INFORMATION SYSTEMS SECURITY AND CRYPTOGRAPHY

Lesson 02

By: Michael Maigwa M. Kangethe

DISCLAIMER

This document does not claim any originality and cannot be used as a substitute for prescribed textbooks. The information presented here is merely a collection by the Lecturer for his respective teaching assignments. Various sources as mentioned at the end of the document as well as freely available material from internet were consulted for preparing this document. The ownership of the information lies with the respective author(s) or institutions.

So Who is a Hacker?

- **Hacking**
  - refers to activities that seek to compromise digital devices, such as computers, smartphones, tablets, and even entire networks.
- **Hacker**
  - A person who breaks into a computer system.

By: Michael Maigwa M. Kangethe

Types of Hackers (Motivation)

- **Black hat**
  - Black hat hackers are cybercriminals that illegally crack systems with malicious intent.
- **White hat**
  - White hat hackers are ethical security hackers who identify and fix vulnerabilities.
- **Gray hat**
  - Gray hat hackers may not have the criminal or malicious intent of a black hat hacker, but they also don’t have the prior knowledge or consent of those whose systems they hack into.

By: Michael Maigwa M. Kangethe

Other types of hackers(Motivation)

- **Green hat hackers**
  - Green hat hackers are “green” in the sense that they’re inexperienced and may lack the technical skills of more experienced hackers. Green hats may rely on phishing and other social engineering techniques to bypass security systems.
- **Blue hat hackers**
  - Blue hat hackers are white hat hackers who are actually employed by an organization to help improve their security systems by conducting penetration tests.
- **Red hat hackers**
  - Also known as vigilante hackers, red hat hackers are motivated by a desire to fight back against black hat hackers, but they do this by infiltrating black hat communities on the dark web and launching hacking attacks against their networks and devices.

By: Michael Maigwa M. Kangethe

Other types of hackers(Motivation+Skill)

- **Script kiddies**
  - This term is often used by amateur hackers who do not care much about coding skills. These hackers usually download simple tools or codes written by other developers and hackers. Their primary goal is often the excitement, to impress friends or get attention.
- **Hacktivists**
  - The hacktivists have somewhat stronger and more defined motives for their actions – this is the online version of an activist. A hacktivist is a hacker or a group of anonymous hackers who think they can bring about social change. These often hack the government and organizations to gain attention or dissatisfaction with their thinking. The purpose of their attacks is often to gain publicity as a result of the attack.
- **Malicious Insider or whistleblower**
  - This could be a nagging employee or a rival-hired employee to gather opponents' trade secrets to stay on top of the game. These hackers can benefit from their easy access to information and their role in the company to hack the system.
- **State sponsored hackers**
  - These are employed by their state or nation authorities to 'sniff' around and penetrate security to obtain confidential information from other governments to stay on top online. These have infinitely large budgets and extremely advanced tools available.

By: Michael Maigwa M. Kangethe

IT security standards

IT security standards or cyber security standards are techniques generally outlined in published materials that attempt to protect the cyber environment of a user or organization.

This environment includes users themselves, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks.

The principal objective is to reduce the risks, including preventing or mitigating cyber-attacks. These published materials consist of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies.

By: Michael Maigwa M. Kangethe

International Standards

- **ISO/IEC 27001 and 27002 (International Organization for Standardization)**
  - ISO/IEC 27001 is the international standard for information security. It sets out the specification for an effective ISMS (information security management system). ISO 27001's best-practice approach helps organisations manage their information security by addressing people, processes and technology.
- **ISO/IEC 15408**
  - establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of ISO/IEC 15408 which in its entirety is meant to be used as the basis for evaluation of security properties of IT products.
  - This standard develops what is called the “Common Criteria.” It allows many different software and hardware products to be integrated and tested in a secure way.

By: Michael Maigwa M. Kangethe

International Standards

- **IEC 62443 (International Electrotechnical Commission)**
  - The IEC 62443 cybersecurity standard defines processes, techniques and requirements for Industrial Automation and Control Systems (IACS). Its documents are the result of the IEC standards creation process where all national committees involved agree upon a common standard.
- **ISO/SAE 21434 (Society of Automobile Engineers)**
  - This document specifies engineering requirements for cybersecurity risk management regarding concept, product development, production, operation, maintenance and decommissioning of electrical and electronic (E/E) systems in road vehicles, including their components and interfaces.

By: Michael Maigwa M. Kangethe

International Standards

- **ETSI EN 303 645(European Telecommunications Standards Institute)**
  - The ETSI EN 303 645 standard provides a set of baseline requirements for security in consumer Internet of things (IoT) devices. It contains technical controls and organizational policies for developers and manufacturers of Internet-connected consumer devices. The standard was released in June 2020 and is intended to be complemented by other, more specific standards. As many consumer IoT devices handle personally identifiable information (PII), implementing the standard helps with complying to the General Data Protection Regulation (GDPR) in the EU.

By: Michael Maigwa M. Kangethe

International Standards ETSI EN 303 645 cont…

The Cybersecurity provisions in this European standard are:

- No universal default passwords
- Implement a means to manage reports of vulnerabilities
- Keep software updated
- Securely store sensitive security parameters
- Communicate securely
- Minimize exposed attack surfaces
- Ensure software integrity
- Ensure that personal data is secure
- Make systems resilient to outages
- Examine system telemetry data
- Make it easy for users to delete user data
- Make installation and maintenance of devices easy
- Validate input data

By: Michael Maigwa M. Kangethe

National Standards

- **NERC (North American Electric Reliability Corporation)**
  - What does NERC do? NERC develops and enforces Reliability Standards; monitors the Bulk-Power System; assesses adequacy annually via a 10-year forecast and winter and summer forecasts; audits owners, operators and users for preparedness; and educates and trains industry personnel.
- **NIST (National Institute of Standards and Technology)**
  - NIST Cybersecurity Framework is a set of guidelines for mitigating organizational cybersecurity risks, published by the US National Institute of Standards and Technology (NIST) based on existing standards, guidelines, and practices. The framework "provides a high level taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes", in addition to guidance on the protection of privacy and civil liberties in a cybersecurity context.

By: Michael Maigwa M. Kangethe

National Standards

- **FIPS 140 (Federal Information Processing Standard)**
  - FIPS 140-2 is a NIST publication that lists security requirements for cryptographic modules protecting sensitive but unclassified information in computer and telecommunications systems. FIPS stands for "Federal Information Processing Standard," and 140-2 is the publication number for this particular FIPS.
  - FIPS dictate certain requirements for a range of cybersecurity matters, including computer encryption schemes, key generation methods, computer security, and interoperability (amongst other things), and stipulate which are acceptable
- **Cyber Essentials(National Institute of Standards and Technology)**
  - Cyber Essentials is a United Kingdom government information assurance scheme that is operated by the National Cyber Security Centre (NCSC). It encourages organizations to adopt good practice in information security. Cyber Essentials also includes an assurance framework and a simple set of security controls to protect information from threats coming from the internet.

By: Michael Maigwa M. Kangethe

National Standards

- **Essential Eight**
  - The Australian Cyber Security Centre has developed prioritised mitigation strategies, in the form of the Strategies to Mitigate Cyber Security Incidents, to help organisations protect themselves against various cyber threats. The most effective of these mitigation strategies are called the Essential Eight.
- **BSI IT-Grundschutz(Federal Office for Information Security - Germany)**
  - They contain recommendations on methods, processes and procedures as well as approaches and measures for various aspects of information security. Users from public authorities and companies as well as manufacturers or service providers can use the BSI standards to make their business processes and data more secure.

By: Michael Maigwa M. Kangethe

Industry-specific Standards

- **PCI DSS (Payment Card Industry Data Security Standard)**
  - The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes. The PCI Standard is mandated by the card brands but administered by the Payment Card Industry Security Standards Council. The standard was created to increase controls around cardholder data to reduce credit card fraud.
- **UL 2900 (Underwriters Laboratories)**
  - UL 2900 is a series of standards published by UL. The standards include general cybersecurity requirements (UL 2900-1) as well as specific requirements for medical products (UL 2900-2-1), industrial systems (UL 2900-2-2), and security and life safety signalling systems (UL 2900-2-3).

By: Michael Maigwa M. Kangethe

Access Control

- A security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimizes risk to the business or organization.
- There are two types of access control: physical and logical. Physical access control limits access to campuses, buildings, rooms and physical IT assets. Logical access control limits connections to computer networks, system files and data.
- The goal of access control is to minimize the security risk of unauthorized access to physical and logical systems. Access control is a fundamental component of security compliance programs that ensures security technology and access control policies are in place to protect confidential information, such as customer data.

By: Michael Maigwa M. Kangethe

How access control works

Access controls identify an individual or entity, verify the person or application is who or what it claims to be, and authorizes the access level and set of actions associated with the username or IP address. Directory services and protocols, including Lightweight Directory Access Protocol and Security Assertion Markup Language, provide access controls for authenticating and authorizing users and entities and enabling them to connect to computer resources, such as distributed applications and web servers.

By: Michael Maigwa M. Kangethe

Key features to look for in access control software:

- Event logs and export
- Capacity management
- Real-time analytics
- Lockdown
- SSO and SCIM
- Automated provisioning
- Remote and scheduled unlocks
- Video camera integration
- Intrusion detection and alerts
- Visitor management features
- In-and-out tracking
- 2FA on mobile credentials

By: Michael Maigwa M. Kangethe

Types Of Access Control

Mandatory access control (MAC)

- This is a security model in which access rights are regulated by a central authority based on multiple levels of security. Often used in government and military environments, classifications are assigned to system resources and the operating system or security kernel. MAC grants or denies access to resource objects based on the information security clearance of the user or device. For example, Security-Enhanced Linux is an implementation of MAC on Linux.
- There are two security models associated with MAC: Biba and Bell-LaPadula. The Biba model is focused on the integrity of information, whereas the Bell-LaPadula model is focused on the confidentiality of information. Biba is a setup where a user with lower clearance can read higher-level information (called “read up”) and a user with high-level clearance can write for lower levels of clearance (called “write down”). The Biba model is typically utilized in businesses where employees at lower levels can read higher-level information and executives can write to inform the lower-level employees.

By: Michael Maigwa M. Kangethe

Types Of Access Control cont…

Discretionary Access Control (DAC)

- This is an access control method in which owners or administrators of the protected system, data or resource set the policies defining who or what is authorized to access the resource. Many of these systems enable administrators to limit the propagation of access rights. A common criticism of DAC systems is a lack of centralized control.
- This gives DAC two major weaknesses. First, it gives the end-user complete control to set security level settings for other users which could result in users having higher privileges than they're supposed to. Secondly, and worse, the permissions that the end-user has are inherited into other programs they execute.

By: Michael Maigwa M. Kangethe

Types Of Access Control cont…

Role-Based Access Control (RBAC)

- This is a widely used access control mechanism that restricts access to computer resources based on individuals or groups with defined business functions --
- *e.g., So, instead of assigning John permissions as a security manager, the position of security manager already has permissions assigned to it. In essence, John would just need access to the security manager profile.* RBAC makes life easier for the system administrator of the organization.
- The big issue with this access control model is that if John requires access to other files, there has to be another way to do it since the roles are only associated with the position; otherwise, security managers from other organizations could get access to files they are unauthorized for.

By: Michael Maigwa M. Kangethe

Types Of Access Control cont…

Rule-Based Access Control (RBAC or RB-RBAC)

- This is a security model in which the system administrator defines the rules that govern access to resource objects. These rules are often based on conditions, such as time of day or location. It is not uncommon to use some form of both rule-based access control and RBAC to enforce access policies and procedures.
- The additional “rules” of Rule-Based Access Control requiring implementation may need to be “programmed” into the network by the custodian or system administrator in the form of code versus “checking the box.”

By: Michael Maigwa M. Kangethe

Types Of Access Control cont…

Attribute-Based Access Control (ABAC)

- This is a methodology that manages access rights by evaluating a set of rules, policies and relationships using the attributes of users, systems and environmental conditions.
- These attributes are associated with the subject, the object, the action and the environment. For example, a sales rep (subject) may try to access a client's record (object) in order to update the information (action) from his office during work hours (environment).
- This approach allows more fine-tuning of access controls compared to a role-based approach. For example, we could deny access based on the environment (e.g., time of day) or action (e.g., deleting records). The downside is that can be more difficult to get these controls up and running.

Types Of Access Control cont…

Risk-Based Access Control

- A dynamic access control model that determines access based on the level of evaluated risk involved in the transaction. One commonly-used example is identifying the risk profile of the user logging in. If the device being logged in from is not recognized, that could elevate the risk to prompt additional authentication. If an action deemed high-risk occurs, such as attempting to update banking information, that could trigger more risk-based prompts.
- One recent study found risk-based controls to be less annoying to users than some other forms of authentication. For example, two-factor authentication was “significantly more cumbersome to use and significantly more unnecessarily complex compared to [the tested risk-based authentication] conditions.”

Challenges of Access Control

- Dynamically managing distributed IT environments
- Compliance visibility through consistent reporting
- Password Fatigue
- Data governance and visibility through regular reporting
- Centralize user directories and avoid application specific cells

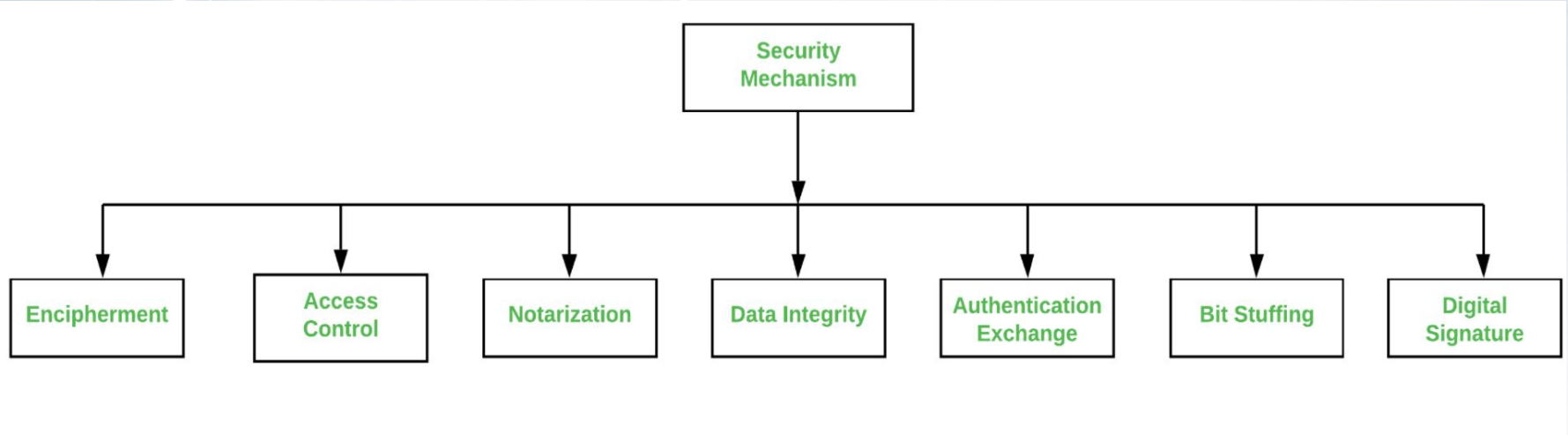
By: Michael Maigwa M. Kangethe

Security Mechanism

Security mechanisms are technical tools and techniques that are used to implement security services. A mechanism might operate by itself, or with others, to provide a particular service. Examples of common security mechanisms are as follows: Cryptography.

By: Michael Maigwa M. Kangethe

Types of Security Mechanism (Revisit)



By: Michael Maigwa M. Kangethe

Types of Security Mechanism cont…

- **Encipherment**
  - This security mechanism deals with hiding and covering of data which helps data to become confidential. It is achieved by applying mathematical calculations or algorithms which reconstruct information into not readable form. It is achieved by two famous techniques named Cryptography and Encipherment. Level of data encryption is dependent on the algorithm used for encipherment.
- **Access Control**
  - This mechanism is used to stop unattended access to data which you are sending. It can be achieved by various techniques such as applying passwords, using firewall, or just by adding PIN to data.
- **Notarization**
  - This security mechanism involves use of trusted third party in communication. It acts as mediator between sender and receiver so that if any chance of conflict is reduced. This mediator keeps record of requests made by sender to receiver for later denied.

By: Michael Maigwa M. Kangethe

Types of Security Mechanism cont…

- **Data Integrity**
  - This security mechanism is used by appending value to data to which is created by data itself. It is similar to sending packet of information known to both sending and receiving parties and checked before and after data is received. When this packet or data which is appended is checked and is the same while sending and receiving data integrity is maintained.
- **Authentication exchange**
  - This security mechanism deals with identity to be known in communication. This is achieved at the TCP/IP layer where two-way handshaking mechanism is used to ensure data is sent or not
- **Bit stuffing**
  - This security mechanism is used to add some extra bits into data which is being transmitted. It helps data to be checked at the receiving end and is achieved by Even parity or Odd Parity.

By: Michael Maigwa M. Kangethe

Types of Security Mechanism cont…

- **Digital Signature**
  - This security mechanism is achieved by adding digital data that is not visible to eyes. It is form of electronic signature which is added by sender which is checked by receiver electronically. This mechanism is used to preserve data which is not more confidential but sender's identity is to be notified.

Information Security Audit

A security audit is a systematic evaluation of the security of a company's information system by measuring how well it conforms to an established set of criteria. A thorough audit typically assesses the security of the system's physical configuration and environment, software, information handling processes and user practices.

There are several reasons to do a security audit. They include these six goals:

- Identify security problems and gaps, as well as system weaknesses.
- Establish a security baseline that future audits can be compared with.
- Comply with internal organization security policies.
- Comply with external regulatory requirements.
- Determine if security training is adequate.
- Identify unnecessary resources.

By: Michael Maigwa M. Kangethe

Types of Security Audits

- **Internal audits**
  - In these audits, a business uses its own resources and internal audit department. Internal audits are used when an organization wants to validate business systems for policy and procedure compliance.
- **External audits**
  - With these audits, an outside organization is brought in to conduct an audit. External audits are also conducted when an organization needs to confirm it is conforming to industry standards or government regulations.

By: Michael Maigwa M. Kangethe

What systems does an audit cover?

- **Network vulnerabilities**
  - Auditors look for weaknesses in any network component that an attacker could exploit to access systems or information or cause damage. Information as it travels between two points is particularly vulnerable. Security audits and regular network monitoring keep track of network traffic, including emails, instant messages, files and other communications. Network availability and access points are also included in this part of the audit.
- **Security controls**
  - With this part of the audit, the auditor looks at how effective a company's security controls are. That includes evaluating how well an organization has implemented the policies and procedures it has established to safeguard its information and systems. For example, an auditor may check to see if the company retains administrative control over its mobile devices. The auditor tests the company's controls to make sure they are effective and that the company is following its own policies and procedures.
- **Encryption.**
  - This part of the audit verifies that an organization has controls in place to manage data encryption processes.

By: Michael Maigwa M. Kangethe

What systems does an audit cover? cont…

- **Software systems**
  - Here, software systems are examined to ensure they are working properly and providing accurate information. They are also checked to ensure controls are in place to prevent unauthorized users from gaining access to private data. The areas examined include data processing, software development and computer systems.
- **Architecture management capabilities**
  - Auditors verify that IT management has organizational structures and procedures in place to create an efficient and controlled environment to process information.
- **Telecommunications controls**
  - Auditors check that telecommunications controls are working on both client and server sides, as well as on the network that connects them.

By: Michael Maigwa M. Kangethe

What systems does an audit cover? cont…

- **Systems development audit.**
  - Audits covering this area verify that any systems under development meet security objectives set by the organization. This part of the audit is also done to ensure that systems under development are following set standards.
- **Information processing.**
  - These audits verify that data processing security measures are in place.

By: Michael Maigwa M. Kangethe

Steps involved in a security audit

Agree on Goals	Define the Scope of the Audit	Conduct the audit and Identify threats	Evaluate security and risks	Determine the needed controls
Include all stakeholders in discussions of what should be achieved with the audit.	List all assets to be audited, including computer equipment, internal documentation and processed data.	List potential threats related to each Threats can include the loss of data, equipment or records through natural disasters, malware or unauthorized users.	Assess the risk of each of the identified threats happening, and how well the organization can defend against them.	Identify what security measures must be implemented or improved to minimize risks.

By: Michael Maigwa M. Kangethe

Generally, computer security audits are performed by:

- **Federal or State Regulators**
  - Information security audits would primarily be prepared by the partners of these regulators.
  - Examples include: Certified accountants, Cybersecurity and Infrastructure Security Agency (CISA), Federal Office of Thrift Supervision (OTS), Office of the Comptroller of the Currency (OCC), U.S. Department of Justice (DOJ), etc.
- **Corporate Internal Auditors**
  - If the information security audit is an internal audit, it may be performed by internal auditors employed by the organization.
  - Examples include: Certificated accountants, Cybersecurity and Infrastructure Security Agency (CISA), and Certified Internet Audit Professional (CIAP)
- **External Auditors**
  - Typically, third-party experts employed by an independent organization and specializing in the field of data security are hired when state or federal auditors are not accessible.
- **Consultants**
  - Outsourcing the technology auditing where the organization lacks the specialized skill set.

By: Michael Maigwa M. Kangethe

Test vs. assessment vs. audit (Please Note)

An audit is a way to validate that an organization is adhering to procedures and security policies set internally, as well as those that standards groups and regulatory agencies set. Organizations can conduct audits themselves or bring in third parties to do them. Security audit best practices are available from various industry organizations.

A test, such as a penetration test, is a procedure to check that a specific system is working as it should. IT professionals doing the testing are looking for gaps that might open vulnerabilities. With a pen test, for instance, the security analyst is hacking into the system in the same way that a threat actor might, to determine what an attacker can see and access.

By: Michael Maigwa M. Kangethe

Jobs in information security

- **Information Security Officer (ISO)**
  - Information Security Officer (ISO) is a relatively new position, which has emerged in organizations to deal in the aftermath of chaotic growth in information technology and network communication. The role of the ISO has been very nebulous since the problem that they were created to address was not defined clearly. The role of an ISO has become one of following the dynamics of the security environment and keeping the risk posture balanced for the organization.

By: Michael Maigwa M. Kangethe

Certifications in information security

- Certified Information Systems Manager (CISM)
- Certified in Risk and Information Systems Control (CRISC)
- Certified in the Governance of Enterprise IT (CGEIT)
- Certified Information System Auditor (CISA)
- CSX (Cybersecurity Nexus Fundamentals)
- CSXP (Cybersecurity Nexus Practitioner)

By: Michael Maigwa M. Kangethe

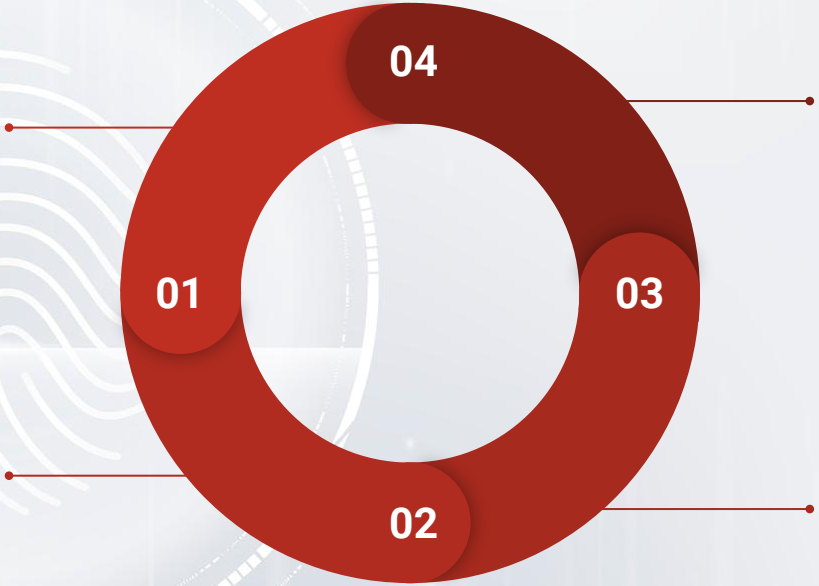
Test vs. assessment vs. audit (Please Note) Cont…

An assessment is a planned test such as a risk or vulnerability assessment. It looks at how a system should operate and then compares that to the system's current operational state. For example, a vulnerability assessment of a computer system checks the status of the security measures protecting that system and whether they are responding the way they should.

Security audits are one part of an overall strategy for protecting IT systems and data.

By: Michael Maigwa M. Kangethe

The Information Security Lifecycle



Identify

Know what it is you are trying to protect. Define the scope of the assessment. From Hardware to all associated software and data

Assess

This step covers all aspects of assessment, from reviewing your current processes and procedures to actually performing vulnerability scans.

Monitor

Monitor the security you have in place and the security you've recently changed and updated. Once, in your mind, you've strengthened your security posture as a whole it's important to ensure it remains that way. In addition to monitoring changes you've made it's important to monitor new systems that are introduced into the ecosystem of your company's network.

Protect

This step of the information security lifecycle is sometimes referred to as the "mitigation" step, since the actual objective of the step is to mitigate all of the risks identified during the assessment period.

By: Michael Maigwa M. Kangethe

References

- https://www.isms.online/iso-27000/#:~:text=What%20is%20the%20ISO%2027000%20series%20of%20standards%3F,Standardisation%20and%20International%20Electrotechnical%20Commission.
- https://en.wikipedia.org/wiki/IT_security_standards
- https://www.avast.com/c-hacker-types#:~:text=Hackers%20fall%20into%20three%20general,hacking%20is%20malicious%20or%20illegal.
- https://www.techtarget.com/searchsecurity/definition/access-control#:~:text=There%20are%20two%20types%20of,networks%2C%20system%20files%20and%20data.
- https://resources.infosecinstitute.com/certification/access-control-models-and-methods/
- https://www.getkisi.com/blog/top-10-best-access-control-software
- https://masomomsingi.co.ke/bit3102-bbit301-bct2106-information-systems-security-and-cryptography-network-security-information-security-policy/
- https://www.techtarget.com/searchcio/definition/security-audit
- https://en.wikipedia.org/wiki/Information_security_audit
- https://plextrac.com/the-information-security-lifecycle/#:~:text=Identify%2C%20Assess%2C%20Protect%2C%20and%20Monitor

By: Michael Maigwa M. Kangethe