University Of Bahrain

College of Information Technology

Department of Information Systems

ITIS466
Kifah Design and Printing

Network Infrastructure Audit Report

Prepared by:

Faiza Mohammed Saleem	**20177463**
Muhammed Fadhel Fuhad	**20155823**
Safna Nisa Manzil	**20172223**
Tamara Hassan	**20147828**

Instructor: Dr. Mohamed Tayeb Mahmood

Academic Year 2020-2021, Second semester

INDEPENDENT AUDITOR'S REPORT

Kifah Design and printing

Road No.1401, Riffa, Kingdom of Bahrain

We are presenting the results of our IT audit Kifah Design and Printing Network Infrastructure Audit Report covering the period of 17 April to 19 April 2021. The report includes our conclusions and/or opinion regarding the prioritization of network risks, and recommending the best remedies and potential areas which need improvement. The audit was conducted in accordance with the IS Audit and Assurance Standards and IS Audit and Assurance Guidelines issued by ISACA. We believe that the evidence obtained provides a reasonable basis for our conclusions and findings regarding the audit objectives.

Safna Nisa Manzil

TABLE OF CONTENTS

INTRODUCTION

Kifah Design and Printing provide a service and sometimes they provide the products that the customer wants them to print on. Their attention to detail, creative problem-solving, customer responsiveness, and on-time delivery keep them ahead of the competition. They also have a highly qualified prepress team that provides clients with proofs and assistance in a timely manner. The design logos, wedding cards, and so on also they can provide you with a customized fabric. As they say, “they print anything on anything”.

Its mission is as follows: “We seek to provide the best quality that lasts for a lifetime.”

The primary objectives of their business are:

1. Opening another branch
2. Export products to other countries.
3. Introducing more variety types of printing that cannot be found anywhere except Kifah design and printing.
4. Increase interest rate to 50%.

Their customer/client base includes anyone who wishes to print any kind of design on any kind of material. Kifah Design and Printing are currently located in Riffa, Kingdom of Bahrain but they have planned to expand their business to neighboring countries.

They are a printing and communications design firm of medium scale. They offer cutting-edge printing (both digital and offset), as well as professional graphic design, binding, and bulk mailing services. So the applicable IT infrastructure covers the servers, routers, infrastructure software, storage equipment and switches. Finally, they have a highly professional finishing department with a wide range of cutters, directories, and stitching equipment to ensure that your tasks are completed with the utmost care.

The primary goal of our audit was to define and review Kifah Design and Printing's network infrastructure, as well as possible areas where it needs development.

Our audit was subjected to the Network infrastructure and implementation area of Kifah Design and Printing where we identify and prioritize risks in their network, and then prescribe the optimal solutions.

EXECUTIVE SUMMARY

The key purpose of our project was to perform an audit of Kifah Design and Printing's core network infrastructure and implementation. The audit's ultimate goal was to map and inventory the network in terms of hardware and software. It's a difficult job that necessitates manually identifying network components. One of the objectives was to define the IT security requirements that the organization adheres to, as well as to identify the access control systems in place to ensure that only approved employees have access to those systems and that access is both permitted exclusively and restricted accordingly. At Kifah the employees have different access rules for various systems and applications. The organization makes an effort to align workers with the company's goals and policies. It also does a fine job with data backup. Unavoidable risks were discovered despite a detailed understanding of the scope, sensitivity, and complexity of the company's network infrastructure. As we tried to determine the presence of a business continuity plan and a disaster recovery plan, it came to our attention that the contingency plans must be revised because there is no automatic device replacement in the event of a disaster.

AUDIT SCOPE

In accordance with ISACA's IS Audit Assurance standard and guidelines, we performed an audit of network infrastructure and implementation at the Kifah Design and Printing, for the period of 17 April to 19 April 2021.

Prior to the audit, we planned how the audit will be conducted in order to gain sufficient information and evidence that will help us in the findings.

The scope of our audit will involve a thorough examination and evaluation of the adequacy and effectiveness of the company's network infrastructure such as the network to which the system is connected to, determining the inventory i.e., identifying the kind of devices running on the network, how well the devices are connected and protected from any unauthorized access or environmental damage and identify if any security concerns are needed to be addressed on.

Our scope was limited to conducting the audit only at one location being the head office of the company where we could personally hold meetings with the CEO and employees of the organization. We were restricted from visiting their workshop where their orders are being processed, network devices etc are installed because of the current COVID pandemic situation. So our overall audit strategy was dependent on the information that we collected during the meeting with the CEO and employee of Kifah Design and printing.

AUDIT OBJECTIVES

Our audit objective was to ensure that standards are in place for designing and selecting a network architecture and to identify potential areas that needed improvements as appropriate.

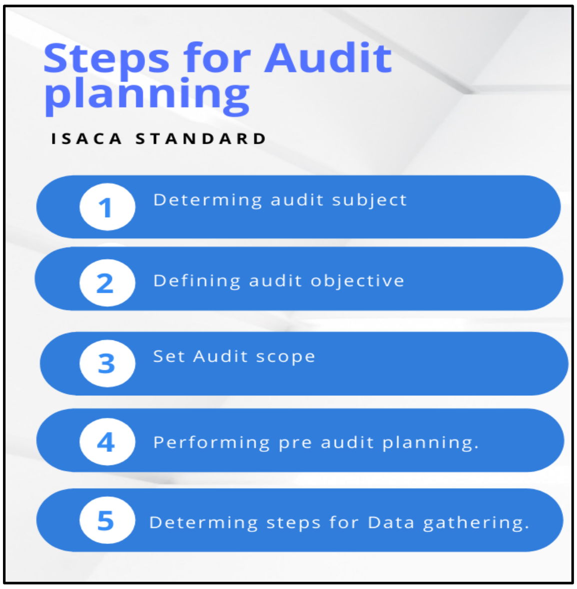
Other objectives are to ensure that:

a) The physical, environmental and logical controls over the network infrastructure are well maintained, adequate and appropriate.
b) The company resources are optimized.
c) It keeps up with the latest developments in its field of business.
d) Employees are aware of their responsibilities and work to fulfill the company's objectives.
e) To determine the internal control system (Network Security Access) in which the IT security architecture provides controlled access to and protection of the company's electronic information.
f) How well and to what extent the security measure is being implemented.

AUDIT METHODOLOGY

Pre-audit/Audit planning

In order to determine the scope and objectives of the audit, we performed pre-audit (audit planning) steps where we researched Kifah Design and Printing mission, vision, related business processes, and supporting technologies and gathered as much information that will help us with the audit. After collecting some relevant information about the organization we followed the audit steps below to complete the process. We had a meeting with the CEO of Kifah Design and printing at the main office and collected the information of their organization but were not able to get access into their workshop where network hardware devices, printing devices etc are all installed. By reviewing relevant documents and conducting the interview, we were able to identify the organization's legal, and regulatory criteria, as well as the network infrastructure. Our overall audit strategy was dependent on the information collected during the meeting we had with the CEO and employee of Kifah Design and printing.



Steps for Audit planning

ISACA STANDARD

1 Determing audit subject

2 Defining audit objective

3 Set Audit scope

4 Performing pre audit planning.

5 Determing steps for Data gathering.

Conducting the Audit:

Our audit was conducted in accordance with IS Audit and Assurance Standards and IS Audit and Assurance Guidelines issued by ISACA. We started choosing the auditee organization by discussing amongst the team members and finalized Kifah Design and Printing as our auditee organization by 26th of April,2021. After choosing the auditee organization, we started to develop our auditing strategies. We then asked for a meeting with the head of the organization to discuss our auditing program with them, for which the CEO of Kifah Design and printing positively replied. Our meeting with the CEO was scheduled on 17th May and was attended by two members of our team. On the next consecutive days, 18th and 19th of may we interviewed two of the employees of the organization in which one of them is responsible for maintaining network security. Prior to the meeting, about 45 questions were prepared based on the network infrastructure and implementation area of the organization, and the responses to those questions and other information from the meeting were viewed and observed carefully. As we were not authorized to view their network devices visually or to enter the workshop, the only methodology to conduct the audit was the meeting with the CEO and employees. The audit results from the meeting were then discussed among the team members for further analysis and documentation.

For the content and structure of the audit report, we adopted the IS Audit and Assurance Standard, which clarifies the scope, objectives, duration of coverage, nature and extent of the audit work performed. The audit criteria that was used in the audit included management policies and procedures, and management control guidelines, which are outlined in COBIT® 5, as issued by ISACA.

AUDIT RESULTS OR AUDIT FINDINGS

1. System Network

Finding	System network and location
Condition	The organization’s system uses the LAN network and operates on more than one location.
Criteria	Systems should be connected via networks to facilitate resource sharing and convenient communication. The system should operate in several locations in case of emergency such as system failure or fire etc.
Cause/Effect	The organization has reduced risks since it uses the LAN network which enables resource sharing, improved security and communication, as well as operates on multiple locations.
Recommendation	Continued use of LAN and system setup on multiple locations.

2. Network devices and file server

Finding	Secure network hardware, software and file server location.
Condition	Kifah D&P has its network hardware placed in a safe location with access to only the network administrator. The file servers are locked and secured. All the network hardware and software devices infrastructure problems of Kifah D&P have been reviewed periodically.
Criteria	Network devices including both hardware, software and file servers should be placed in safe and monitored environments and the access should be given to only those responsible for it.
Cause/Effect	The organization has reduced data loss and misuse risks because it secures the hardware and

	servers and limits access to it. But it was identified that it has problems with its software as some of the software components cannot handle the graphic design problems.
Recommendation	Continued safeguarding of network hardware and limited access. Introduce a convenient, adaptable, problem-free, safe, and accurate graphic design program that can help in designing a wider variety of designs.

3. Key logs

Finding	Key logs monitoring and access
Condition	The network file server facilities in Kifah D&P are monitored to avoid unauthorized access and accessible by only the network administrator
Criteria	The key logs of employees entering and leaving the network premises must be monitored to keep track of their activities within the organization and limit access to avoid unauthorized access.
Cause/Effect	Kifah D&P tracks employee activities therefore any issues related to employee logs are minimized.
Recommendation	Continued key logs monitoring and limited access.

4. Network and transmission wiring

Finding	Network and transmission wiring
Condition	Kifah D&P maintains secure network and transmission wiring
Criteria	The physical network transmission wiring should be secured for safety as well as to avoid damage at times of fire or other harmful situation.

Cause/Effect	Maintenance of wiring and associated controls leads to a safe working environment
Recommendation	Maintenance of circuits and replacing frayed wires

5. Environment controls: Server facility

Finding	Environmental controls
Condition	Kifah D&P does not have any electrical surge protectors and fire extinguishers. The systems are kept in adequate ventilation to avoid overheating. The network modules are fitted with UPSs and they have data backup on cloud and the server rooms are cleaned and maintained and they have fire alarms to notify employers of possible fire threats.
Criteria	The organization should have electrical surge regulators and protectors to ensure stable and regular flow of power within the network. They should implement HVAC systems to maintain desirable temperatures for a safe work environment and asset (data or otherwise) protection. Fire suppression systems such as fire alarms, fire extinguishers and sprinklers etc. should be installed. UPS allows the Kifah D&pto regulate workflow and support network operations. Data backup should be done on a secure and reliable platform such as cloud. The server rooms should be regularly cleaned and maintained.
Cause/Effect	Kifah D&P does not have disaster management in place. Though they have fire alarms, the fire suppression systems are not installed in case of emergency which puts the organization at a potentially high risk of damage. With fire alarms, at most, they can contact the firefighting crew for help but Kifah D&P could face enough loss of property and data until help arrives. The organization has UPS installed which

	allows the network to continue operating in case of slight power fluctuations or gradual power loss. Their data is backed up reliably on the cloud and offline storage media are protected from damage. The have well maintained and regularly cleaned server rooms
Recommendation	Install fire suppression systems (fire extinguishers and sprinklers etc.) and set up training sessions to train employees to enact in case of emergency.

6. Logical security control: Passwords

Finding	Logical security authentication
Condition	Kifah D&P organization does not assign passwords to employees because they claim to share their work and hence they don't perform any further secure operations to preserve sensitive information.
Criteria	Passwords should be assigned to secure data and systems so that colleagues or an unauthorized person does not get access to an employees' system and work. Sufficient authorization and authentication procedures should be deployed to prevent misuse and loss of data.
Cause/Effect	Kifah D&P is at high risk of data theft or misuse since they don't have any security controls in place to secure employee's systems and organizational resources. This could lead to potential loss of business/customers if they encounter such misfortune.
Recommendation	Passwords, multi-step verifications, fingerprinting, biometric scanning etc. should be deployed wherever it seems adequate to secure the organization's systems and work between colleagues.

7. Network access

Finding	Network access safety, monitoring and recording
Condition	The network access authorization is given only when that person requires the details to do any configuration. The network workstations do not become inactive and in case if it does, the hardware supervisor can be contacted remotely. Kifah D&P has a program set up to record login attempts and the manager/supervisor's accounts are reviewed periodically. The information of communication lines connected to the outside is maintained by the network supervisor.
Criteria	Authorization should be given only when it is absolutely required and the activities taking place after handing over authorization should be monitored. Network workstations should be equipped with high infrastructure to prevent system downfall or inactivity and there should be immediate contact available in case of a system behavior irregularity. All attempts to log into supervisor accounts, whether successful or not, should be recorded in the database. These accounts should go through evaluations periodically to detect any malicious or unauthorized activities. Information on communication and interactions to the outside of the organization should be updated regularly and maintained to avoid any misuse.
Cause/Effect	Kifah D&P follows adequate authorization procedures, network workstation functions and contact procedures as well as records login details, followed by reviewing accounts and maintaining communication information. Hence they do not face many risks in this network access area.
Recommendation	Once authorization is given, the activities that follow should be monitored. All data collected on attempted logins, communications etc. should be reviewed regularly to avoid neglect or overlooking of any malicious activity.

8. Network access change request

Finding	Network updates approval and documentation
Condition	Network connections changes are approved by the manager before deployment and the network logical access configurations such as extensions, updates, and deletions are well documented.
Criteria	Network updates and any changes should be done only after they have been approved by the authority responsible to overview these areas. The configurations taking place should be documented to ensure adequate tracking of activities. This also allows employees to lookup documentations in case of similar situations.
Cause/Effect	Kifah D&P follows appropriate procedures to authorize and document network configurations. This leads to a well-organized and stable workflow.
Recommendation	It is advised to continue documenting network changes and get authorization before deploying changes.

9. Network Testing

Finding	Preparing a test plan for the network.
Condition	Kifah D&P implements/follows appropriate test plans in order to test their network for identifying the vulnerabilities within their network, and in hardware and communication links.
Criteria	Kifah D&P implements test plans like Recovery testing for ensuring backup and recovery of data procedures are working properly, Security testing for verifying that their network meet security requirements,Volume testing for ensuring their network runs smoothly when subjected to high data processing loads over

	extended periods of time and Performance testing in order to test the performance of their network.
Cause/Effect	By implementing such plans Kifah D&P can identify the vulnerabilities within their network, then analyze it and find appropriate solutions for it or correct it.
Recommendation	Though Kifah D&P have appropriate test plans implemented, it cannot assure to completely identify the vulnerabilities within the network. Implementing test plans like penetration testing (pen test) will ensure more consistent network security, locate network vulnerabilities and identify areas which need improvement and security gaps.

10. Security reports

Finding	Access authorization, security reports review,
Condition	Kifah D&P has authorized access procedures and they regularly analyze security reports. Prepared follow-up procedures are also set up in case of unauthorized access.
Criteria	The organization should review network software maintenance activities, network systems documentation, authorization documentation and network system software security
Cause/Effect	Though the organization has the above procedures and analysis (mentioned in the Condition row), it is insufficient to get the big picture of what is required and what is going on in the organization, therefore Kifah D&P are at a risk of cyber threats, system malfunctions due to inadequate maintenance of softwares and security softwares.

Recommendation	It is recommended to: Review and test system software implementation to determine the adequacy of controls in: •Authorization procedures •Access security features •Documentation requirements •Documentation of system testing •Audit trails Review authorization documentation to determine whether: •Additions, deletions, or changes to access authorization have been documented •The attempted violation reporting review and follow-up Review system software security to ensure: •Procedures have been established to restrict the ability to avoid logical security access controls •Procedures have been established to limit access to the system interrupt capability •Security provided by the system software is adequate •Existing physical and logical security provisions are adequate to restrict access to the master consoles •System software vendor-supplied installation passwords were changed at the time of installation

11. Security mechanism

Finding	Security procedures mechanism
Condition	Kifah D&P network datafiles/datasets have been documented well and have been checked for stable security conditions. Programs, transaction processors, and datasets have been approved before launch to individuals. They use

	encryption techniques to protect sensitive data on the network. They have established procedures on the distributed processing network to ensure hardware and software effectiveness.
Criteria	The organization should keep a record of its confidential files and data to avoid any data misuse, loss or misplacement. It should periodically check if these files/data have been tampered with and secure its location and access controls. Approval of senior management and network administrators responsible should be granted before it any programs, transaction processors and datasets are launched for organizational use. Encryption and decryption techniques should be used to safeguard sensitive data. Procedures to ensure effective controls over the hardware and software used by the departments, served by the distributed processing network should be established and well documented.
Cause/Effect	Kifah D&P followsa protocol and secures all confidential information related to its business and its customers and they have procedures to check and review these files regularly.
Recommendation	Continued review of confidential files and secure authorization to avoid any misuse in future. Document any procedures enacted to record activities for future reference.

12. Network operation procedures

Finding	Procedures in place for continued network operations
Condition	Kifah D&P has guaranteed procedures to affirm data compatibility of the network datasets. They have appropriate procedures for recovery and restart network procedures. There IS distributed network configuration is set up to combat

	network service inability. Kifah D&P ensures that they apply by the laws and regulations of Bahrain during its data transmission operations.
Criteria	Organizations should have a compatible relationship between networks and associated data. If the organization does not have compatible infrastructure it must develop or outsource to preserve compatibility. Appropriate recovery procedures should be established and documented beforehand to quickly respond to issues regarding a lack of connectivity at one location, which could impact network's ability to provide service to other sites. All organizations should abide by the laws and regulations of the countries they operate in to avoid any legal or issues disputes.
Cause/Effect	Kifah D&P does not face many risks in this area as it follows almost all above mentioned criteria, except for documentation. Hence it's at low risk of business disruptions.
Recommendation	It is mandatory to document established procedures to refer to in future and keep track of organizational activities.

13. Interview of the person responsible for maintaining network security

Finding	Network security maintenance personnel interview
Condition	Network security maintenance personnel at Kifah D&P are mindful of the risks of physical and logical access that must be avoided and of the importance of constantly monitoring logons and keeping track of employee changes. They are also knowledgeable of maintaining and monitoring access.

Criteria	Network security maintenance personnel should be aware of the risks the organization would face if physical and logical access is compromised. They must constantly monitor logons and keep track of employee activities in the particular network areas they are responsible for. Maintenance and monitoring access should not be taken for granted followed regularly.
Cause/Effect	Since Kifah D&P follows suitable authorization procedures, network workstation functions, and contact processes, as well as evaluating accounts and maintaining communication data, they are not exposed to many threats in the network access area.
Recommendation	Train the network personnel and inform them of the critical network access controls, risks and infrastructure.

14. Interview employee

Finding	Organization’s designated employee
Condition	Kifah D&P’s employees are aware of management policies regarding network security and confidentiality. Their organization does not have a Bring-Your-Own-Device (BYOD) Policy for employees. They do not have proper employee termination procedures in place such as reclaiming identification badges and deactivating other access methods.
Criteria	Organization’s employees should be aware of management policies regarding network security and confidentiality through proper documentation and enforcement. The organization should have a Bring-Your-Own-Device (BYOD) Policy for employees for their comfort but their devices should be connected to a separate network that does not

	integrate/interact with the organization’s main secure networking to avoid any potential risks of security compromise such as third-party applications. BYOD policy gives the organization insight into which devices are connecting with the organization's networks and the vulnerabilities that come with it. Appropriate employee termination procedures in place such as reclaiming identification badges and deactivating other access methods such as card-key readers and biometric devices.
Cause/Effect	Since the employees are made aware of the network management policies and use other networks to connect their devices, it can cause the organization to reduce potential network risks, decrease their bandwidth demands, and minimize network exposure as much as possible.
Recommendation	Document management policies and make sure employees are aware of them. Enforce a BYOD policy to assure employees comfort. Appropriate employee termination procedures such as reclaiming identification badges and deactivating other access methods such as card-key readers and biometric devices to avoid breach of security.

Management Response

Management responded expressing their decision to use LAN across many regions, key logs monitoring and securing network hardware, as well as limiting access to it. They shall also be introducing a graphic design program that can assist in the creation of a broader range of designs. Their response included the installation of fire suppression systems as well as the maintenance of circuits and frayed wires. Security and monitoring of the organization's systems will be prioritized, with regular reviews to ensure that hostile activity is not overlooked. Before deploying changes, undue attention will be taken to document network modifications and obtain authorization. Test plans will be prioritized, such as penetration testing to verify network security, the finding of network vulnerabilities, and the identification of areas that need improvement and security gaps. Continued inspection of secret files, as well as security authorization, to prevent further misuse will also be looked into.

AUDIT CONCLUSION/OPINION

The purpose of this section is to provide an overall conclusion or opinion with respect to the engagement's audit objectives. Understandably, the engagement was performed as an examination with an appropriate level of audit testing, in accordance with all relevant audit standards, and conclusions based on sufficient, relevant and valid evidence.

We discovered at the end of the audit that Kifah design and printing has acceptable security measures in place as well as the required precautions in place to protect their business. They do, however, require a significant security upgrade to stay up with internet threats and attacks. Because there are no security controls in place to guard staff systems and organizational resources, Kifah D&P is at significant risk of data theft or misuse. If they experience such disaster, this could result in a loss of consumers. They are not exposed to many risks in the network access area since Kifah D&P follows proper authorisation procedures, network workstation functions, and contact processes, as well as evaluating accounts and maintaining communication data. Implementing test plans such as penetration testing (pen test) will improve network security by locating network vulnerabilities, identifying areas for improvement, and identifying security gaps. Disaster management is not in place at Kifah D&P. Despite the fact that they have fire alarms, they do not have fire suppression equipment in place in the event of a fire, putting the organization at risk of serious damage. Kifah should install fire suppression equipment and hold training sessions to prepare personnel for emergency situations. They make good use of customer feedback and change accordingly, as well as paying attention to employee needs. The company often reminds its personnel to be cautious with consumer information and has yet to receive any complaints.

PPENDICES

A. Acronyms and abbreviation:

BYOD: Bring-Your-Own-Device

UPS: Uninterruptible Power Supply

HVAC: Heating, Ventilation and Air Conditioning

B. Glossary of terms:

BYOD (Bring-Your-Own-Device)-It's an IT policy that allows and even encourages employees to use personal electronic devices like smartphones, tablets, and laptops to access company data and systems.

C. Full copy of auditee response

Audit Questionnaire

Network infrastructure and implementation

Questions	No	Yes	Remarks
1. Is the system on the network?		Yes	
2. If the system is on the network, is it connected to : Internal LAN and/or on intranet? WAN and MAN and/or on extranet? Web based /public domain?		Yes	It is connected on internal LAN network
3. The system is functioning at : Only one location? OR More than one? OR Less than 5 locations?		Yes	The system is functioning on more than one location

2. Network hardware devices and file server			
1. Are network hardware devices placed in a safe location and only the network administrator has access to them?		Yes	

2. Is the housing of network file servers locked or otherwise secured to prevent removal of boards, chips or computers itself?		Yes	
3. Have you reviewed your infrastructure problems that include both hardware and software components.		Yes	
4. Key logs			
1. Is it possible to monitor the keys to the network file server facilities in order to avoid the possibility of unauthorized access?		Yes	
2. Are keys assigned only to the appropriate people, e.g., the network administrator and support staff?		Yes	There is a key only for the network administrator
4. Network and transmission wiring			
1. Is the wiring physically secured?		Yes	
5. Environment controls: Server facility			
1. Have you installed any electric surge protectors?	No		There is no need for it.
2. Are there necessary fire prevention systems and adequate disaster suppression means available?		Yes	They have a fire alarm

3. Are there fire extinguishers nearby that are tested on a daily basis?	No		There will be a potential risk to lose the workshop which is why they must do that as they have many machines and electricity wires
4. Are the systems kept in adequate ventilation? Do they have HVAC systems to maintain desirable temperature?		Yes	
5. Are the main network modules fitted with an UPS that allows the network to continue operating in case of slight power fluctuations or gradual power loss in the middle of a sustained power outage?		Yes	the main network modules fitted with an UPS that allows the network to continue operating in case of slight power fluctuations
6. Is the data backed up on the cloud? Are the backup media protected from environmental damage?		Yes	They store there backup on cloud that's why it is protected from environmental damage
7. Is the data on backup diskettes, tapes, CD-ROMs, and other offline storage media protected from environmental damage?		Yes	They use cloud system to store backup data
8. Is the server room free of dust, smoke, and other debris, particularly food?		Yes	The server room is well cleaned every day
9. Are the server anti-malware softwares and firewalls deployed and maintained? If yes, how often?		yes	It is always upgraded and maintained, every month
10. Are the server operating systems being upgraded to the latest service release?		Yes	The server operating systems being upgraded to the latest service release

6. Logical security control: **Passwords**			
1. Are employees assigned unique passwords?	No		They don't need to so as they share the work they do
2. Is it necessary for employees to update their passwords on a regular basis?	No		there is no potential risk as the since each user is not assigned their own unique passwords and they have access to every device.
7. Network access			
1. Is network access based on written authorization and given on a need-to-know/need-to-do individual's responsibilities?		Yes	
2. Do network workstations become inactive for a certain amount of time? Is it possible to contact the machine supervisor remotely?	No		The network workstation never becomes inactive for a certain amount of time. The manager device is contacted remotely.
3. Have all attempts to log in to the supervisor account been recorded in the computer system?		Yes	
4. Is it possible to do an independent review of supervisory or managerial accounts?		Yes	

5. Is up-to-date information regarding all communication lines connected to the outside maintained by the network supervisor?		Yes	
8. Network access change request			
1. Are demands for network connection changes approved by the appropriate manager?		Yes	
2. Are demands for network logical access extensions, updates, and deletions documented?		Yes	
9. Network Testing			
1. Are appropriate implementation, conversion and acceptance test plans developed for the organization's distributed data processing network, hardware and communication links?		Yes	
10. Security reports			
1. Is only authorized access occurring?		Yes	
2. Is it possible to review security reports thoroughly and in a timely manner?		Yes	
3. Are follow-up procedures taking place regularly and effectively in case of unauthorized access?		Yes	
11. Security mechanism			
1. Have you listed all of the network's confidential files/datasets and determined the security conditions ?		Yes	

2. Are only approved programs, transaction processors, and datasets accessible to individuals?		Yes	
3. Is encryption being used to protect sensitive data on the network?		Yes	
4. Were procedures established to ensure effective controls over the hardware and software used by the departments served by the distributed processing network?		Yes	
12. Network operation procedures			
1. Do you have procedures in place to guarantee that data compatibility is correctly applied to all of the network's datasets?		Yes	
2. Have you built appropriate restart and recovery procedures at each user location that the distributed distribution network serves?		Yes	
3. Has the IS distributed network been configured in such a way that a lack of connectivity at one location has a minimal impact on the network's ability to provide service to other sites?		Yes	
4. Are there provisions to ensure consistency with the laws and regulations governing transmission of data?		Yes	
13. Interview of the person responsible for maintaining network security			

1. Is the person mindful of the risks of physical and logical access that must be avoided?		Yes	
2. Is the individual aware of the importance of constantly monitoring logons and keeping track of employee changes?		Yes	
3. Is the person knowledgeable in how to maintain and monitor access?		Yes	
14. Interview employees			
1. Are the employees aware of management policies regarding network security and confidentiality?		Yes	
2. Does your organization have a Bring-Your-Own-Device (BYOD) Policy for employees? If yes, Have you reviewed Your Bring-Your-Own-Device (BYOD) Policy of employees?	No		
3. Are proper employee termination procedures in place such as reclaiming identification badges and deactivating other access methods such as card-key readers and biometric devices?	No		The company does not handle such sophisticated procedures yet.

D: Auditee representative details:

The audit was assisted by **Mr. Thaer Hasan Salem** holding the **CEO** position at Kifah design and printing. He has provided his contact information as follows Kifah.printing@gmail.com and assured his undivided availability and attention any time of need.