IDENTITY AND ACCESS MANAGEMENT (IAM)

About me

Rassoul Zadeh

SABSA, CISM, CISSP, CRISC, COBIT, CEH, TOGAF Certified

IT and Security Expert Since 1999

https://www.linkedin.com/in/rghaznavizadeh/

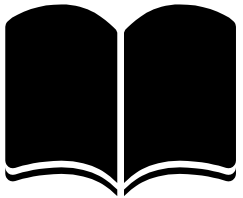
Area of expertise

- Security Architecture
- Security Governance
- Audit & Compliance
- Risk management
- Incident Management
- Security Operation
- Ethical hacking

“Identity and Access Management is a fundamental and critical cybersecurity capability, to ensure the right people and things have the right access to the right resources at the right time.”

—NIST (National Institute of Standards & Technology)

IAM Domains



1. Identification, Authentication, Authorization & Accounting (IAAA)
2. Privileged Access Management (PAM)
3. Identity Governance and Administration (IGA)
4. Data Governance and Protection

Identification, Authentication, Authorization & Accounting (IAAA)

1.

1. CIA Principles
2. IAAA definition
3. Nonrepudiation, Least privileges (Need to Know) & Job rotation principles
4. Kerberos
5. Identity Federation & SSO
6. Passwords and Biometrics

Lab: Setting up Active Directory, and windows domain. Test different type of privileges & policies on domain computers. (Windows 2016 and Windows 10)

Information Security Core Principles (CIA)

- Confidentiality
- Integrity
  - Authenticity
  - Accuracy
  - Non-Repudiation
- Availability

Confidentiality

Examples of confidential data

- PII (Personal Identifiable Information)
- PHI (Personal Health Information)
- IP (Intellectual Property)

Example of controls

- Encryption
- Separation of duty
- Least privileges

Integrity

Authenticity

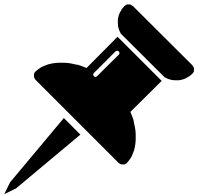
Provide assurance that a message, transaction, or other exchange of data is from the source that it claims to be from.

Accuracy

The stored data on the systems is accurate, trusted, and not modified by unauthorized person.

Non-Repudiation

Assure that senders or recipients can prove that they sent or received the message and cannot deny that.



Availability

Redundancy & Failover

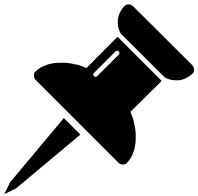
System need to be available all the time, and failing one component shouldn’t have an impact on system operation.

Accessibility

End users need to be able to access the systems and applications all the time without interruption.

Disaster Recovery

In case of a disaster, systems need to be restored and recovered as quick as possible.



Quiz

Virus is a software or computer program that connect itself to another software or computer program to harm computer system and corrupt its data. Choose the most relevant security principle that virus is against it?

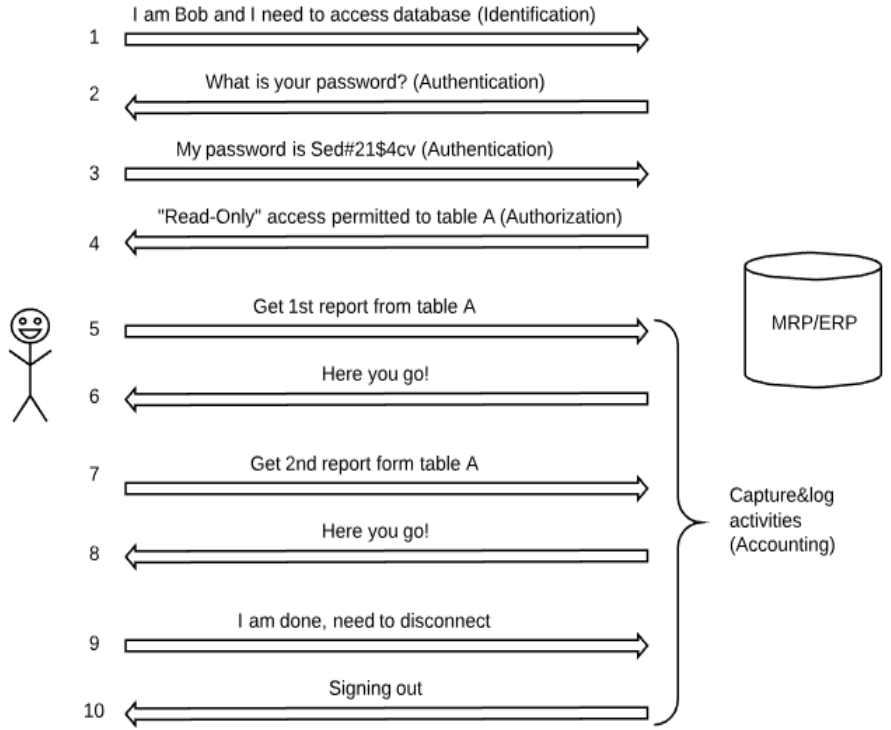
1- Confidentiality

2-Integrity

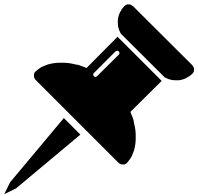
3-Availability

Identification, Authentication, Authorization, Accounting (IAAA)

Set of controls to govern accessing to digital resources, and data, and a mechanism to audit and track the usage, as well as bill for services used.



Information Security Concepts



Least privileges

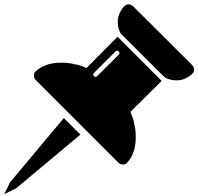
The “least privilege” or “need to know” concept means that only minimum information must be shared with subjects, and only with those who need that information.

Separation of duty

Segregation or Separation of duty concept means to ensure critical roles are not assigned to single user to avoid any possibility of fraud or similar malicious activity.

Job rotation

When one person is on the same job for a long time, that would increase the risks of frauds and collusion. Job rotation is a control to detect and prevent errors and frauds.



Kerberos

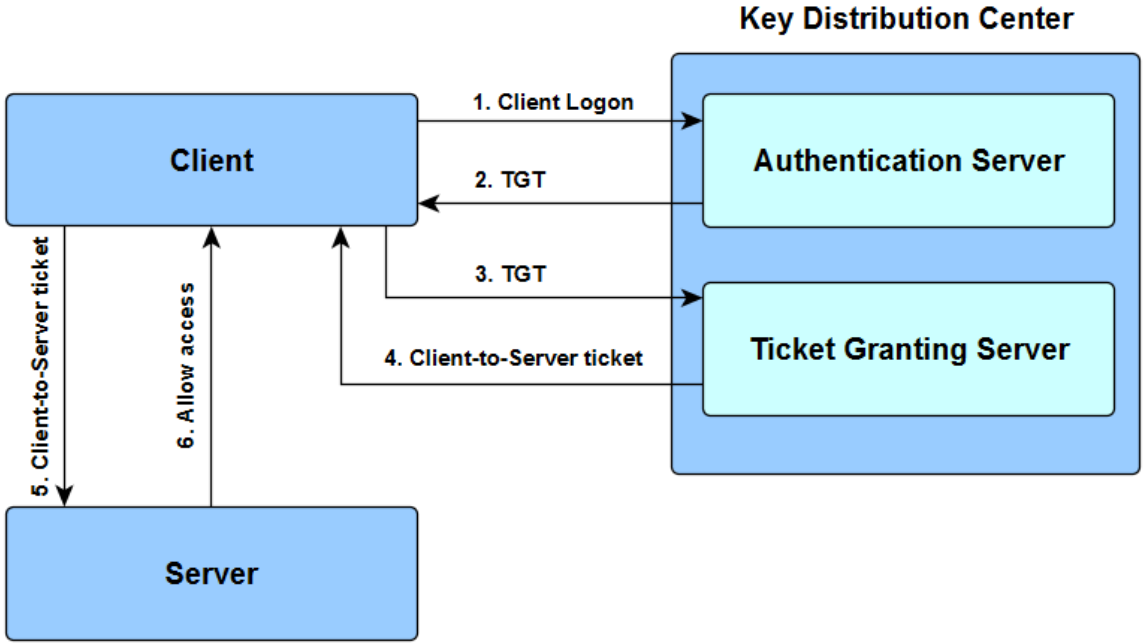
What is Kerberos?

Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography.

How does it work?

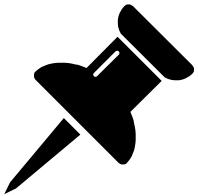
It works on the basis of tickets to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner.

Kerberos Operation



Kerberos Operation

- Client sends an authenticator request to KDC (Key Distribution Centre), encrypted by its password
- KDC knows all the passwords on the network, so it decrypt the request by client's password to confirm it is valid
- After confirming the client is who they say they are, KDC issues a TGT (Ticket Granting Ticket) to the client, encrypted by its own key
- Client stores TGT in its Kerberos tray located on the memory (normally valid for 8 hours)
- When client needs access to a resource (e.g. share folder on a server), it sends the TGT back to the KDC, and requests access
- KDC validates the TGT, and then issues another ticket to the client encrypted with the destination server key
- The client sends that ticket to the destination server. The server decrypts it with its key to ensure it is valid, and then allows client to access



Quiz

Your company has some servers in a global data center. You take your Driver license there, and after some verification, they issue an ID card for you in order to fast track your entry into the facility going forward. The issued ID is similar to which Kerberos feature?

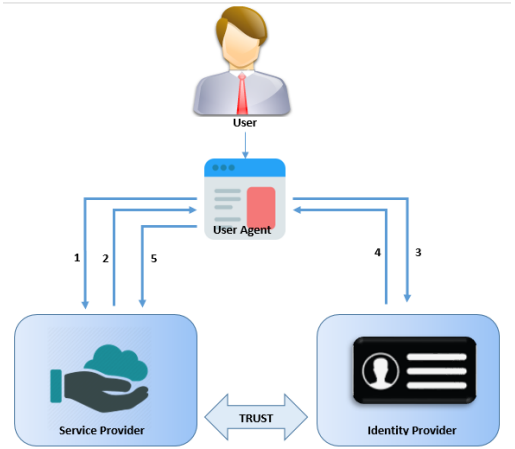
1- KDC

2-TGT

3-Client-to-Server ticket

Identity Federation

Federation connects different identity management systems together (hence the name federation). In a federated system, a central home node or identity provider stores the users' identities.



Identity Federation

Service Provider (SP)

Users use the applications or services provided by the service providers. For example, Oracle is the SP for Oracle cloud financial solutions.

Identity Provider (IDP)

Users authenticate against Identity Providers. IDP is normally where all the user information located, and all service providers can use those to authenticate users against the same credentials. Some examples of IDP are Okta, or Microsoft ADFS while there are also free IDPs like Google, Facebook.

SAML & SSO

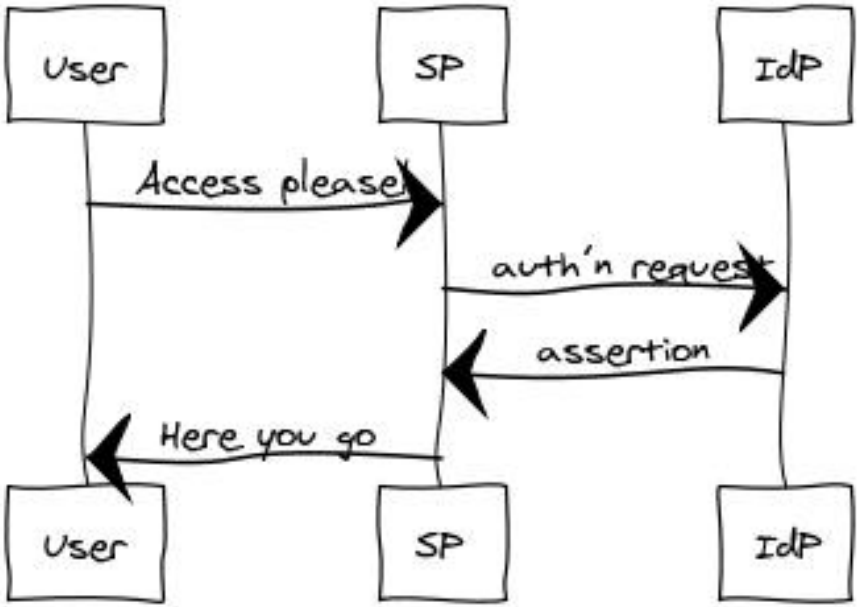
Single Sign-On (SSO)

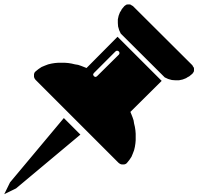
Single sign-on (SSO) is a session and user authentication service that permits a user to use one set of login credentials (e.g., name and password), and authenticate once to access multiple applications.

SAML

Security Assertion Markup Language (SAML) is an XML-based framework for Single Sign-On. It provides authentication and authorization between two entities: a Service Provider and an Identity Provider.

SAML/Federation Operation





Quiz

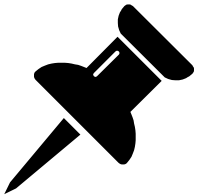
Which of the below statements is correct about federated identity and SSO?

1- It minimizes the risks of credential theft, as it is centralized

2- The risks are high because credentials are transferred on the internet between SP and IDP

3-The risks could be high, as if one account is hacked, attacker can access all of the resources with same credential

Authentication Factors



Something you know

Passwords, passphrases, PIN numbers, Passcodes.

Something you have

USB Token, Mobile phone, Email access, etc.

Something you are

Biometrics.

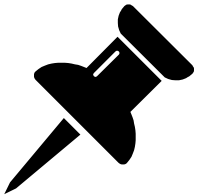
Something you do

Typing speed, location, etc.

NIST Guideline

NIST Special Publication 800-63B

Authentication methods



Single Factor

Username and Passwords

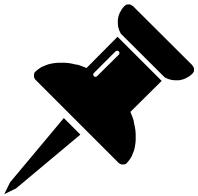
2 Factor

Using an additional authentication method in addition to password. E.g. SMS verification

Multi Factor

Other methods in addition to 2nd factor, like biometrics, or human characters like typing speed, location, etc.

Strong Authentication

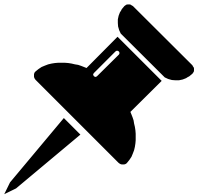


Strong Passwords

- Min 8 characters
- Mix characters, numbers and symbols
- Avoid known, easy to guess or historical passwords
- Use Passphrases instead
  - Sequence of words or other text

NIST Special Publication 800-63B

Strong Authentication



2nd Factor (Token-based authentication)

- Synchronous: They are time-based, synced with a server, and change on specific interval
  - E.g. RSA USB Token, Google authenticator
- Asynchronous: They are not synced with a server
  - E.g. SMS text, Email message

Strong Authentication

Biometrics

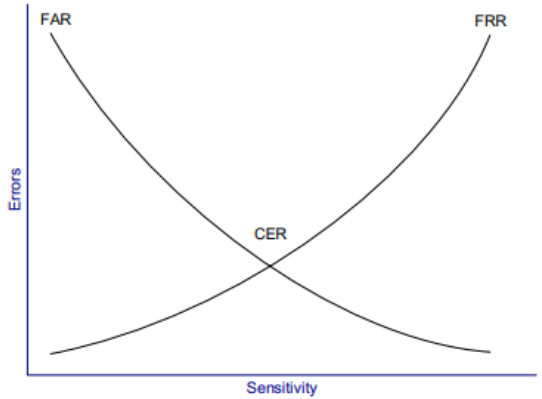
- Fingerprint scan uses person’s unique fingerprint and identifies against the database.
- Retina scan is a laser scan of the capillaries that feed the retina of the back of the eye.
- Iris scan is using the picture of colored portion of the eye, and then compares photos within the authentication database
- Facial scanning (also called facial recognition) is the process of passively taking a picture of a subject's face and comparing that picture to a list stored in a database

Strong Authentication

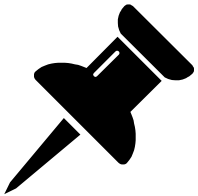
Biometrics

- Keyboard dynamics refer to how hard a person presses each key and the rhythm in which the keys are pressed.
- Dynamic signatures measure the process by which someone signs his/her name.
- voiceprint measures the subject's tone of voice while stating a specific sentence or phrase.

Biometrics Rates



- **False reject rate**: A false rejection occurs when an authorized subject is rejected by the biometric system as unauthorized. (That's bad user experience.)
- **False accept rate**: A false acceptance occurs when an unauthorized subject is accepted as valid. (That's a big security risk.)
- **Crossover error rate**: The CER describes the point where the FRR and FAR are equal. CER is also known as the equal error rate (EER). The CER describes the overall accuracy of a biometric system.



Quiz

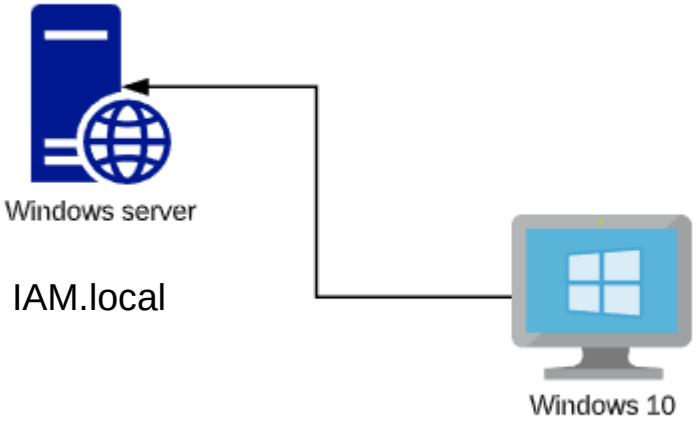
Which one of the below combination of authentication methods is not using a single factor authentication?

1- Password and Security question

2- Passcode and PIN number

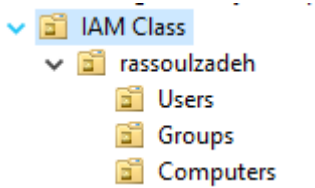
3- Password and SMS code

LAB

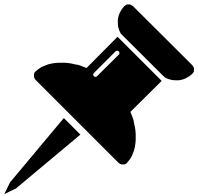


LAB

- Login to Win10 with your admin account and default password
- Change your password!
- Open AD users and computers management tool, Go to “IAM Class” OU
- Create an OU with your name (fnamelname)
  - OU is the “Organization Unit” used in Microsoft Active Directory
- Create 3x new sub-OU, as it shows on the picture



LAB

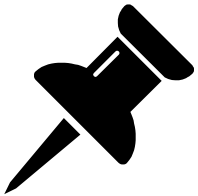


- Login to Win10 with your admin account
- Go to your own OU, and “Users” section
- Create a user with username being “user.<finitial><lname>1” (e.g. user.rzadeh1)
- Open computer management on your Win10
- Add the domain created users to “Remote Desktop Users” group
- Logout from the machine, and log back in with the standard user created
- Try to create a new user on AD user management tool, what changed?

LAB

- Login to Win10 with your admin account
- Go to your own OU, and “Users” section
- Find your username and modify its properties
- Update the tabs for General, Address, Telephones and Organization
- Go to Account tab, review the username, and account options

LAB

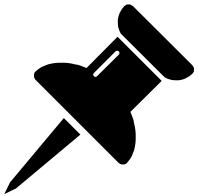


- Open AD user management tool
- Find your computer name, and move the object to your own OU ->“Computers”
- Run “Group policy management” and create a new policy and link it to your OU
- Edit the policy and go to Computer Configuration->Windows settings>security settings ->Account settings->password policy settings, and apply the below changes:

LAB

- Enforce password history: 0
- Minimum password length: 6 character
- Password must meet complexity: Disabled
- Now logout and log back in with your standard user
- Open a command prompt and run this command: “gpupdate /force” (Or restart)
- Now try to change the password a few times, try simple passwords with less or greater than 6 characters

LAB



- Log back in with Admin account and change the policy setting again:
- Enforce password history: 5
- Minimum password length: 8 character
- Password must meet complexity: Enabled
- Now logout and log back in with your standard user
- Open a command prompt and run this command: “gpupdate /force” (Or restart)
- Now try to change the password a few times, try simple passwords, and less than 8 character, and passwords you used before

LAB

- Log back in with Admin account and change the Lockout policy setting:
- Review the Account lockout policy
- Set the lockout policy as below:
- Account lockout duration: 30 min
- Account lockout threshold: 3 invalid logon
- Reset account lockout counter after: 30 min
- Run “gpupdate /force” command

LAB

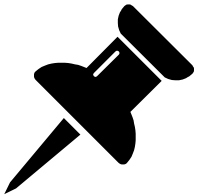
- Logout and try to login with your standard account
- Try entering wrong password for 3 times
- Your account should be locked for 30 min now
- Login with your admin account
- Open AD user management tool
- Find your standard user name, go to properties, select “unlock this account” and Apply
- Logout and Log back in with your standard account

Privileged Access Management (PAM)

2.

1. Privileged or Administration accounts
2. Privileged Credential Management
3. Privileged Session Management
4. Privileged Accounts Monitoring and Analysis
5. Privileged Access Management Solutions
6. Application Whitelisting and Software Restrictions

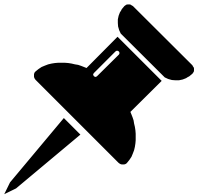
Lab: Continue with previous lab. Test different type of privileged groups on AD. Rename the local admin accounts, and update the policies. Utilize password management solutions. Live ManageEngine PAM demo.



Privileged accounts

Privileged accounts are those with special permissions on a system, application, database or any other asset that can be used to perform any administration activity (E.g. changing the configuration), or have full access to the data.

Key principle: *Always enforce least privilege over end users, endpoints, accounts, applications, services, systems, etc.*



Privileged accounts

Local admins

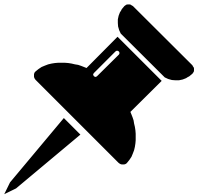
Non-personal accounts that provide administrative access to the local host or instance only.

Domain Admins

Privileged administrative access across all workstations and servers within Windows domain.

Emergency Admins

Provide unprivileged users with administrative access to secure systems in the case of an emergency (Also referred to as ‘breakglass’ accounts.)



Privileged accounts

Root Accounts

Super administrations access to systems or applications. (E.g. Linux, AWS)

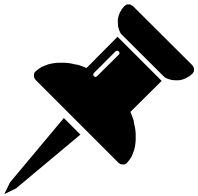
Service Accounts

Can be privileged local or domain accounts that are used by an application or service to interact with the operating system. (e.g. backup account)

Application Admins

Have special access to applications and their databases to import/export data, run scripts, create backups and restores, etc.

Privileged Credential Management



Password Managers

Password managers are important for storing and managing credentials. Storing passwords on documents, spreadsheets, or papers could result in data breach.

Shared Credentials

Using shared privileged credential must be avoided unless it is absolutely necessary. Utilizing shared credentials could increase the risks of data loss.

Access & Encryption

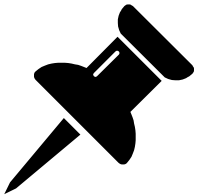
All credentials must be encrypted and only accessible by those who need or own them.

Privileged Session Management

Man In the Middle Attack (MITM)

Attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other.

Privileged Session Management



Session Integrity

Is the destination authentic?

Are the changes on the system being tracked?

Session Monitoring

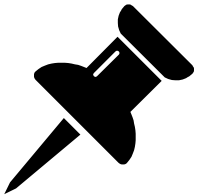
Are we monitoring the usage of privileged accounts?

Can we track the activities later for audit purposes?

Session Encryption

Is the session between privileged user and the asset encrypted?

Can only authorized people view the traffic?



Quiz

Which one of the below protects us against man in the middle attack?

1- Encryption

2- Authentication

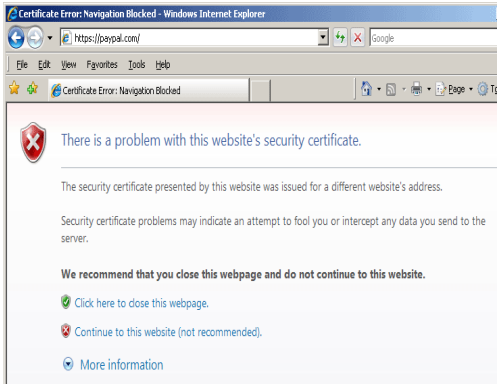
3- Authorization

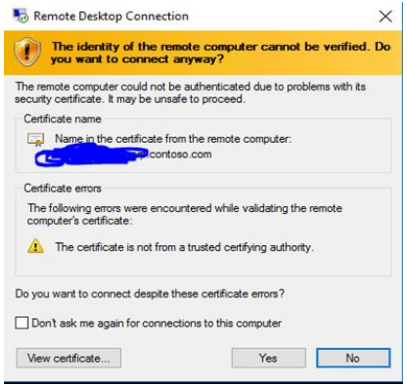
4- Password managers

Privileged Session Management

Certificates & Encryption

Certificates are used to verify and validate users and applications. They can also used to encrypt the session between client and server.





Privileged Account Monitoring & Analysis

Logging and Auditing

Any activity performed by a privileged account need to be logged, so can be audited later if required.

Anomalies & Alerting

Privileged accounts usage should be monitored for malicious usage, and when detected alerts need to be generated.

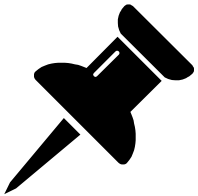
Session Recording

Privileged sessions need to recorded, where possible due to laws and regulations, so can be reviewed and tracked later, if needed.

Privileged Access Management Solutions

What is PAM?

Privileged access management (PAM) consists of the cybersecurity strategies and technologies for exerting control over the privileged access and permissions for users, accounts, processes, and systems across an IT environment.



PAM Components

Credential Management

Privileged credentials stored in a secure database.

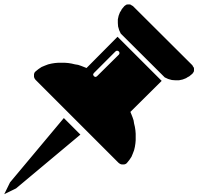
Access Management

Only authorized users can access the credentials or systems. MFA can be enabled to access resources.

Session Management

Secure connectivity to the resources is provided via PAM. This can be RDP, SSH, HTTPS, etc.

Sessions can also be recorded, if needed.



PAM Components

Logging and Auditing

Any activity performed by a privileged account is logged, and can be audited later if required.

Security Monitoring

Privileged accounts are monitored for malicious usage, and any anomaly will generate an alert.

Reporting

Reports can be generated based on the usage of privileged accounts and administration activities.

Quiz

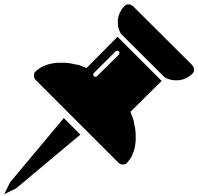
What is the highest risk that PAM solution will help to minimize?

1- IT administrators abuse admin privileges to access unauthorized data

2- Sensitive passwords are stored on documents or spreadsheet

3- Malicious usage of privileged accounts

Application whitelisting



Application whitelisting, one of the Australian Signals Directorate (ASD)’s Essential Eight cyber threat mitigation strategies, is primarily designed to protect against malicious code execution on protected systems.

When implemented properly it ensures that only authorised applications (e.g. executables, software libraries, scripts and installers) can be executed.

Software Restriction Policies

Software Restriction Policies (SRP) is Group Policy-based feature that identifies software programs running on computers in a domain, and controls the ability of those programs to run. Software restriction policies are part of the Microsoft security and management strategy to assist enterprises in increasing the reliability, integrity, and manageability of their computers.

Note: Applocker is the new Microsoft solution for software restriction.

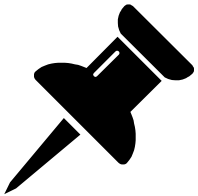
LAB

- Login to Win10 with your admin account
- Open AD user management tool, Go to “IAM Class”->”Admins” OU
- Create a user with username being “admin.firstinitiallastname.dhcp”
  - Add this user to “DHCP Administrators” group
- Create a user with username being “admin.firstinitiallastname.dns”
  - Add this user to “DNS Administrators” group

LAB

- Login to Win10 with the account created for DHCP
  - On remote server administration tool, select DHCP
  - Try to create a new scope, and see the results. (Don’t need to create anything, cancel after you see the prompt)
  - Try to run other administration tools, like DNS and see the results
  - Try creating a new user with AD user management tool

LAB

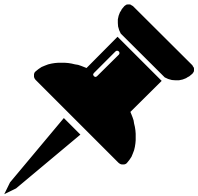


- Login to Win10 with the account created for DNS
  - On remote server administration tool, select DNS
  - Click on the “Forward Lookup Zones” then domain zone name
  - Create a TXT record, with your fnamelname as record name and text
    - Use “Other New Records” to create a txt record
  - Try to run other administration tools, like DHCP and see the results
  - Try creating a new user with AD user management tool

LAB

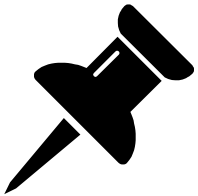
- Login to Win10 laptop with local admin account (use .\administrator to login locally)
- Logout and Login to Win10 laptop with your domain admin account
- Press Win+”R”, then type “gpedit.msc” and enter to open group policy
- Go to Computer->Windows->Security settings and then Security options
- Find “Accounts: Rename administrator account” and rename the machine local admin account name to “iamadmin”
- Logout and Log back into Win10 with local account (try .\administrator and .\iamadmin)

LAB



- Login to Win10 laptop with your domain admin account
- Hold Windows button and “R” then type “gpedit.msc” and enter
- Go to Computer->Windows->Security settings and then Audit policy
- Find “Audit privilege use” and select both “Success” and “Failure”
- Open computer management and create a test group
- Go to Windows event viewer, Windows logs and review security logs

LAB



- Register for a LastPass account (https://www.lastpass.com/)
- Install LastPass and login
- Add all of your Windows accounts and passwords to LastPass
  - Use “Server” as the type of item
- Review the item types you can add, is there anything else you can add there?
  - Web passwords, notes, address, etc.

LAB

- Go to PAM36 demo on ManageEngine (https://pam360demo.manageengine.com/)
- Login with Password Administrator role & review
- Login with Password user role & review
- Login with Password Auditor role and
  - Create a user access and use activity report
  - Create a full ISO 27001 compliance report

Identity Governance and Administration (IGA)

3.

1. User Onboarding & Termination
2. Access Requests, Role Changes
3. Access Controls
4. Role-Based Access Control
5. Access validation & Certification
6. Segregation of Duties
7. Identity Auditing and Reporting
8. Identity Lifecycle Management (ILM)

Lab: Continue with the previous lab. Create specific groups for specific roles. Review logging and auditing capabilities of AD. Live demo of ManageEngine ADAudit Plus.

User Onboarding

Account creation

As soon as a user starts working for an organization, a new account need to be created for him/her.

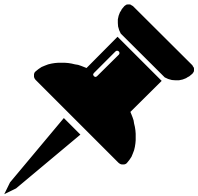
Access requirements

All access requirements for the new starter need to be evaluated, and requested.

Training requirements

The new starter need to be trained on policies, and security requirements before accessing systems.

User Onboarding – Examples



Account creation

Account on Human Resource Platform to start employment.

Account on Active Directory to connect to network.

Access requirements

Physical Access: ID Badge, Laptop, Mobile device

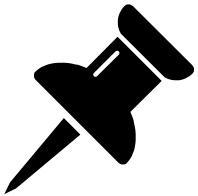
Application Access: Windows domain, Finance application, Helpdesk system, etc.

Training requirements

Information Security Policy.

Security Awareness Training.

IT induction training.



User Termination

Account termination

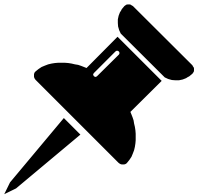
As soon as a user contract is terminated, their user accounts need to be closed or disabled.

Access revocation

As soon as a user is left, or contract is terminated, his/her access to all systems need to be revoked.

Asset collection

Upon termination of a contract, all the assets used by a user need to collected. Data on personal asset need to be wiped.



Role changes

Permission inheritance challenges

When a user starts working in a department, he/she might have specific permissions based on where is working. When they are moved to a different department, their old access permissions need to be revoked.

Example: Rob is working in Finance department, and has access to financial data, but after a while he joins IT department. After joining IT, Rob still has access to financial data unless there is a process to revoke his permissions.

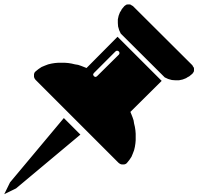
Quiz

A new IT Administrator is joining your company on Monday. Which one of the below is not an immediate requirement for him?

1- Creating a user account

2- Induction and security training

3- Admin access provisioning to IT systems



Access Controls

Centralized

Permissions and Privileges are assigned to users centrally by administrators.

Decentralized

Permissions and privileges can be managed on each asset, and not managed centrally.

Benefits & Challenges

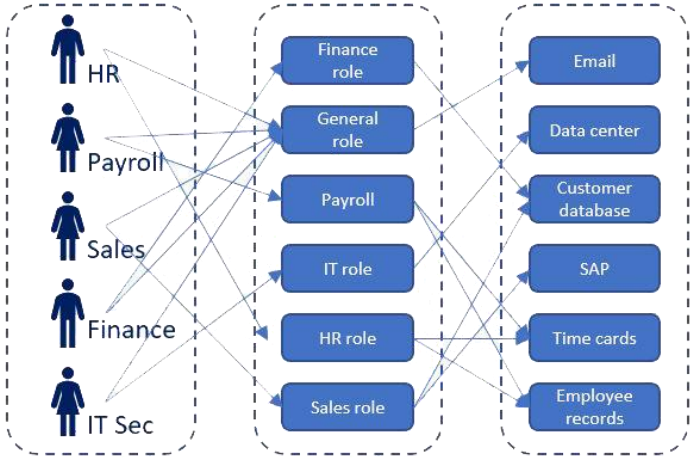
Decentralized Access Controls are easier to implement, but harder to manage and monitor for security violations.

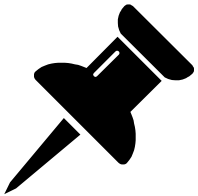
Role Base Access Control (RBAC)

RBAC

Centralized access-control mechanism defined around roles and privileges.

Each user will have a role, and permissions are assigned to roles, not users.





Quiz

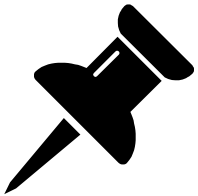
Which one is the downside of the centralized access management model?

1- Administration overhead

2- User training

3- Security risks

Access validation & Certification



Access validation

Data or System owner need to review and validate the access given to individuals.

Access Certification

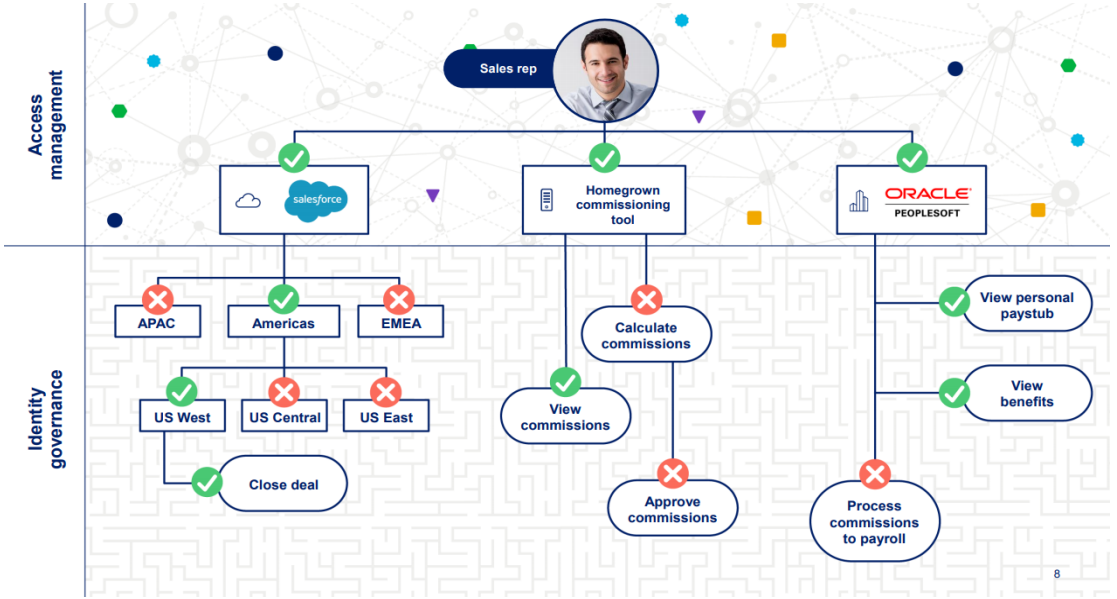
Data or System owner need to update, adjust and confirm/certify that access given to individuals is correct.

Frequency

Access validation and certification is an ongoing process. For privileged accounts, it is recommended to do this at least on monthly bases.

NIST Special Publication 800-53
AC-6 LEAST PRIVILEGE

Access validation example



Segregation of Duties

What is SoD?

The goal of segregation of duties is to prevent combinations of roles that could facilitate fraud or embezzlement.

Compliance

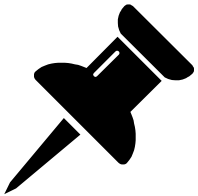
SoD is one of the top control requirements on Sarbanes Oxley (SOX). SOX is one of the biggest financial compliance frameworks for public companies to protect customers and shareholders.

Australia's equivalent of Sarbanes-Oxley are the ASX corporate governance principles released in March 2003. (Provides guidelines unlike SOX mandatory controls)

Segregation of duty – Some examples

- Example 1:
  - Creating a new supplier
  - Submitting an invoice
  - Approving for payment
- Example 2:
  - Requesting a user access to sensitive data
  - Approving user access to data, and adding to relevant group
- Example 3:
  - Going out for dinner with your manager
  - Pay for your manager's dinner
  - Submit the invoice and get it approved by your manager

Identity Auditing and Reporting



Event logging

All access requests and updates activities need to be logged and should be tamper-proof.

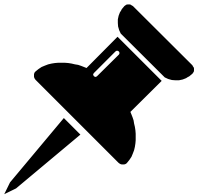
Alerting & Reporting

Invalid user access & risky users should be reported and generate an alert. On-demand reports should be created for audit activities.

Compliance

Should be able to prove your compliance controls are working to auditors.

Quiz



What best explains the purpose of access validation?

1- To provide necessary permission to those who need it

2- To avoid attacker gaining access to sensitive information

3- To apply “least privilege” concept

Identity Lifecycle Management (ILM)

What is ILM?

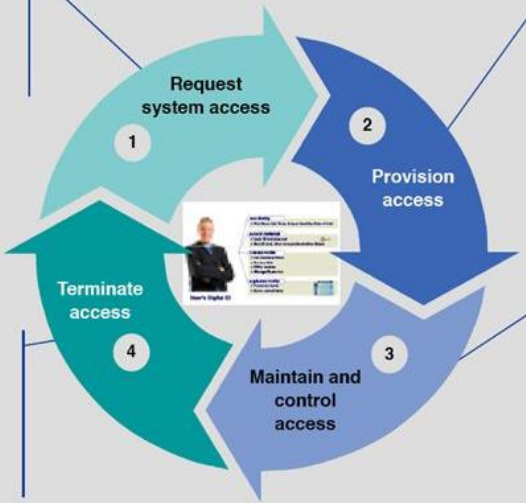
Identity Lifecycle Management, or ILM, refers to a collection of technologies and business processes utilized in creating, managing, coordinating and restricting the identification, access and governance of identities for access to business tools and information.

-Webopedia

Identity Lifecycle Management

Identity Lifecycle Management

- Identity is created as the first step of on-boarding employees, contractors, or business partners
- Identity is created in authoritative sources, such as HR system

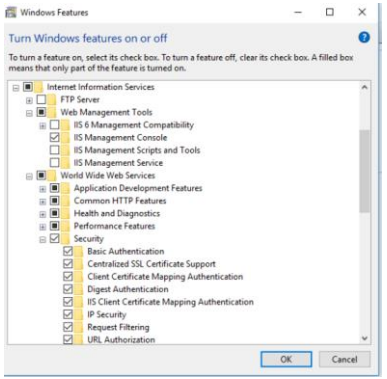


- User accounts are set up for each of the resources that user will access
- Initial access permissions are appropriately configured on each resource

- Removing user access permissions from all managed resources
- Scheduled user termination
- Unscheduled user termination

- User lifecycle management:
  - Access request
  - Transfer
  - Status change
  - Approvals
- Access Review
  - User access recertification
  - Approver actions
  - Administrator actions

LAB



- Login to Win10 with your admin account
- Go to Control Panel->Programs->Turn Windows features on or off
- Select Internet information services, and everything in “Security”
- Install all the selection by clicking on OK
- Open a browser and browse http://localhost
- Open IIS, go to default website->Authentication and disable anonymous authentication
- Open a browser again, and browse http://localhost

LAB

- Open IIS, go to default website->Authentication
- Enable Windows Authentication
- Open a browser again, and browse http://localhost
- Open IIS, go to default website->Authentication
- Disable Windows Authentication and Enable Basic Authentication
- Open a browser again, and browse http://localhost
- Try login with your standard user (domain\user.name1)

LAB

- Open IIS, go to default website-> “Edit Permission” from the Action tab
- Go to Security tab -> Add your standard user (user.name1) and deny all permissions
- Open a browser in private mode (or clear the cache), and browse http://localhost
- When prompted for password try “domain\user.name1”
- Try again with “domain\admin.name”

LAB

- Login to Win10 with your admin account
- Open AD user management and go to your OU
- Create a few security group on “Groups” OU, as below
  - FinanceGroup.<finitial.lname> (e.g. FinanceGroup.rzadeh)
  - HRGroup.<finitial.lname>
  - ITGroup.<finitial.lname>

LAB

- Login to Win10 with your admin account
- Open AD user management and go to your OU
- Create a few users on “Users” OU, as below
  - FinanceUser.<finitial.lname> (e.g. FinanceGroup.rzadeh)
  - HRUser.<finitial.lname>
  - ITUser.<finitial.lname>

LAB

- Login to Win10 with your admin account
- Open AD user management and assign the below users to their relevant group
  - FinanceUser.<finitial.lname> To FinanceGroup.<finitial.lname>
  - HRUser.<finitial.lname> To HRGroup.<finitial.lname>
  - ITUser.<finitial.lname> To ITGroup.<finitial.lname>

LAB

- Open IIS, go to default website-> “Edit Permission” from the Action tab
- Only allow the FinanceGroup you created to access this website, and prevent ITGroup and HRGroup from loading this website.
- Open a browser in private mode (or clear the cache), and browse http://localhost
- Verify the settings are working properly. Try browsing with different users.

LAB

- Login to Win10 laptop with your domain admin account
- Hold Windows button and “R” then type “gpedit.msc” and enter
- Go to Computer->Windows->Security settings and then Audit policy
- Select both “Success” and “Failure” for all audit options
- Go to Windows event viewer, Windows logs and review security logs

LAB

- Go to ADAuditPlus demo on ManageEngine (https://demo.adauditplus.com/)
- Login with Technician Account
- Review the dashboard
- Create a report for the last 24 hours on below items
  - All AD changes
  - Recently created users
  - User permission changes
  - Logon failures

Data Governance and Protection

4.

1. Data Types and Classification
2. Industry and local laws and regulations
3. Structured vs Unstructured Data Management & Monitoring
4. Security Policies, Standards, and Procedures
5. Data Breach and Incident Response Process

Lab: Continue with previous lab. Create different share for different groups and test access controls. Live demo of ManageEngine ADAudit Plus. Incident Response Table top exercise.

Data Types and Classification

Data types

Different data or Information types have different meaning for individuals and organizations.

For example, patient records are important for a healthcare company, while credit card information is important for a bank.

Some Sensitive Data Types

PII

Personally identifiable information.

Important for all industries.

PHI

Protected health information.

Important for Healthcare.

IP

Intellectual Property.

Important for innovators.

Financial

Credit cards, financial data, etc.

Important for financial industries and others.

PII/PHI – Identifiable information

- Full name
- Home address
- Email address
- Social security number
- Passport number
- Driver's license number
- Credit card numbers
- Date of birth
- Telephone number
- Log in details
- Location data
- Medicare number
- Medical records
- Device identifiers and serial numbers
- Health insurance beneficiary numbers
- Biometric identifiers

Quiz

Which combination below is not considered highly identifiable information?

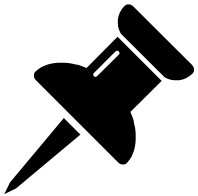
1- Firstname, Lastname and Birth date

2- Firstname, Birthday, and Email Address

3- Firstname, Driver license number

4- Firstname, Country, Eye color

Intellectual Property



- **Trademark**: Refers to the specific attributes which are unique to each organization, like logos, words, slogans, or images.
- **Trade Secret**: Company confidential and valuable information that are used for operation and growth, and are not publicly available
- **Licensing**: Legal and contractual agreement between vendor or provider and the customer
- **Patent**: Recognizable license or right by a government authority on an intellectual property for a specific period of time.

Data Classification

Protective marking		Business impact level	Compromise of information confidentiality would be expected to cause:
Public	UNOFFICIAL	No business impact	No damage. This information does not form part of official duty.
	OFFICIAL	1 Low business impact	No or insignificant damage. This is the majority of routine information.
	OFFICIAL: Sensitive	2 Low to medium business impact	Limited damage to an individual, organisation or government generally if compromised.
PROTECTED	PROTECTED	3 High business impact	**Damage** to the national interest, organisations or individuals.
SECRET	SECRET	4 Extreme business impact	**Serious damage** to the national interest, organisations or individuals.
TOP SECRET	TOP SECRET	5 Catastrophic business impact	**Exceptionally grave damage** to the national interest, organisations or individuals.

Industry and local laws and regulations

Australian Government

Office of the Australian Information Commissioner

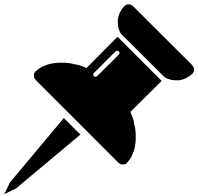
ACSC Australian Cyber Security Centre

Australian Cyber Security Centre (ACSC)

The Australian Cyber Security Centre (ACSC) is the Australian Government's lead on national cyber security. It brings together cyber security capabilities from across the Australian Government to improve the cyber resilience of the Australian community. ACSC is part of Australian Signals Directorate (ASD).

Reference: https://www.asd.gov.au/cyber

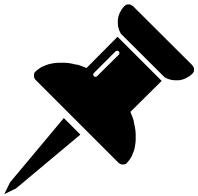
Protective Security Policy Framework



The Protective Security Policy Framework (PSPF) has been developed to assist Australian Government entities to protect their people, information and assets, at home and overseas.

Reference: https://www.protectivesecurity.gov.au/

OAIC (Office of the Australian Information Commissioner)



OIAC is responsible for privacy functions that are conferred by the Privacy Act and other laws. Under the Privacy Act a person can make a complaint to us about the handling of their personal information by Australian, ACT and Norfolk Island government agencies and private sector organisations covered by the Privacy Act.

Reference: https://www.oaic.gov.au/

PCI Security Standards Council

The PCI Security Standards Council (PCI SSC) is a global forum that brings together payments industry stakeholders to develop and drive adoption of data security standards and resources for safe payments worldwide.

Reference: https://www.pcisecuritystandards.org/

HIPAA (Health Insurance Portability and Accountability Act)

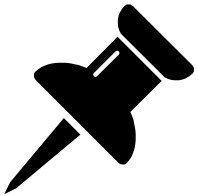
The Health Insurance Portability and Accountability. It was created primarily to modernize the flow of healthcare information, and protect Personally Identifiable Information maintained by the healthcare and healthcare insurance industries.

Reference: https://www.hhs.gov/hipaa/index.html

GDPR (General Data Protection Regulation)

The General Data Protection Regulation 2016/679 is a regulation in EU law on data protection and privacy in the European Union and the European Economic Area. It also addresses the transfer of personal data outside the EU and EEA areas.

Reference: https://gdpr.eu/



Quiz

Which of the below frameworks is the most relevant for banks?

1- HIPAA

2- PSPF

3- PCI

Structured vs Unstructured Data

Structured Data

Referring to the data that is organized and formatted in a way that is easily searchable.

Example of structured data is data in databases like SQL

Unstructured Data

Referring to the data that is not organized, and is not in a pre-defined format. This type of data is hard to monitor, process and analyse.

Example of unstructured data is Microsoft Office documents.

Data Management & Monitoring

Structured Data

- User Access Controls: Give access to users who need to have access
- Database Security Monitoring: Monitor security of database and access violations
- Logging and Auditing: Monitor activities on the database
- Data Encryption: Encrypt your data and secure the keys

Data Management & Monitoring

Unstructured Data

- User Permissions: Allow access to who need to have access
- Data Encryption: Encrypt the files and secure the key
- Metadata and Labelling: Classify data by assigning a metadata to them
- Data Loss Prevention Solutions (DLP): Identify and protect sensitive data automatically
- File Integrity Monitoring: Identify and detect changes to the files

Quiz

Microsoft word and excel documents stored in a central storage location are what type of data?

1- Structured

2- Unstructured

Security Policy Framework

- Policy: Outlines senior management’s expectation of security
- Standard: Formalizes mandatory security requirements to protect assets
- Procedure: Explains how to perform security functions within organization
- Guideline: Outlines recommendations, statements and instructions
- Baseline: Minimum security for technology specification, configurations, architecture

Security Policy Framework

Document Type	Description	Mandatory/Discretionary
Security Policy	Business expectation and requirements for security	Mandatory
Security Standard	Detailed technology and process requirements to protect assets	Mandatory
Security Procedure	Step by step work instruction to ensure policies and standards are followed properly	Mandatory
Security Guideline	Best practices and recommendations about security aligned with policy	Discretionary
Security Baseline	Minimum level of accepted security controls	Minimum Mandatory, Additional Discretionary

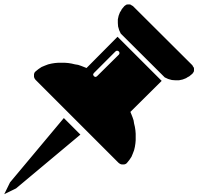
Data Breach and Incident Response Process

- Companies are required to have a process in place to be able to respond to security incidents when they happen
- Companies are required to understand their liabilities, and notify relevant authorities when sensitive data is lost.

Incident Response Process

- **Preparation –** Ensure skills and resources are available to effectively respond to any incident.
- **Identification –** Detect incidents in several ways, (e.g. phone call, monitoring).
- **Containment –** Isolate the incident and prevent further damage.
- **Remediation –** Determine cause and symptoms of incident, act to remediate.
- **Recovery –** Restore to normal state and operational use.
- **Lessons Learned –** Document / Debrief incident details to improve the process.

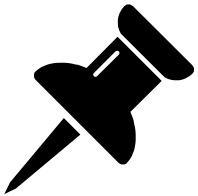
Notifiable data breaches (OAIC)



A data breach happens when personal information is accessed or disclosed without authorisation or is lost. If the Privacy Act 1988 covers your organisation or agency, you must notify affected individuals and us when a data breach involving personal information is likely to result in serious harm.

Reference: https://www.oaic.gov.au/privacy/notifiable-data-breaches/

When to report a data breach (OAIC)

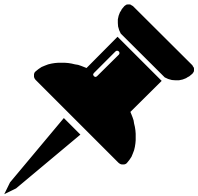


Under the Notifiable Data Breach (NDB) scheme an organisation or agency must notify affected individuals and the OAIC about an eligible data breach.

An eligible data breach occurs when:

- there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an organisation or agency holds
- this is likely to result in serious harm to one or more individuals, and
- the organisation or agency hasn't been able to prevent the likely risk of serious harm with remedial action

LAB

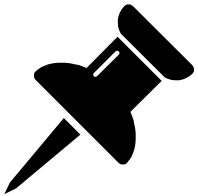


- Login to Win10 with your admin account
- On your C: drive create a folder called IA and 4 subfolder
  - Public, Finance, IT, HR
- On each folder properties and security settings, assign the permission to relevant groups and deny other groups
  - Public folder should be accessible to everyone
- Login with different users and try accessing those folder
  - If you have access, try to create a text file in each folder

LAB

- Login to Win10 with your admin account
- On your C: browse to the folders created
- Allow ITGroup to read from other folders but not be able to write
- Login with ITUser you created
- Try opening the text files from different folders
- Try creating text files in different folders

LAB

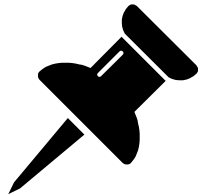


- Login to Win10 with your admin account
- On your C: browse to the folders created
- On Finance folder properties got to security tab->Advanced->Auditing
- Add “Everyone” in there as principle and select Full Control as permission, then OK.
- Hold Windows button and “R” then type “gpedit.msc” and enter
- Go to Computer->Windows->Security settings and then Audit policy
- Ensure both success and failure is selected for “Audit Object Access”

LAB

- Login to Win10 with your ITUser account
- On your C: browse to the folders created
- Open Finance folder and review some files
- Try to copy some files in the Finance folder
- Open Event Viewer and Security logs. Filter the logs for Event ID 4663
- Review the audit logs

Assignments



IAM-Assignments.docx