# CHAPTER 5: ICT SECURITY THREATS

## 5.1 Introduction

This unit covers the competencies required to provide ICT security. They include identification of security threats, installation of security control measures, implementation of security measures, testing of system vulnerability and monitoring of the security system.

## 5.1 Performance Standard

- Identified and classified security threats
- Identified and categorized security control measures
- Implemented ICT security policy
- Developed a schedule system testing plan

## 5.3 Learning Outcome

### 5.3.1 List of the Learning Outcomes

These are the key learning outcomes, which make up workplace function:

- Identify security threats
- Establish and Install security measures
- Deploy security measures
- Test system vulnerability
- Monitor security system



### 5.3.2 Learning Outcome 1: Identify security threats

#### 5.3.2.1 Learning Activities

The following are the performance criteria:

- Security threats are identified based on the vulnerability of the system.
- Security threats are categorized according to the risk impact
- Appropriate security measures are selected as per the security threats

Trainees to demonstrate knowledge in relation to:

- Definition of security threats
- Categories of security threats: Internal and External
- Importance of Computer Security to an Organization
- Identification of Common threats: Fraud and theft, Employee sabotage, Loss of physical and infrastructure support, Malicious hackers and code, Industrial espionage, Threats to personal privacy, Natural Calamities, Cyber crime
- Constraints to computer security: Cost, User responsibility, Integration challenges, Inadequate Assessment

### 5.3.2.2 Information Sheet

**A threat,** in the context of **computer security,** refers to anything that has the potential to cause serious harm to a computer system. A threat is something that may or may not happen, but has the potential to cause serious damage. Threats can lead to attacks on computer systems, networks and more.

An **internal threat** originating inside a company, government agency, or institution, and typically an exploit by a disgruntled employee denied promotion or informed of employment termination. An attacker who has sought temporary employment with a target and uses social engineering skills to get on the inside also can launch such exploits.

**External threat,** originate outside a company, government agency, or institution. In contrast, an internal threat is one originating inside the organization typically by an employee or "insider."

**Importance of computer security to an organization:**
**To protect company's assets:** This can be considered as the primary goal of securing the computers and computer networks. The assets mean the information that is stored in the computer networks, which are as crucial and valuable as the tangible assets of the company. The computer and network security is concerned with the integrity, protection and safe access of the confidential information. It also involves the accessibility of information in a meaningful manner.



**To comply with regulatory requirements and ethical responsibilities:** It is the responsibility of every organization to develop procedures and policies addressing the security requirements of every organization. These policies work for the safety and security of any organization and are compulsory for any organization working on computers. Protection of company's assets would mean that it is protected from liability addressing to the ethical responsibilities of an organization.

**For competitive advantage:** Developing an effective security system for networks will give the organization a competitive edge. In the arena of Internet financial services and e-commerce, network security assumes prime importance. The customers would avail the services of Internet banking only if the networks are secured.

**Fraud and theft** have a lot in common. Both are criminal acts, and both are forcibly taking something from others without asking permission. Both are all about stealing and both are bad things.

**Read:** Difference between fraud and theft:
http://www.differencebetween.net/miscellaneous/difference-between-fraud-and-theft/#ixzz5qRVXtQ00

**Identification of common threats:** It is important to identify and appropriately manage common threats to an organization.

- **Employee sabotage:** Employees are most familiar with their employer's computers and applications, this include knowing what actions might cause the most damage, mischief, or sabotage.
- **The loss of supporting infrastructure** includes power failures (outages, spikes, and brownouts), loss of communications, water outages and leaks, sewer problems, lack of transportation services, fire, flood, civil unrest, and strikes.
- **The term malicious hackers,** sometimes called crackers, refer to those who break into computers without authorization. They can include both outsiders and insiders. Much of the rise of hacker activity is often attributed to increases in connectivity in both government and industry.
- **Malicious code** refers to viruses, worms, Trojan horses, logic bombs, and other "uninvited" software. Sometimes mistakenly associated only with personal computers, malicious code can attack other platforms.
- **Industrial espionage** is the act of gathering proprietary data from private companies or the government for the purpose of aiding another company(ies). Industrial espionage can be perpetrated either by companies seeking to improve their competitive advantage or by governments seeking to aid their domestic industries.



**Threats to personal privacy**

- The accumulation of vast amounts of electronic information about individuals by governments, credit bureaus, and private companies, combined with the ability of computers to monitor, process, and aggregate large amounts of information about individuals have created a threat to individual privacy.
- **Natural calamities**, such as earthquakes, floods and hurricanes, can damage computer. Fires, extreme temperatures and lightning strikes can cause major physical damage and lead to loss of data.

**Cybercrime,** or computer-oriented crime, is a crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target.

**User responsibility**

- Use computer and information systems in an ethical and legal manner.
- Agree not to duplicate or use copyrighted or proprietary software without proper authorization.

**The challenge of integration** between physical and cyber security creates a number of challenges. First, no single system exists to confirm a person's identity because each functional security department controls its own identity database. Second, the lack of integration increases the potential for theft.

**Case studies - Cyber Crime around the world**

**Wanna Cry virus hits the NHS, 2017**

The most widespread cyber attack ever, hackers managed to gain access to the NHS' computer system in mid-2017, causes chaos among the UK's medical system. The same hacking tools were used to attack worldwide freight company FedEx and infected computers in 150 countries. Ransomware affectionately named "WannaCry" was delivered via email in the form of an attachment. Once a user clicked on the attachment, the virus was spread through their computer, locking up all of their files and demanding money before they could be accessed again. As many as 300,000 computers were infected with the virus.

It was only stopped when a 22-year-old security researcher from Devon managed to find the kill switch, after the NHS had been down for a number of days.

**JP and Morgan Chase & Co target of giant hacking conglomerate, 2015**

Late in 2015, three men were charged with stealing data from millions of people around the world, as part of a hacking conglomerate that spanned the best part of a decade. The group stole information from more than 83 million customers from JP Morgan alone, and are thought to have made hundred of millions of dollars in illegal profits. Along with personal data, the hacking group also stole information related to company performance and news, which allowed them to manipulate stock prices and make enormous financial gain.



**Sony Pictures crippled by GOP hackers, 2014**

In late 2014, major entertainment company Sony Pictures were hit with a crippling virus. Cyber crime group Guardians of Peace (GOP) were behind the apparent blackmail attempt, which saw around 100 terabytes of sensitive data stolen from the company.

**One billion user accounts stolen from Yahoo, 2013**

In one of the largest cases of data theft in history, Yahoo had information from more than one billion user accounts stolen in 2013. Personal information including names, phone numbers, passwords and email addresses were taken from the Internet giant.


Source: https://www.nation.co.ke

**Figure 61: Cyber crime in Kenya**



### 5.3.2.3 Self-Assessment

i. What is the difference between fraud and theft?
ii. Differentiate internal and external threads?
iii. What is hacking?
iv. What is malicious?
v. Differentiate hacking and cybercrime?
vi. **Case situation:** One of your friend's social media accounts has been hacked. What will you do to help him?
viii. Review various risks associated with computer security and make a detail report on how to address them.
ix. What are the training contents you will consider for helping community understand the security treats related to cyber security?
x. **Case situation:** You at working as a consultant to the Financial Auditing firm. They want you to evaluate their employee contract and ensure that there are strict rules against cyber crime. What will be your suggestions? They also want you to improvise their security. They are a financial audit firm and they need to ensure security of all their client data.
xi. Which of the following are forms of malicious attack?
   A. Theft of information
   B. Modification of data
   C. Wiping of information
   D. All of the mentioned

E.

xii. What are common security threats?
   A. File Shredding
   B. File sharing and permission
   C. File corrupting
   D. File integrity

xiii. What is not a good practice for user administration ?
   A. Isolating a system after a compromise
   B. Perform random auditing procedures
   C. Granting privileges on a per host basis
   D. Using telnet and FTP for remote access.

xiv. Why would a hacker use a proxy server?
   A. To create a stronger connection with the target.
   B. To create a ghost server on the network.
   C. To obtain a remote access connection.
   D. To hide malicious activity on the network.

xvi. Conduct secondary analysis and share in group discussion regarding challenges of data hacking on social media site.

**5.3.2.4 Tools, Equipment, Supplies and Materials**

Hardware security, Data encryption, Cybersecurity education, LastPass Enterprise, Password



**5.3.2.5 References**


- https://www.avalan.com/blog/bid/385189/Importance-Of-Network-Security-For-Business-Organization
- https://www.yourdictionary.com/external-threat
- https://www.coursehero.com/file/11659891/Employee-sabotage/
- http://www.differencebetween.net/miscellaneous/difference-between-fraud-and-theft/#ixzz5qRVXtQ00
- Cyber Security, authored by John G. Voeller published by Wiley, 2014

### 5.3.3 Learning Outcome 2: Establish and install security measures

#### 5.3.3.1 Learning Activities

The following are the performance criteria:

- ICT Security policy is implemented as per the Kenya Security Act 2018
- Security control measures are identified and categorized as per the laws governing security in ICT.
- Evaluation of Security control measures is done as per the ICT Security policy
- Installation of Security control measures is done as per the ICT Security policy

Trainees to demonstrate knowledge in relation to:

- Definition of security risk management
- Benefits of Risk management
- Risk management procedures: Risk assessment, Risk mitigation Uncertainty analysis, Interdependencies, Cost considerations
- Benefits of security measures
- Types of Security measures: Firewalls, User accounts control, Security policies, Antivirus, Encryption, Secure Socket Layer protocol (SSL), Multi-factor authentication, Malware detection, Site monitoring, Daily or weekly backups
- Application of security measures



#### 5.3.3.2 Information Sheet

Risk is the possibility of something adverse happening. **Risk management** is the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk. Though perhaps not always aware of it, individuals manage risks every day. Actions as routine as buckling a car safety belt, carrying an umbrella when rain is forecast, or writing down a list of things to do rather than trusting to memory fall into the purview of risk management. People recognize various threats to their best interests and take precautions to guard against them or to minimize their effects.

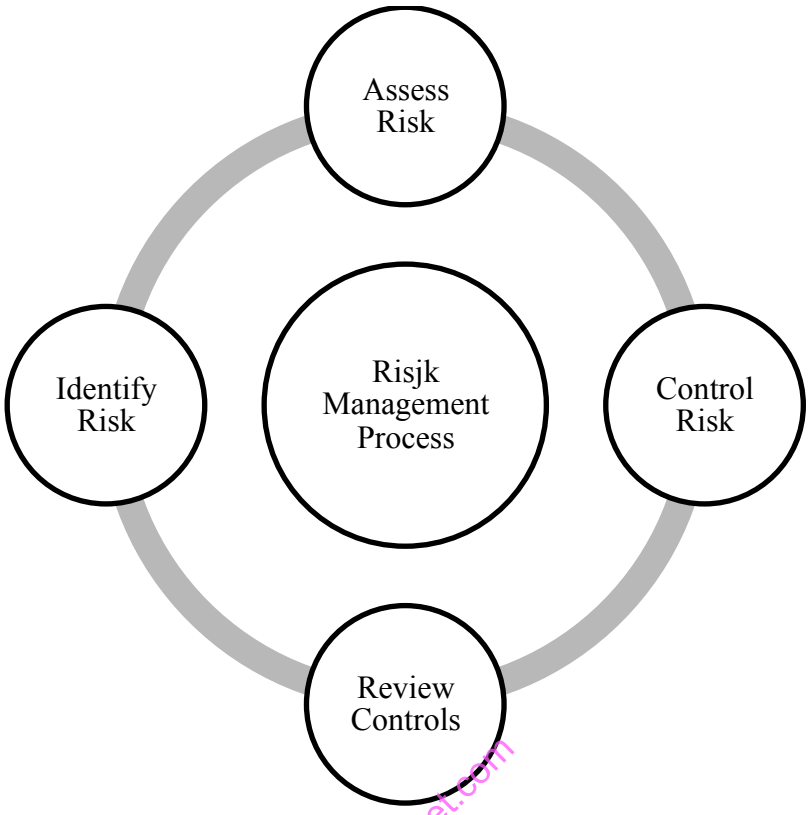
**Risk assessment often produces an important side benefit** in depth knowledge about system and an organization as risk analyst tries to figure out how system and functions are interrelated. **Risk assessment,** the process of analyzing and interpreting risk, is comprised of three basic activities:

- Determining the assessment's scope and methodology;
- Collecting and analyzing data; and
- Interpreting the risk analysis results

**Read:** Introduction to computer security:
http://www.davidsalomon.name/CompSec/auxiliary/handbook.pdf

**Risk mitigation** involves the selection and implementation of security controls to reduce risk

to a level acceptable to management, within applicable constraints.




Source: www.123rf.com

**Figure 62: Risk Management Process**

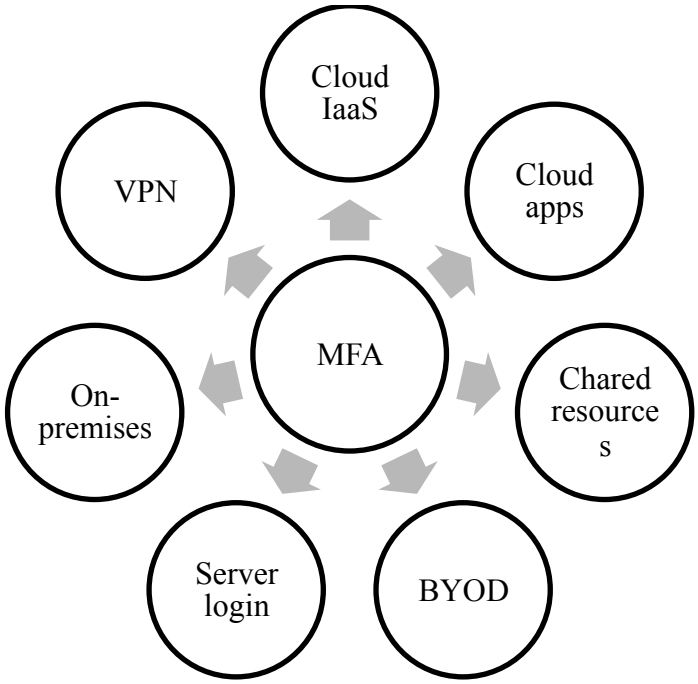


**Interdependencies:** Risk management touches on every control it is, however, most closely related to life cycle management and the security planning process. The requirement to perform risk management is often discussed in organizational policy and is an issue for organizational oversight.

The cost of different methodologies can be significant. A "back-of-the-envelope" analysis or high-medium-low ranking can often provide all the information needed. However, especially for the selection of expensive safeguards or the analysis of systems with unknown consequences, more in-depth analysis may be warranted.

**Secure Sockets Layer (SSL)** is a standard protocol used for the secure transmission of documents over a network. Developed by Netscape, SSL technology creates a secure link between a Web server and browser to ensure private and integral data transmission. SSL uses Transport Control Protocol (TCP) for communication.

**Multi-factor authentication** is an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence to an authentication mechanism: knowledge, possession, and inherence. Two-factor authentication is a type, or subset, of multi-factor authentication.




Source: www.centrify.com

**Figure 63: Multi-factor authentication (MFA)**

**Watch:** Introduction to multi-factor authentication: https://youtu.be/tFv101qURKE



**Malware detection** focuses on detecting intrusions by monitoring the activity of systems and classifying it as normal or anomalous.

**Malware Infection Symptoms**

- Strange emails
- Files wont open
- Programs acting weird
- Pop-up

Source: thelatesttechnews.com

**Figure 64: Malware infection symptoms**

**Watch:** Prevention and detection of malware: https://youtu.be/Ces7UeMQ7ic

**Site monitoring** is the process of testing and verifying that end-users can interact with a website or web application as expected. Website monitoring is often used by businesses to ensure website uptime, performance, and functionality is as expected.

Some common **backup frequencies** you'll see offered include continuous, once per minute, every x minutes (e.g. every 15 minutes), hourly, daily, weekly, monthly, and manually. Continuous backup means that the software is constantly backing up data.

**Application security** encompasses measures taken to improve the security of an application often by finding, fixing and preventing security vulnerabilities.

**Watch:** Introduction to site monitoring: https://youtu.be/Ufw6iuwm1rU

### 5.3.3.3 Self-Assessment

i. What is meant by risk assessment of an organization's ICT department?

ii. What is SSL?

A. Source socket layer
B. Secure socket lay
C. Socket secure layer
D. Secure socket layer

iii. What is Multi-factor authentication?

iv. What is site monitoring?

v. Evaluation of security control measures is done as per the ICT Security policy in the lab

vi. Installation of Security control measures is done as per the ICT Security policy in the lab.

vii. **Case situation:** How can you help an organization to set multi-factor authentication when making any changes on their system administration settings?

viii. _____ is an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence to support credibility.

A. Multi-factor authentication
B. Cost
C. Monitoring



### 5.3.3.4 Tools, Equipment, Supplies and Materials

Computer, anti-virus, maintenance tools, anti-spyware, password management software, Internet

### 5.3.3.5 References


- http://www.davidsalomon.name/CompSec/auxiliary/handbook.pdf
- https://www.keycdn.com/blog/website-monitoring-tools
- Cyber Security, authored by John G. Voeller published by Wiley 2014

### 5.3.4 Learning Outcome 3: Deploy security measures

#### 5.3.4.1 Learning Activities

The following are the performance criteria:

- Physical control measures are implemented according to the ICT security policy
- Logical security control measures are implemented according to the ICT security policy
- ICT Security policy is implemented according to the Kenya security Act 2018

Trainees to demonstrate knowledge in relation to:

- Implement security measures contained in the ICT security policy
- Apply physical and logical risk mitigation measures
- Take corrective action
- Security audit to identify security gaps
- Generate system audit report

#### 5.3.4.2 Information Sheet

Implement security measures contained in the ICT security policy:

- Identify your risks
- Learn from others
- Make sure the policy conforms to legal requirements
- Level of security equals to the level of risk
- Include staff in policy development
- Train your employees
- Get it in writing
- Set clear penalties and enforce them
- Update your staff
- Install the tools you need



**Read:** Successful ICT policy: https://www.computerworld.com/article/2572970/10-steps-to-a-successful-security-policy.html

**Read:** Kenya's ICT policy: http://icta.go.ke/national-ict-policy/

**A logical mitigation strategy** ties assets to threats to vulnerabilities to identify risks. Solutions for the identified risks typically enhance three facets of security: Policies, Procedures and Training; Physical/Electronic Security Systems; and Security Personnel.

**Corrective action** is a process of communicating with the employee to improve attendance, unacceptable behavior or performance. You may take corrective action when other methods such as coaching and performance management have not been successful.

**The network security audit** is a process that many managed security service providers

(MSSPs) offer to their customers. In this process, the MSSP investigates the customer's cyber security policies and the assets on the network to identify any deficiencies that put the customer at risk of a security breach.

#### 5.3.4.3 Self-Assessment

i. What is corrective action?
ii. Define network security audit?
iii. Review the computer lab and prepare a report if it conforms to the ICT Security Act 2018.
iv. Security levels should be _____ to risks involved.
    A. Equal
    B. Great
    C. Appoximate
v. National security of Kenya is govern by _____ .
    A. ICT Authority
    B. Police
    C. Network of ICT

#### 5.3.4.4 Tools, Equipment, Supplies and Materials

Firewall, Malware Protection, Software Updates, Audit and Accountability



#### 5.3.4.5 References


- https://www.computerworld.com/article/2572970/10-steps-to-a-successful-security-policy.html
- https://www.nyu.edu/about/policies-guidelines-compliance/policies-and-guidelines/data-and-system-security-measures.html
- Cyber Security, authored by John G. Voeller published by Wiley 2014


### 5.3.5 Learning Outcome 4: Test system vulnerability

#### 5.3.5.1 Learning Activities

The following are the performance criteria:

- Schedule system testing plan is developed
- Vulnerable levels of the system are identified
- Security ethical penetration is done as per the ICT security policy
- Report on system vulnerability is generated
- Corrective action is taken based on the System Vulnerability report

Trainees to demonstrate knowledge in relation to:

- Definition of vulnerability
- System testing schedule
- Levels of system vulnerability
- Ethical penetration

- System vulnerability test report

### 5.3.5.2 Information Sheet

**Computer vulnerability** is a cyber security term that refers to a defect in a system that can leave it open to attack. This vulnerability could also refer to any type of weakness present in a computer itself, in a set of procedures, or in anything that allows information security to be exposed to a threat.

**A System test schedule** includes the testing steps or tasks, the target start and end dates, and responsibilities. It should also describe how the test will be reviewed, tracked, and approved.

Level of system vulnerability
Critical, High, Medium, Low

**Read:** types of vulnerability:
https://www.atlassian.com/trust/security/security-severity-levels

**Ethical penetration** is a broader term that includes all hacking methods, and other related cyber attack methods. The goal of ethical hacking is still to identify vulnerabilities and fix them before criminals can exploit them, but the approach is much wider in scope than simple testing. In other words, ethical hacking is more of an umbrella term, while penetration testing represents one subset of all ethical hacking techniques.



**Watch:** Ethical penetration: https://youtu.be/BEdaiUzUsgM

**A vulnerability report** is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system.

### 5.3.5.3 Self-Assessment

i. What is ethical penetration?
ii. Define computer vulnerability.
iii. Explain level system vulnerability.
iv. Identify the vulnerability levels of a system. Prepare a case study using an example.
v. Prepare report at a worksite on the security system on their computers and network.
vi. _____ is a broader term that includes all hacking methods, and other related cyber attack methods.
   A. Vulnerability
   B. Ethical penetration
   C. A System test schedule
vii. When is it better to perform a vulnerability assessment versus a penetration test?
   A. It is necessary to perform them together
   B. When you seek a larger overview of the environment, versus a smaller view
   C. Penetration tests are full of false positives and should not be used

D. Penetration tests are potentially damaging to devices and should not be used

viii. _____ is a weakness that can be exploited by attackers.

A. System with virus
B. System without firewall
C. System with vulnerabilities
D. System with strong password

**5.3.5.4 Tools, Equipment, Supplies and Materials**

Wireshark, Nmap, Metasploit, sqlmap

**5.3.5.5 References**

- https://www.hudsoncourses.com/ethical-hacker-vs-penetration-tester/
- https://www.atlassian.com/trust/security/security-severity-levels
- Cyber Security, authored by John G. Voeller published by Wiley 2014

**5.3.6 Learning Outcome 5: Monitor security system**

**5.3.6.1 Learning Activities**

The following are the performance criteria:

- Performance of the security systems is evaluated
- Reports on security system are generated
- Security systems are updated or overhauled based on the security system report



Trainees to demonstrate knowledge in relation to:

- Define monitoring criteria
- Evaluation of system security performance based on defined criteria
- Updating and overhauling of security systems
- Generate monitoring report

**3.3.6.2 Information Sheet**

Given the ubiquitous, unavoidable nature of security risks, quick response time is essential to maintaining system security and automated, continuous security monitoring is the key to quick threat detection and response. **Monitoring criteria** should be for hackers and malware, to disgruntled or careless employees, to outdated or otherwise vulnerable devices and operating systems, to mobile and public cloud computing, to third-party service providers.

The evaluation criteria developed include the following objectives:

- **Measurement:** Provides a metric for assessing comparative levels of trust between different computer systems.
- **Guidance:** Identifies standard security requirements that vendors must build into systems to achieve a given trust level.

- **Acquisition:** Provides customers a standard for specifying acquisition requirements and identifying systems that meet those requirements.
- **Security policy:** The rules and procedures by which a trusted system operates.
- **Discretionary access control (DAC):** Owners of objects are able to assign permissions to other subjects.
- **Mandatory access control (MAC):** Permissions to objects are managed centrally by an administrator.
- **Object reuse:** Protects confidentiality of objects that are reassigned after initial use. For example, a deleted file still exists on storage media; only the file allocation table (FAT) and first character of the file have been modified. Thus residual data may be restored, which describes the problem of data remanence. Object-reuse requirements define procedures for actually erasing the data.
- **Labels:** Sensitivity labels are required in MAC-based systems.
- **Assurance:** Guarantees that a security policy is correctly implemented.
- **System integrity:** Hardware and firmware operate properly and are tested to verify proper operation.
- **Updating and overhauling of Security systems :** When a company needs new data security practices, an external viewpoint can prove invaluable. Remember, a data security auditor has experience helping many different kinds of companies find what they need to change, and that experience can prove invaluable in creating the *right* kind of overhaul plan. Third party intervention provided broader view of the problem at hand for an organization.



**Read:** Planning security overhauling: https://www.infiniwiz.com/planning-a-security-overhaul-here-are-key-tips-on-how-to-start/

**5.3.6.3 Self-Assessment**

i. Define monitoring criteria?

ii. Explain evaluation of system security?

iii. What is overhauling of security?

iv. _____ identifies standard security requirements that vendors must build into systems to achieve a given trust level.
   A. System integrity
   B. Assurance
   C. Guidance
   D. Acquisition

v. _____Hardware and firmware operate properly and are tested to verify proper operation.
   A. System integrity
   B. System architecture
   C. Covert channel analysis

vi. _____ provides a metric for assessing comparative levels of trust between different computer systems.
   A. Guidance

B. Measurement
C. Security policy
D. Monitoring criteria

vii. You are a Network security administrator and your company. Your company has been attacked by hackers, how will you identify what sort of information have been hacked?

viii. You are an ICT manager of a hotel. The General Manager of your hotel called you this afternoon, since he is having difficulty in accessing past customer details. The files are randomly opening and there is gibberish. What are the possibilities that customer data have been hack? What are your suggestion actions?

**5.3.6.4 Tools, Equipment, Supplies and Materials**

Network Performance Monitor, Nmap, Computer

**5.3.6.5 References**


- https://www.dummies.com/programming/certification/evaluation-criteria-systems-security-controls/
- https://www.infiniwiz.com/planning-a-security-overhaul-here-are-key-tips-on-how-to-start/
- https://pdfs.semanticscholar.org/45a2/775770d870b8675fb1301919224c9bcb7361.pdf
- Cyber Security, authored by John G. Voeller published by Wiley 2014