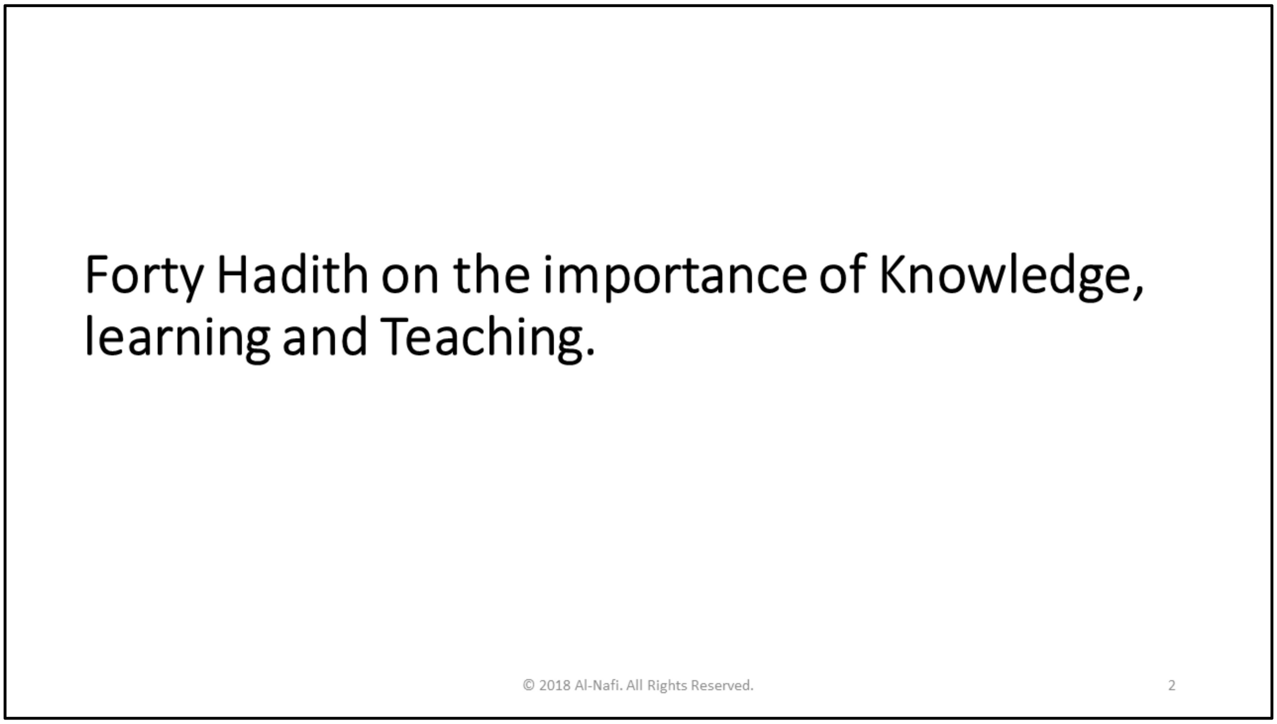
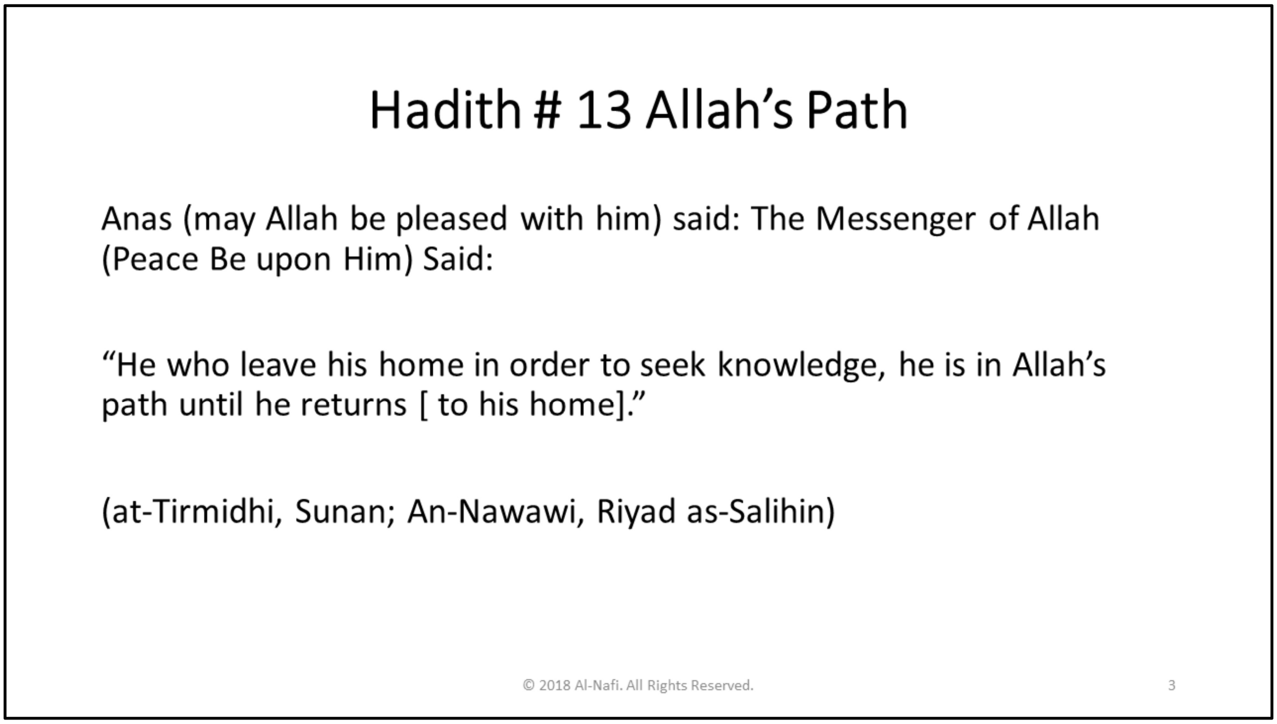
CISSP 700

Security Operations

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



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

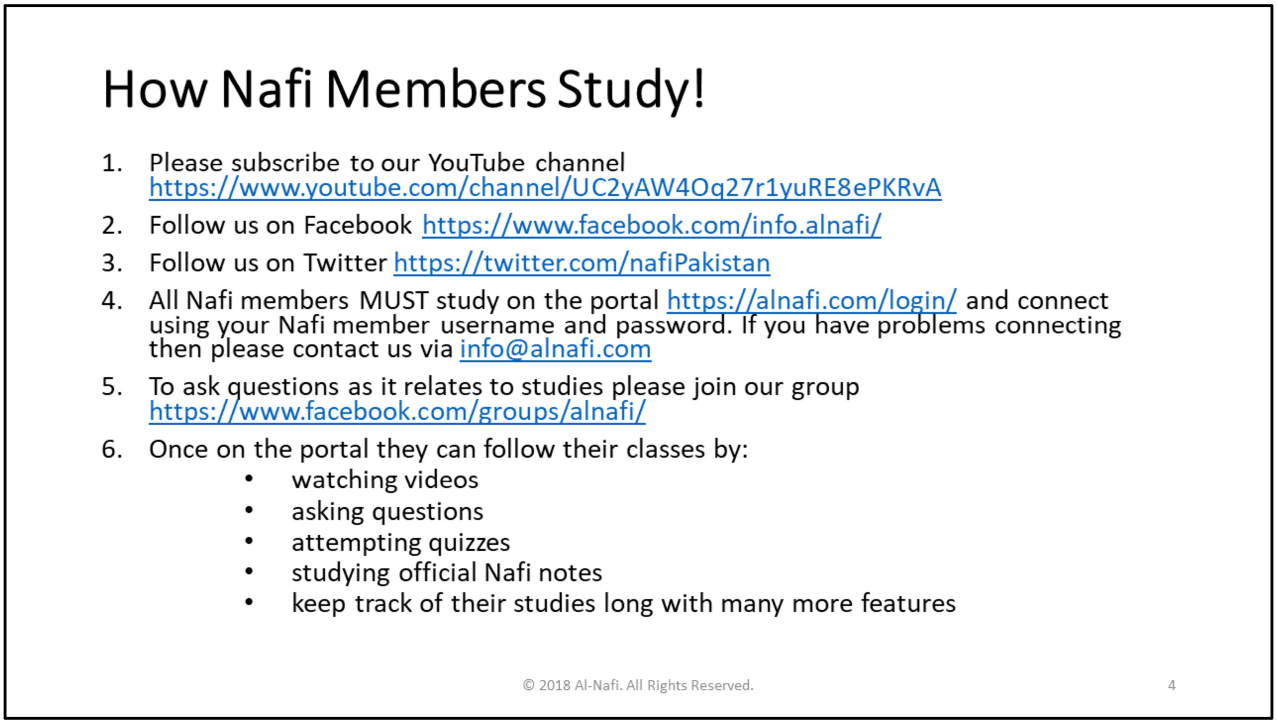


Hadith # 13 Allah’s Path

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

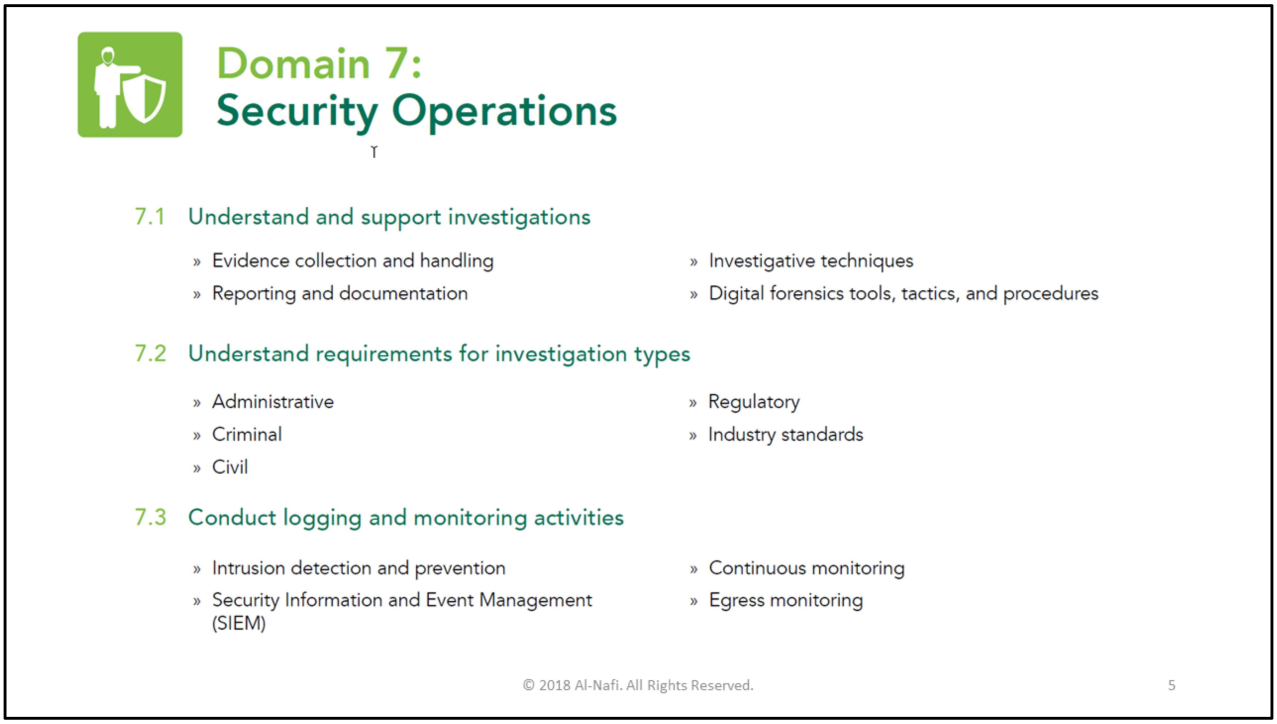
“He who leave his home in order to seek knowledge, he is in Allah’s path until he returns [to his home].”

(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 as it relates to studies please join our group https://www.facebook.com/groups/alnafi/
6. Once on the portal they can follow their classes by:
    - watching videos
    - asking questions
    - attempting quizzes
    - studying official Nafi notes
    - keep track of their studies long with many more features



Domain 7:
Security Operations

7.1 Understand and support investigations

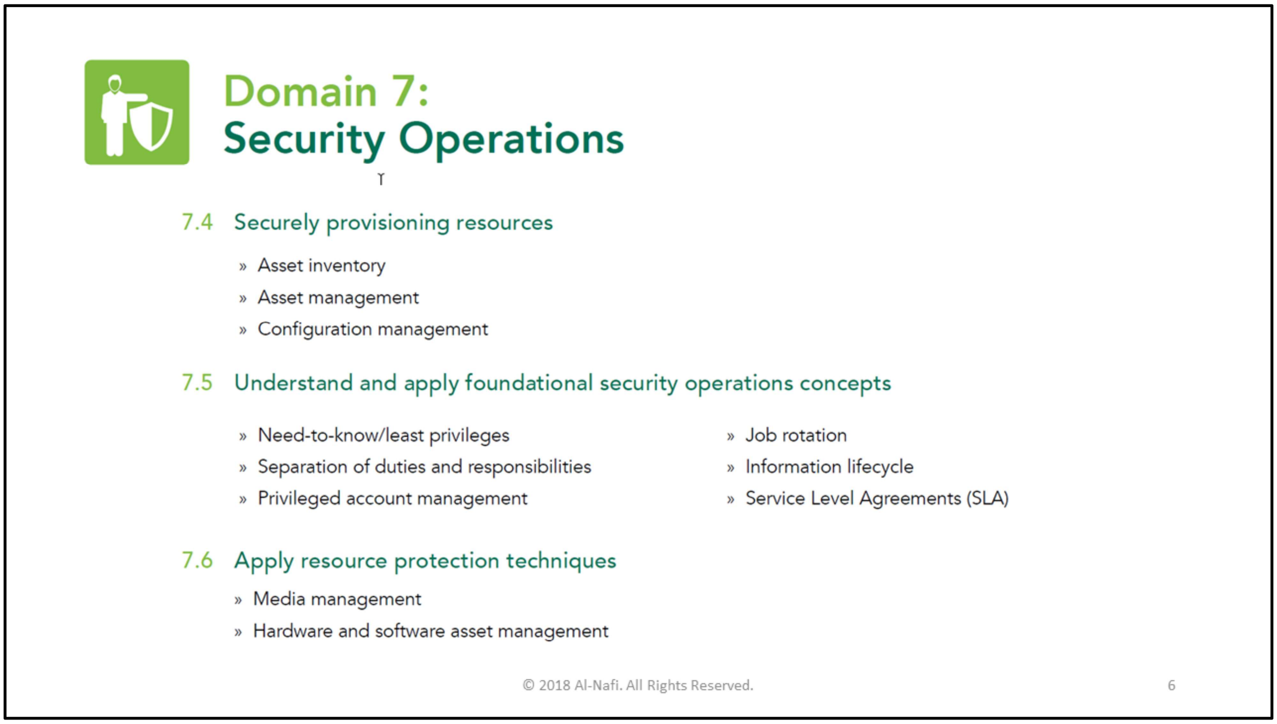
- Evidence collection and handling
- Reporting and documentation
- Investigative techniques
- Digital forensics tools, tactics, and procedures

7.2 Understand requirements for investigation types

- Administrative
- Criminal
- Civil
- Regulatory
- Industry standards

7.3 Conduct logging and monitoring activities

- Intrusion detection and prevention
- Security Information and Event Management (SIEM)
- Continuous monitoring
- Egress monitoring



Domain 7:
Security Operations

7.4 Securely provisioning resources

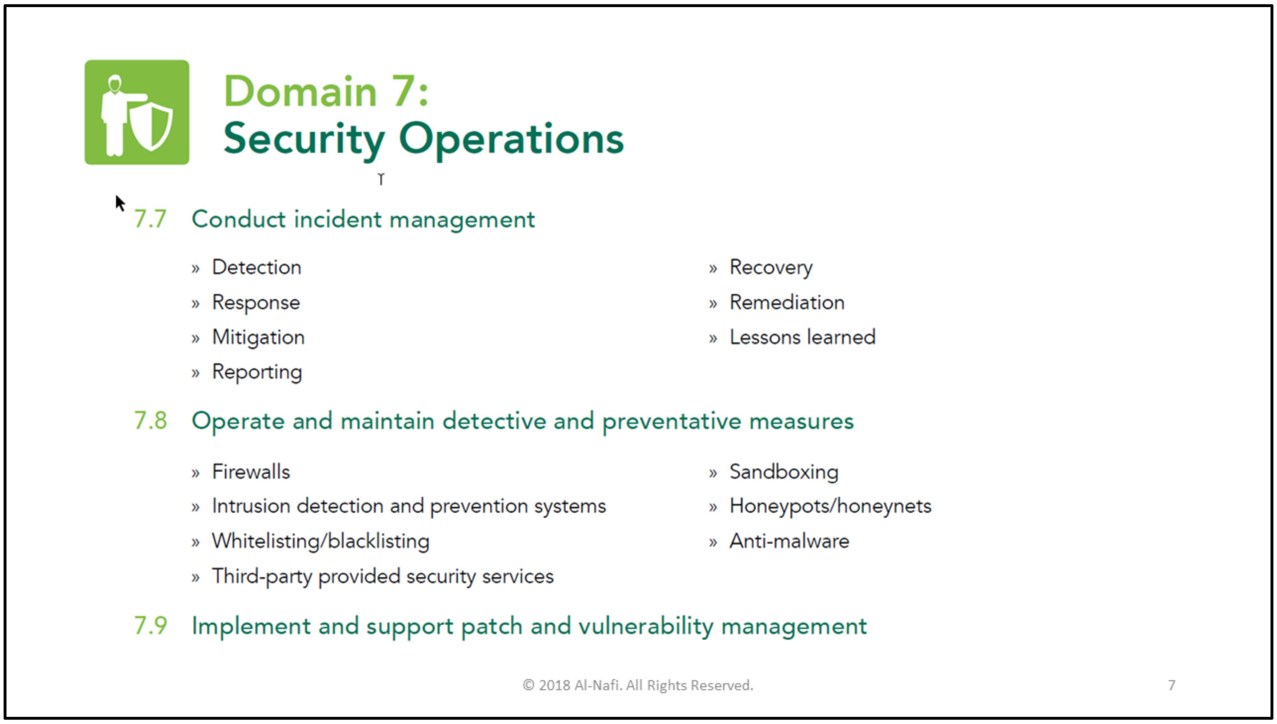
- Asset inventory
- Asset management
- Configuration management

7.5 Understand and apply foundational security operations concepts

- Need-to-know/least privileges
- Separation of duties and responsibilities
- Privileged account management
- Job rotation
- Information lifecycle
- Service Level Agreements (SLA)

7.6 Apply resource protection techniques

- Media management
- Hardware and software asset management



Domain 7: Security Operations

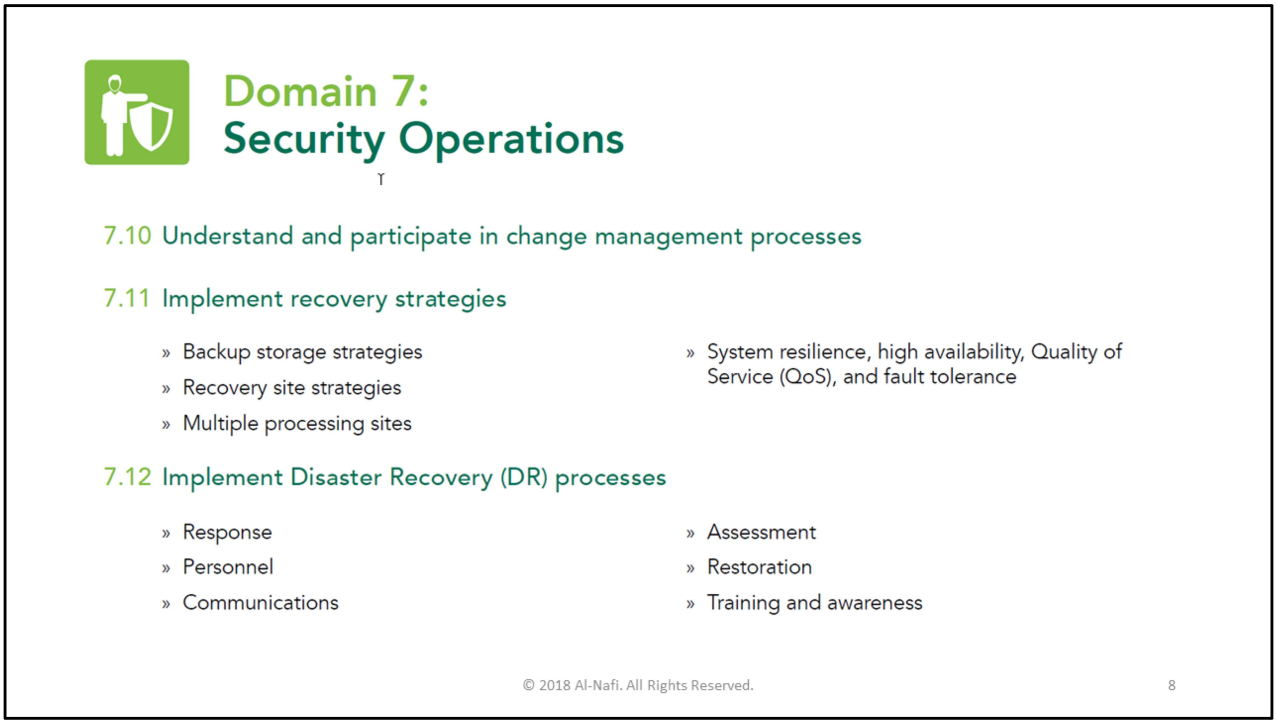
7.7 Conduct incident management

- Detection
- Response
- Mitigation
- Reporting
- Recovery
- Remediation
- Lessons learned

7.8 Operate and maintain detective and preventative measures

- Firewalls
- Intrusion detection and prevention systems
- Whitelisting/blacklisting
- Third-party provided security services
- Sandboxing
- Honeypots/honeynets
- Anti-malware

7.9 Implement and support patch and vulnerability management



Domain 7: Security Operations

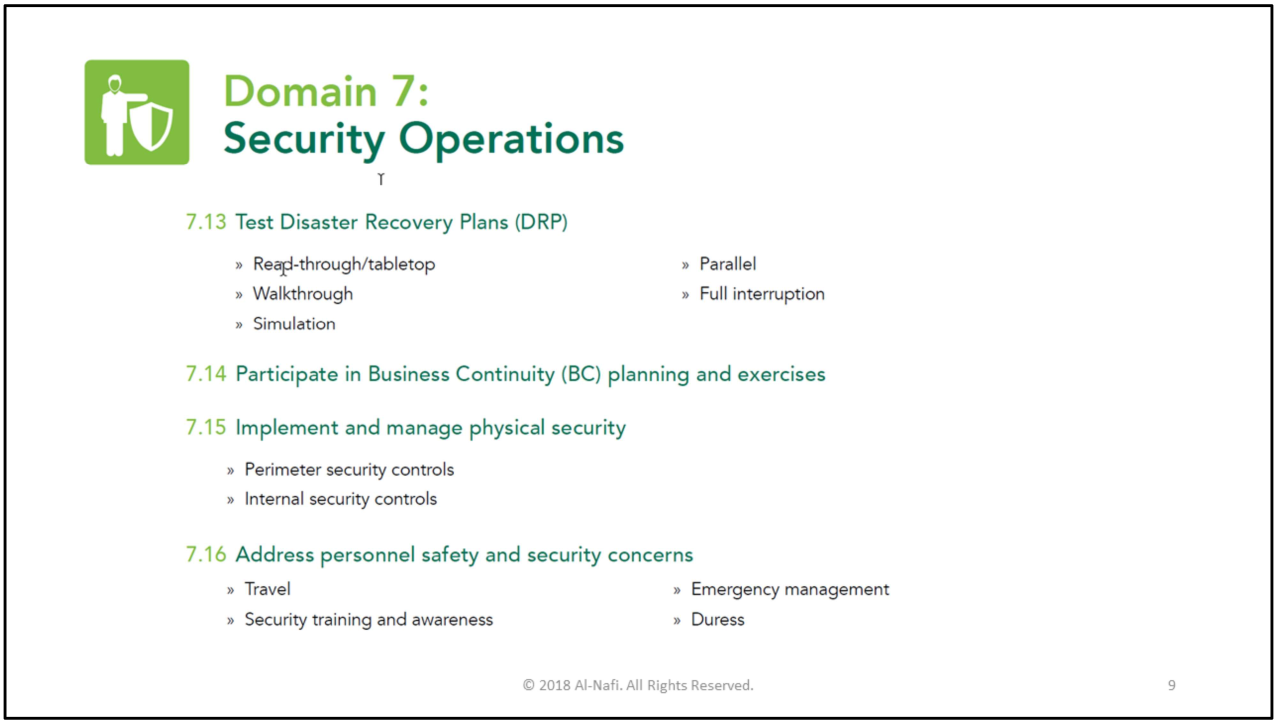
7.10 Understand and participate in change management processes

7.11 Implement recovery strategies

- Backup storage strategies
- Recovery site strategies
- Multiple processing sites
- System resilience, high availability, Quality of Service (QoS), and fault tolerance

7.12 Implement Disaster Recovery (DR) processes

- Response
- Personnel
- Communications
- Assessment
- Restoration
- Training and awareness



Domain 7: Security Operations

7.13 Test Disaster Recovery Plans (DRP)

- Read-through/tabletop
- Walkthrough
- Simulation
- Parallel
- Full interruption

7.14 Participate in Business Continuity (BC) planning and exercises

7.15 Implement and manage physical security

- Perimeter security controls
- Internal security controls

7.16 Address personnel safety and security concerns

- Travel
- Security training and awareness
- Emergency management
- Duress

Security Operations

Domain 7 deals with aspects of security the practitioner encounters while servicing the organization’s operational environment. The course material addresses foundational concepts, asset protection, incident management and response, business continuity and disaster recovery (BCDR), and personnel security.

Need-to-Know/Least Privilege

11

The principle of least privilege (POLP), an important concept in computer security, is the practice of limiting access rights for users to the bare minimum permissions they need to perform their work. Under POLP, users are granted permission to read, write or execute only the files or resources they need to do their jobs: In other words, the least amount of privilege necessary.

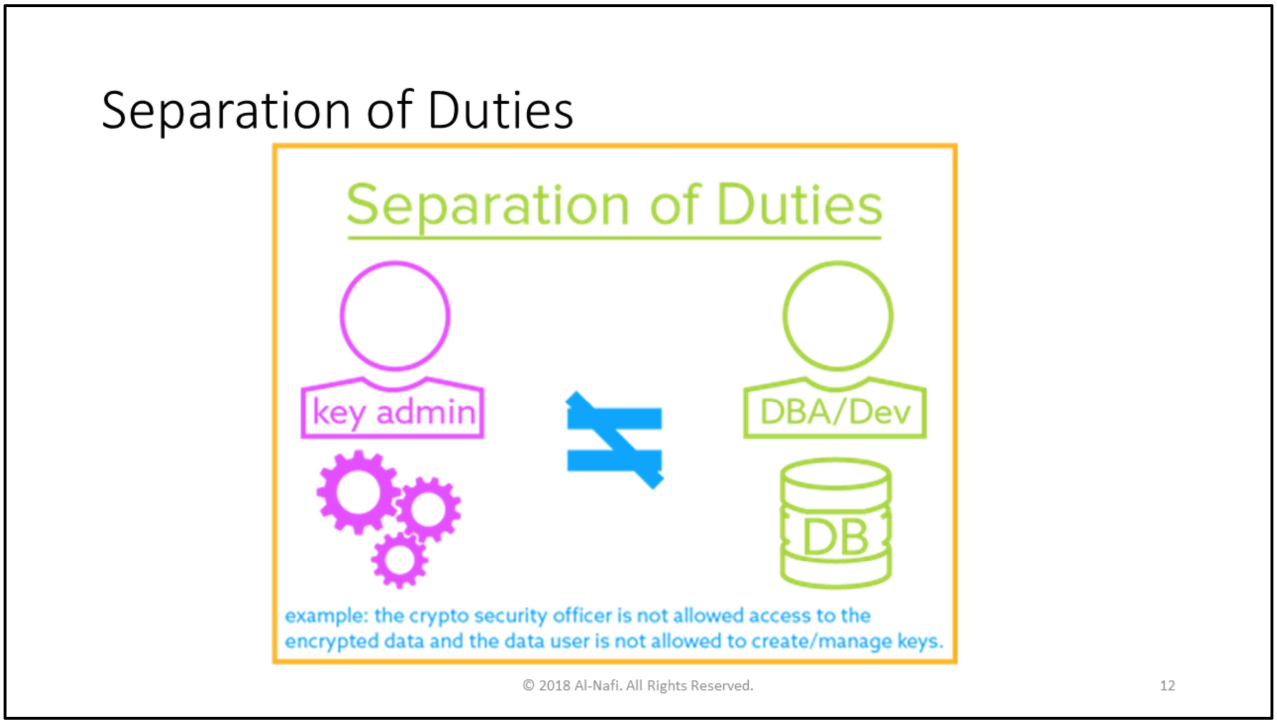
Additionally, the principle of least privilege can be applied to restricting access rights for applications, systems, processes and devices to only those permissions required to perform authorized activities.

Depending on the system, some privilege assignments may be based on attributes that are role-based, such as business units like marketing, human resources or IT, in addition to other parameters such as location, seniority, special circumstances or time of day. Depending on the operating system in use, administrators may need to tailor the different default privilege settings available for different types of user accounts.

Superuser accounts, mainly used for administration by IT staff members, have unlimited privileges over a system. The privileges granted to superuser accounts include full read, write and execute privileges as well as the ability to make changes across a network, e.g., installing or creating software or files, modifying settings and files, and deleting data and users.

Under current best practices for security, access through superuser accounts should be limited to only those required to administer systems; ideally, superuser credentials should never be used to log in to an account, but rather used with the "sudo" ("superuser do") command in Unix/Linux systems, which allows the holder of superuser credentials to issue a single command that is executed with superuser privileges. This reduces the risk of an active superuser session being hijacked.

Applying the principle of least privilege to standard user accounts means granting a limited set of privileges -- just enough privileges for users to get their jobs done, but no more than that. This type of account should be the template for ordinary employees -- least privileged users (LPUs) -- who do not need to manage or administer systems or network resources. These are the type of accounts that most users should be operating the majority of the time.



Separation of Duties

example: the crypto security officer is not allowed access to the encrypted data and the data user is not allowed to create/manage keys.

Separation of duties, also known as Segregation of duties, is the concept of having more than one person required to complete a task. It is a key concept of internal controls and is the most difficult and sometimes the costliest one to achieve. The idea is to spread the tasks and privileges for security tasks among multiple people. No one person should do everything.

Separation of duties is already well-known in financial accounting systems. Companies of all sizes understand not to combine roles such as receiving checks and approving write-offs, depositing cash and reconciling bank statements, approving time cards and have custody of pay checks, and so on. The concept of Separation of duties became more relevant to the IT organization when regulatory mandates such as Sarbanes-Oxley (SOX) and the Gramm-Leach-Bliley Act (GLBA) were enacted. A very high portion of SOX internal control issues, for example, come from or rely on IT. This forced IT organizations to place greater emphasis on Separation of duties across all IT functions, especially security.

What is Separation of Duties?

Separation of duties, as it relates to security, has two primary objectives. The first is the prevention of conflict of interest (real or apparent), wrongful acts, fraud, abuse and errors. The second is the detection of control failures that include security breaches, information theft and circumvention of security controls. Correct Separation of duties is designed to ensure that individuals don’t have conflicting responsibilities or are not responsible for reporting on themselves or their superior.

There is an easy test for Separation of duties.

Can any one person alter or destroy your financial data without being detected?

Can any one person steal or exfiltrate sensitive information?

Does any one person have influence over controls design, implementation and reporting of the effectiveness of the controls?

The answers to all these questions should be “no.” If the answer to any of them is “yes,” then you need to rethink the organization chart to align with proper Separation of duties. Also, the individual responsible for designing and implementing security must not be the same person that is responsible for testing security, conducting security audits or monitoring and reporting on security. Also, the person responsible for information security should not report to the CIO. The reason for this is that the CIO has a vested interest in having the rest of the C-Level staff believe that there are no cybersecurity issues. Anything that is discovered by the tester has the potential to be swept under the rug and not addresses as quickly as it should be. Best industry practice is that the person testing your cybersecurity should not be a member of your organization. They should be a disinterested third party.

Here are a few possible ways to accomplish proper Separation of duties:

Have the individual responsible for information security report to chairman of the audit committee.

Use a third party to monitor security, conduct surprise security audits and security testing.

Have an individual (CISO) responsible for information security report to the board of directors.

The importance of Separation of Duties for security

The issue of Separation of duties in security continues to be significant. It is imperative that there be separation between operations, development and testing of security and all controls to reduce the risk of unauthorized activity or access to operational systems or data. Responsibilities must be assigned to individuals in such a way as to mandate checks and balances within the system and minimize the opportunity for unauthorized access and fraud.

Remember, control techniques surrounding Separation of duties are subject to review by external auditors. Auditors have in the past listed this concern as a material deficiency on the audit report when they determine the risks are great enough. It is just a matter of time before this is done as it relates to IT security. For this reason, as well as objectivity, why not discuss separation of duties as it relates to IT security with your external auditors? It can save you a lot of aggravation, cost and political infighting by getting what they view as necessary in your case.

DNV GL has helped companies implement Separation of duties policies and procedures and has also performed audits to assure that procedures are being followed. Also, we have a team of cybersecurity professionals that can come into your organization to test your cybersecurity through vulnerability assessments and penetration testing. If you would like more information about the services we can offer you, please contact me.