CISSP 500

Identity and Access Management (IAM)

AL NAFI,
A company with a focus on education,
wellbeing and renewable energy.

Forty Hadith on the importance of Knowledge, learning and Teaching.

Hadith # 13 Allah's Path

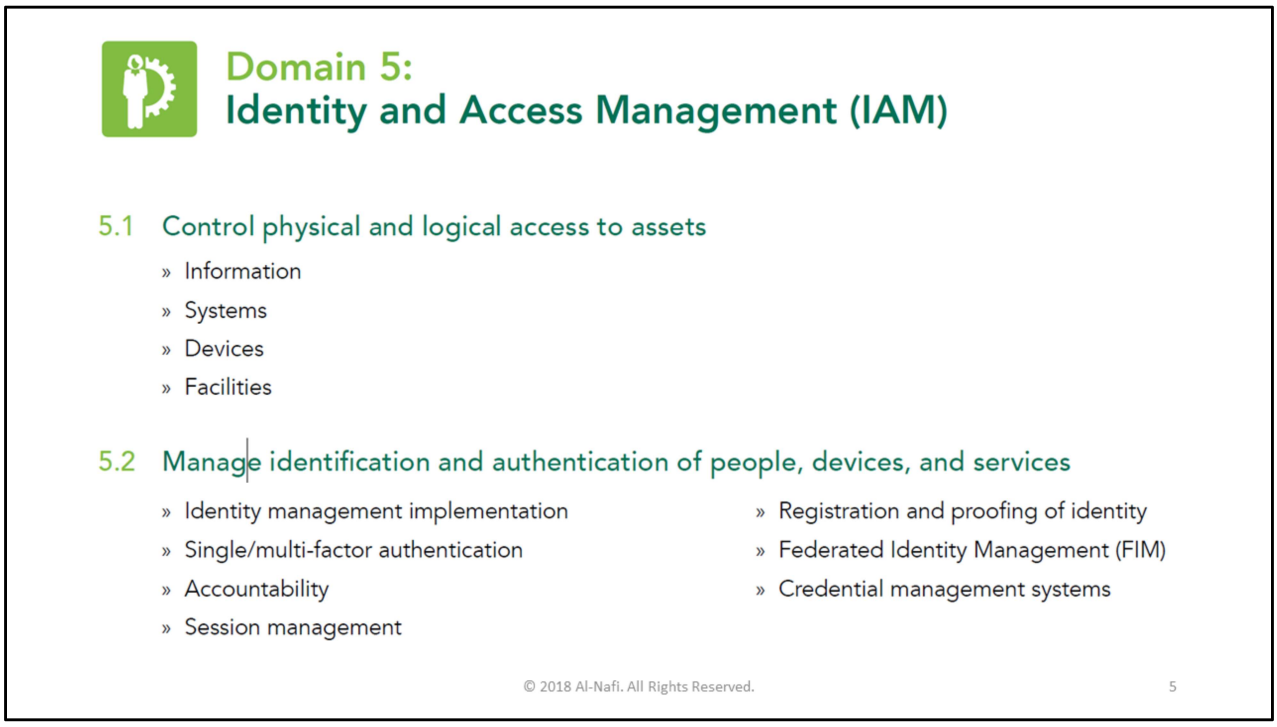
Anas (may Allah be pleased with him) said: The Messenger of Allah (Peace Be upon Him) Said:

"He who leave his home in order to seek knowledge, he is in Allah's path until he returns [to his home]."

(at-Tirmidhi, Sunan; An-Nawawi, Riyad as-Salihin)

How Nafi Members Study!

1. Please subscribe to our YouTube channel https://www.youtube.com/channel/UC2yAW4Oq27r1yuRE8ePKRvA
2. Follow us on Facebook https://www.facebook.com/info.alnafi/
3. Follow us on Twitter https://twitter.com/nafiPakistan
4. All Nafi members MUST study on the portal https://alnafi.com/login/ and connect using your Nafi member username and password. If you have problems connecting then please contact us via info@alnafi.com
5. To ask questions, Join the Al Nafi Official Group https://www.facebook.com/groups/alnafi/
6. Once on the portal they can follow their classes by:
    - watching videos
    - asking questions
    - attempting quizzes and flash cards
    - studying official Nafi notes
    - keep track of their studies long with many more features



Identity and access management (IAM) are core to maintaining confidentiality, integrity, and availability of assets and resources that are critical to business survival and function. Central to maintaining protection of business-critical assets is the ability to name, associate, and apply suitable identity and access control methodologies and technologies that meet specific business needs.

Domain 5:
Identity and Access Management (IAM)

5.3 Integrate identity as a third-party service

- On-premise
- Cloud
- Federated

5.4 Implement and manage authorization mechanisms

- Role Based Access Control (RBAC)
- Rule-based access control
- Mandatory Access Control (MAC)
- Discretionary Access Control (DAC)
- Attribute Based Access Control (ABAC)

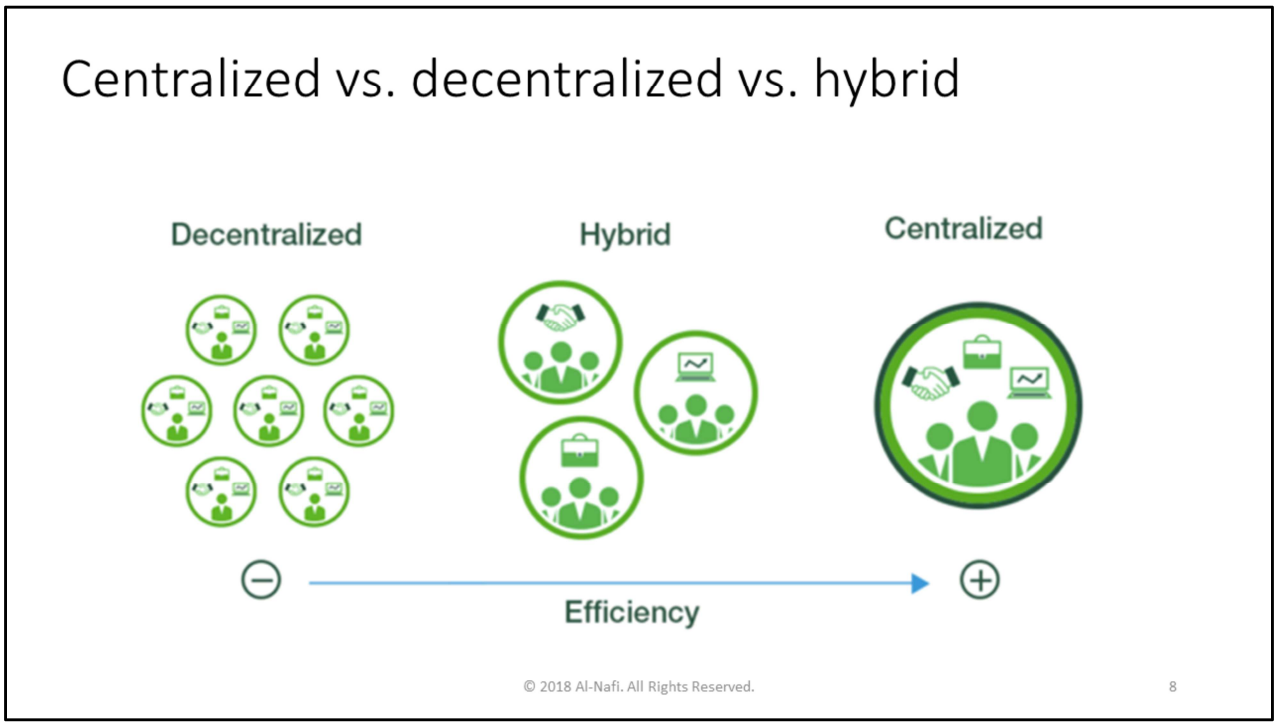
5.5 Manage the identity and access provisioning lifecycle

- User access review
- System account access review
- Provisioning and deprovisioning

Information

Information and the administration of information is key to the management of individual and systemic access control systems. Information can be associated with both logical and physical access control systems. Whether it is a logical or physical access system, the control of that system is maintained somewhere as discrete data and/or information. The management of information related to physical and logical access is accomplished in three primary ways, namely:

- centralized,
- decentralized,
- and hybrid.



Centralized–Centralized administration means that one element is responsible for configuring access controls so that users can access data and perform the activities they need to. As users' information processing needs change, their access can be modified only through central administration, usually after requests have been approved through an established procedure and by the appropriate authority. The main advantage of centralized administration is that very strict control over information can be maintained because the ability to make changes resides with very few persons. Each user's account can be centrally monitored, and closing all access for any user can be easily accomplished if that individual leaves the organization. Consistent and uniform procedures and criteria are usually not difficult to enforce, since relatively few individuals oversee the process.

Decentralized–In contrast to centralized administration, decentralized administration means that access to information is controlled by the owners or creators of the files, whoever or wherever those individuals may be. An advantage of decentralized administration is that control is in the hands of the individuals most accountable for the information, most familiar with it, and best able to judge who should be able to do what in relation to it. One disadvantage, however, is that there

may not be consistency among creators/owners as to procedures and criteria for granting user access and capabilities. Another disadvantage is that when requests are not processed centrally, it may be more difficult to form a system-wide view of all user access on the system at any given time. Different data owners may inadvertently implement combinations of access that introduce conflicts of interest or that are in some way not in the organization's best interest. It may also be difficult to ensure that access is properly terminated when an employee transfers within, or leaves an organization.

Hybrid–In a hybrid approach, centralized control is exercised for some information and decentralized is allowed for other information. One typical arrangement is that central administration is responsible for the broadest and most basic access, and the creators/owners of files control the types of access or users' abilities for the files under their control. For example, when a new employee is hired into a department, a central administrator might provide the employee with a set of access perhaps based on the functional element they are assigned to, job classification, and the specific task the employee was hired to work on. The employee might have read-only access to an organization-wide SharePoint document library and to project status report files, but read and write privileges to his department's weekly activities report. Also, if the employee left a project, the project manager can easily close that employee's access to that file.

Access Control and Administration

 9

Systems

Access controls can be classified by either logical or physical systems. The simplest example of a physical access control system is a door that can be locked, limiting people to one side of the door or the other. A logical access control system is normally operational in an office network where users are allowed or not allowed to login to a system to access data labeled with a classification by users granted a clearance.

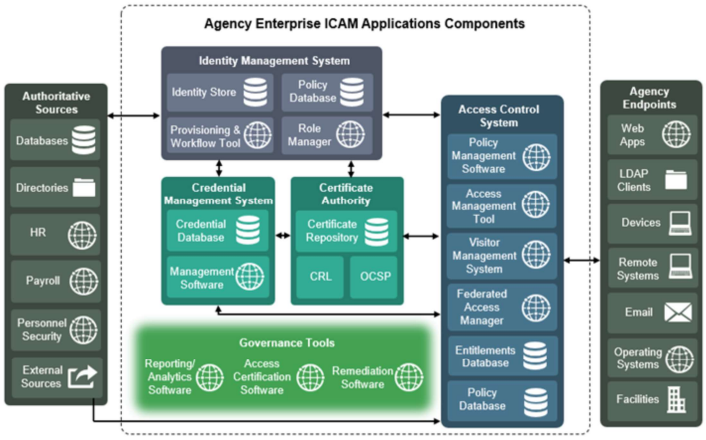
Access Controls and Administration

ISO/IEC 27000:2016(E) defines access control as a "means to ensure that access to assets is authorized and restricted based on business and security requirements." These requirements will be formalized in the organizational policy that is pertinent to individual organizations. Two primary system types that form access controls are physical and logical. Each type requires administration that can have various degrees of involvement from senior management regarding risk based decisions concerning the organizational risk appetite and profile, the data owner concerning "need-to-know" and "least privilege" and asset value determination, the custodian concerning tool implementation to provide appropriate restriction of the assets to

disclosure, destruction, or alteration.

Federal Identity, Credential, and Access Management (FICAM)

https://arch.idmanagement.gov/background/



The Federal Identity, Credential, and Access Management (FICAM) defines logical access control as: “An automated system that controls an individual’s ability to access one or more computer system resources such as a workstation, network, application, or database. A logical access control system requires validation of an individual’s identity through some mechanism such as a Personal Identification Number (PIN), card, biometric, or other token. It has the capability to assign different access privileges to meet different persons depending on their roles and responsibilities in an organization.”

Logical access control requires more complex and nuanced administration than physical. Before selection and implementation of the logical access control type, the data owner has classified and categorized the data. Categorizing the data will reveal the impact that would occur if there is disclosure, alteration, or destruction. Classifying the data will define the value of discreet assets and who should have access and authorization. Logical access controls are often built into the operating system, or may be part of the “logic” of applications programs or major utilities, such as database management systems (DBMS). They may also be implemented in add-on security packages that are installed into an operating system; such packages

are available for a variety of systems, including PCs and mainframes. Additionally, logical access controls may be present in specialized components that regulate communications between computers and networks.