authenticated, users are granted permissions base d on their roles or privileges.
- Authorization limits access to only what is necessary for each user to perform their job functions, minimizing pote ntial misuse.
- Example; A finance employee may have access to the pa yroll system but no access confidential HR records.

Principles of Access Control

4. Accountability Principle

- Accountability ensures that actions can be traced back to specific individuals or systems, providing an audit trail of access and activity.
- It helps to detect and investigate security incidents as we ll as enforce responsibility for misuse of access.

Example of an accountability activity;

- Logging user activity, such as file access, modifications, and logins, to maintain records that can be audited.

Principles of Access Control

5. Least Privilege Principle;

- Least privilege grants users only the minimum level of ac cess necessary to perform their duties.
- It reduces the potential for accidental or malicious misus e of access by limiting unnecessary permissions.
- Example: A user being temporarily granted access /perm issions to a specific task.

Principles of Access Control

6. Separation of Duties principle

- Separation of duties ensures that no single individual has control over all aspects of any critical or high-risk process.
- This principle helps to mitigates risks of fraud and errors by dividing tasks and responsibilities among multiple people.
- **Example:** In financial systems, the roles of the requestor, approver, and reviewer in transaction workflows are separated.

7. Need-to-Know principle

- Need-to-know restricts access to data based on specific requirements for users to complete their job tasks.

Example: Only members of a legal team working on a specific case have access to case-related documents.

Identity Management

What Is Identity Management?

- Identity management is the process of creating, maintaining, and closing user accounts and providing the mechanisms used to authenticate users.
- This allows controllers to confirm that a person is who they claim to be (authentication), and access control allows one to restrict his or her activities to authorized actions.
- In practice, the concepts of identity management and access control are combined and are difficult to separate.
- For this reason, many people refer to both fields together as identity and access management (IAM).

Identity and Access Management Systems (IAM)

What are Identity and Access Management (IAMs)?

- Identity and Access Management systems are tools and processes that help organizations manage who can acce ss their digital resources and what they can do within tho se resources.
- They ensure that only authorized people can get into syst ems, applications, and networks.
- These authorized people must also only get access to the parts they need for their roles.

Elements of IAM systems

1. Identity Management

- IAM systems aim to create and manage the digital identities of users within the organization.
- Each user is assigned a unique digital identity with respect to their job role.
- This identity includes information like usernames, passwords, job roles, and personal details.
- **Example:** When a new employee joins, they are given an account with login credentials (like a username and password) that will give them access to the systems they need.

Elements of IAM systems

2. Access Management

- IAM systems control which resources each user can acce ss and what actions they can perform.
- Based on the user’s identity and role, the system determin es what permissions they should have on the system e.g viewing, editing, or deleting information.
- **Example:** An HR employee may have access to employe e records, while a finance employee has access to financi al data. Each role has specific permissions tied to it.

Elements of IAM systems

3. Authentication management

- IAM systems verify that a user’s identity is legitimate befo re allowing access.
- IAM systems use various authentication methods, like pa sswords, biometrics, or multi-factor authentication (MFA), to confirm users.
- **Example:** A user enters their password, and then a one-ti me code is sent to their mobile phone, to log in securely.
- That’s a 2 factor Authentication. More secure method and not easy to guess or steal.

Elements of IAM systems

4. Authorization

- AIMs enforce access rules that determine what each authe nticated user is allowed to do within the system.
- Once a user is authenticated, the system checks their auth orization/ permissions to see and what actions they're allow ed to take based on their role and the rules set by the organ ization.
- **Example:** After logging in, an intern might have "read-only" access, while a manager has "edit" or "delete" permissions i n certain areas.

Elements of IAM systems

5. Monitoring and Auditing

- IAMs track user activities and ensure that access policies are followed.
- IAM systems log all access events and actions taken by u sers, providing an audit history for security and complianc e purposes.
- **Example:** If a user tries to access a restricted area, the s ystem logs this event and may trigger an alert.

Advantages of IAM Systems

- **Improved Security:** IAM systems reduce unauthorized access, ensuring that only the right people can access s ensitive information.
- **Better Compliance:** They help organizations to comply with regulations by keeping records of who accessed wh at information and when.
- **Enhanced Efficiency:** IAMs automates access manage ment, making it easier for IT teams to onboard, offboard, and manage user access.

Best Practices for Access Control

- Best practices for access control in IT risk management focus on securing sensitive data and systems, reducing unauthorized access managing risks, and aligning companies with complian ce requirements.

These practices include;

1. Apply the Principle of Least Privilege

- Grant users the minimum level of access required to perform t heir duties.
- That helps to reduce risks by limiting exposure to critical data a nd resources, minimizing potential misuse.

Best Practices for Access Control

2. Enforce Role-Based Access Control

- Define access based on job roles rather than individual pe rmissions.
- Create roles like “Manager” and “Employee,” each with sp ecific access rights, so that anyone assigned the role auto matically inherits its permissions according to their roles.

3. Implement Multi-Factor Authentication (MFA)

- Use multiple forms of verification for access, such as a pa ssword plus a second factor like a one-time code.
- Set the system requires users to enter a password and a o ne-time code sent to user’s phone, making unauthorized a ccess much harder thus more secure.

Best Practices for Access Control

4. Regularly Review and Audit Access Permissions

- Periodically review access rights to ensure they rema in appropriate and aligned with current roles and resp onsibilities.
- Conduct access audits every quarter to confirm that a ll permissions are current and remove any that are no longer needed.

5. Utilize Separation of Duties

- Divide critical tasks among multiple users to prevent any single person from having complete control over high-risk functions.

6. Adopt the Need-to-Know Principle

- Restrict access to sensitive data based on specifi c job requirements.
- E.g; Allow only team members working on a proje ct to access its data so that unrelated department s cannot, even if have similar access levels.

Best Practices for Access Control

7. Implement Strong Password Policies

- Enforce policies for creating complex passwords e.g require passwords that include uppercase, lowercas e letters, numbers, and special characters, and man date changes every 90 days.

8. Log and Monitor Access Activities

- Keep a record of all user actions within systems, inc luding login attempts and access to sensitive data.
- Set up alerts for unauthorized access attempts or u nusual patterns, like multiple failed logins, and revie w logs regularly.

9. Educate Employees on Access Control Policies

- Train employees on security policies, access control rules, and the risks of improper access.
- Conduct annual training sessions to raises awarenes s, encourage adherence to security practices, and re duce accidental breaches.

Week 8 Summary

1. Access control and Identity Management (AIM)

- A critical component of IT risk management and contr ol which focuses on managing and securing user iden tities, access rights, and permissions within an organi zation.

2. Access

- The ability of a subject (user) and an object (computer s) to interact.

3. Access Control

- Access control is the process of following rules to allo w or deny access to the computer user.

4. The access control process steps;

1. Identification: The process by which a subject i dentifies itself to the access control system.
2. Authentication: Verification of the subject's ide ntity.
3. Authorization: The decision to allow or deny th e subject to access an object.

Week 8 Summary

5. Authentication methods;

1. Password: A secret word or combination of characters that is know n only to the subject.

2. Token: Something the subject has that no one else does, such as a smart card, driving license, passport etc.

3. Fingerprint scan: Involves optical analysis of a person's fingerprint then compare the results with the recorded sample to verify his /her i dentity.

6. principal components of any access control

Policies—The rules that govern who gets access to which resources.

Subjects—The user, network, process, or application requesting acc ess to a resource.

Objects—The resource which the subject desires to access (e.g, files , databases, printers, and physical facilities).

7. Elements of access control

Policies—Clear statements of the business requirements r egarding access to resources.

Procedures—Nontechnical methods, such as business pro cesses and background checks, used to enforce policies.

Tools—Technical methods, such as file system access cont rols and network firewalls, used to enforce policies.

Week 8 Summary

8. subjects of access control

Authorized: Have presented authenticated credentials an d have been approved for access to the resource.

Unauthorized: Have presented authenticated credentials but are not approved for access to the resource.

Unknown: Have not presented authenticated credentials.

9. Objects of Access control

- Information—Any type of data
- Technology—Applications, systems, and networks
- Physical location—Physical locations such as building s and rooms.

10. Principles of Access Control

1. Identification Principle

Identification is the process of recognizing and distingui shing an individual or entity in the system

2. Authentication Principle

Authentication verifies the identity claimed during the id entification phase.

Week 8 Summary

3. Authorization Principle

- Authorization determines what a user is allowed to access or perform within the system.

4. Accountability Principle

- Accountability ensures that actions can be traced back to specific individuals or systems, providing an audit trail of access and activity.

5. Least Privilege Principle;

- Least privilege grants users only the minimum level of access necessary to perform their duties

6. Separation of Duties principle

- Separation of duties ensures that no single individual has control over all aspects of any critical or high-risk process.

7. Need-to-Know principle

- Need-to-know restricts access to data based on specific requirements for users to complete their job tasks.

Week 8 Summary

11. Is Identity Management

- Identity management is the process of creating, maintaining, and closing user accounts and providing the mechanisms used to authenticate users

12. Identity and Access Management (IAMs)

- Identity and Access Management systems are tools and processes that help organizations manage who can access their digital resources and what they can do within those resources

13. Elements of IAMs

1. Identity Management

- IAM systems aim to create and manage the digital identities of users within the organization.

2. Access Management

IAM systems control which resources each user can access and what actions they can perform.

3. Authentication management

IAM systems verify that a user's identity is legitimate before allowing access.

Week 8 Summary

4. Authorization

- AIMs enforce access rules that determine what each authenticated user is allowed to do within the system.

5. Monitoring and Auditing

- IAMs track user activities and ensure that access policies are followed.

14. Advantages IAMs

- **Improved Security:** IAM systems reduce unauthorized access, ensuring that only the right people can access sensitive information.
- **Better Compliance:** They help organizations to comply with regulations b y keeping records of who accessed what information and when.
- **Enhanced Efficiency:** IAMs automates access management, making it e asier for IT teams to onboard, offboard, and manage user access.

Week 8 Summary

14. Best Practices for Access Control

1. Apply the Principle of Least Privilege

2. Enforce Role-Based Access Control

Enforce Role-Based Access Control

3. Implement Multi-Factor Authentication (MFA)

4. Regularly Review and Audit Access Permissions

5. Utilize Separation of Duties

6. Adopt the Need-to-Know Principle

7. Implement Strong Password Policies

8. Log and Monitor Access Activities

9. Educate Employees on Access Control Policies

References

- *Access Control and Identity Management, Mike Chapple and Sean C. Mills third edition, Jones & Bartlett Learning, 2020.*
- *Identity and Access Management: Business Performance Through Connected Intelligence, Ertem Osmanoglu, Syngress, 2013.*
- *Consumer Identity and Access Management: Design Fundamentals, Simon Moffatt, 2021.*

End of Week 8

NEXT LECTURE we will look at-;

***Week 9**: Incident Management and Response*

See u There!