IT INFRASTRUCTURE MANAGEMENT WEEK 9 ASSIGNMENT

1.Explain about the different identity management models.

Identity management (IdM), also known as identity and access management (IAM) ensures that authorized people – and only authorized people – have access to the technology resources they need to perform their job functions. It includes polices and technologies that encompass an organization-wide process to properly identify, authenticate, and authorize people, groups of people, or software applications through attributes including user access rights and restrictions based on their identities.

An identity management system prevents unauthorized access to systems and resources, helps prevent exfiltration of enterprise or protected data, and raises alerts and alarms when access attempts are made by unauthorized personnel or programs, whether from inside or outside the enterprise perimeter.

Identity management solutions not only protect software and data access, they also protect the hardware resources in an enterprise, such as servers, networks, and storage devices from unauthorized access which could lead to a ransomware attack. Identity management has gained importance over the past decade due to the growing number of global regulatory, compliance, and governance mandates that seek to protect sensitive data from exposure of any kind.

IdM and IAM systems generally are part of IT security and IT Data management within the enterprise, and identity and access management tools are widely available for the broad range of devices that users rely on to perform business functions from phones and tablets to desktop computers running Windows, Linux, iOS or Android.

IdM and IAM are terms often used interchangeably, however identity management is more focused on a user identity (or username), and the roles, permissions, and groups that user belongs to. IdM also focuses on protecting identities through a variety of technologies such as passwords, biometrics, multi-factor authentication, and other digital identities. This is usually achieved by the adoption of identity management software applications and platforms.

How does Identity Management Work?

As part of an overall IAM framework which covers access management and identity management, enterprises typically utilize both user management component and a central directory component such as Active Directory for Windows or Apache Directory Studio or Open LDAP for Linux systems.

The user management component handles delegation of admin authority, tracking roles and responsibilities for each user and group, provisioning and de-provisioning user accounts, and password management. Some or all of these functions, such as password reset, are typically self-service to reduce the burden on IT staff.

The central directory is a repository off all user and group data for the enterprise. As such, a major role of this component is to synchronize the directory or repository across the enterprise, which can span on-premises and public or private cloud components. This enables a single view of the users and their permissions at anytime, anywhere in a hybrid cloud or multi-cloud infrastructure.

An IAM framework also includes two access components. Authentication addresses issues like sign-on (and single sign-on), managing active sessions, and providing strong authentication via token or biometric device. Authorization uses roles, attributes, and rules in a user record to determine whether a particular user, device, or application should be granted access to a resource.

Why do we need identity management?

A recent (ISC)² study found that 80% of breaches were due to identity access issues, namely weak or mismanaged credentials. If proper controls are not in place – or procedures and processes for IAM not properly followed, passwords could become compromised, phishing attacks enabled, and breaches or ransomware attacks become a reality. Fortunately, modern IAM platforms offer automation of many of the functions to help ensure controls are utilized, such as removing a user from the directory when the HR system indicated an employee has left the organization.

Since new privacy and data secrecy legislation is so frequently created, IAM can play another important role, that of helping the organization stay in compliance with the myriad of regulatory and governance mandates in effect, ensuringthat only authorized users have access to data, but that the data itself is where it should be. In the end, IT security is largely about access, so a solid IAM strategy is a critical component of overall IT security and offers a first line of protection to any threat, whether from outside or inside the firewall.

What are the business benefits of identity management?

The ability to successfully protect assets – including digital assets – can have a direct bottom-line impact on the value of the organization. IAM accelerates the time to value for anyone who needs access to enterprise resources to perform their job, often speeding the time between onboarding a new employee until when they have access to system resources from days to minutes.

Besides providing an enhanced business value as a result of improved security, there are other tangible business benefits. Automation of IAM tasks frees up IT for bottom-line focused projects, and self-service identity management tools improve the overall productivity of employees, contractors, and other users who access corporate resources.

Implementing an overall IAM framework can provide opportunities for growth, by improving scalability of those services critical to onboarding new users, and that reduction of IT manpower translates to a better ROI for the IT organization as a whole.

Identity and access management has become the foundation for all of these business benefits and continues to protect the enterprise from threats that could lead to data theft, malicious attacks, or exposing sensitive customer, patient, or legal information