Project Part 2

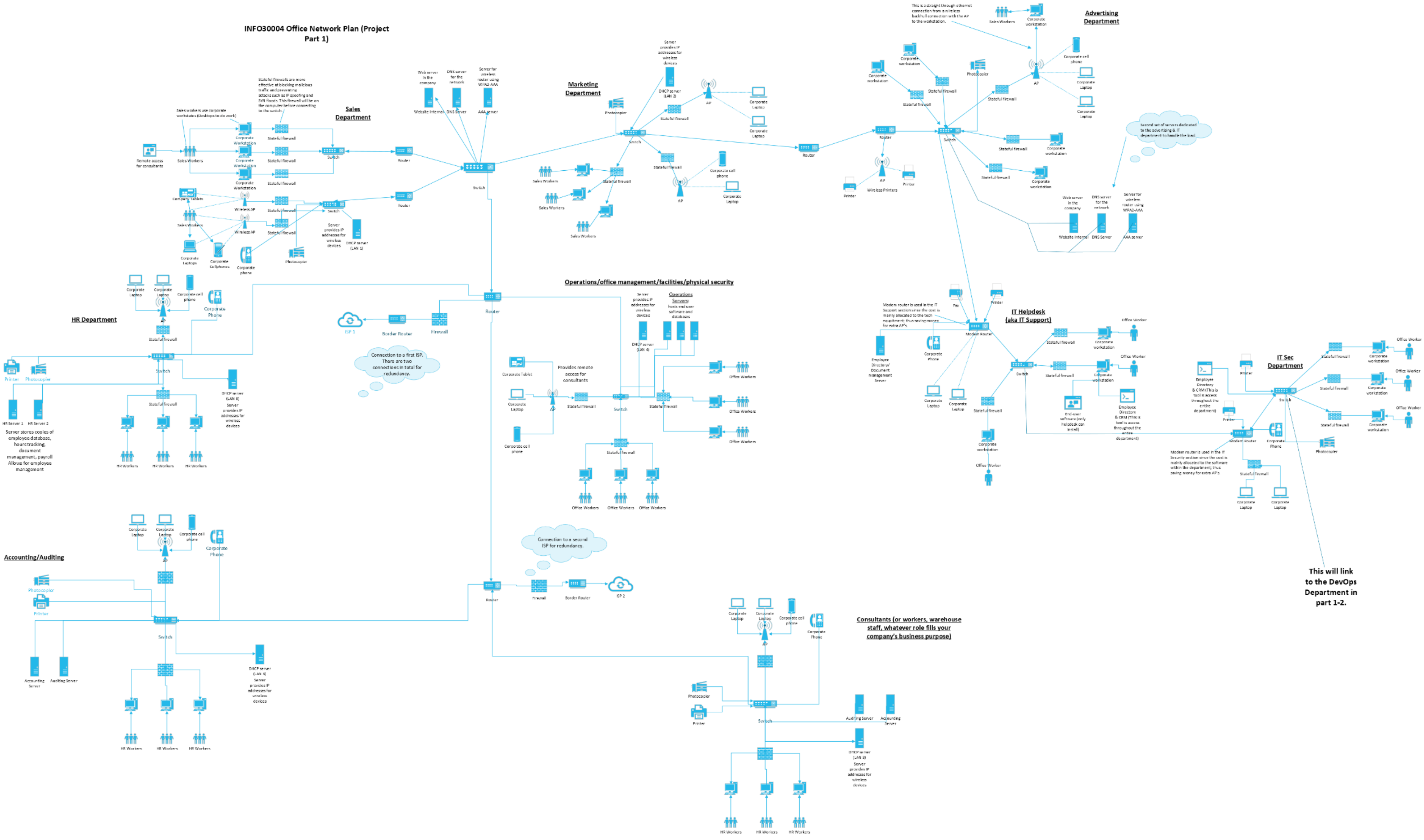
Jackson Yuan and Neryl Anne Denosta

Professor Pedram Habibi

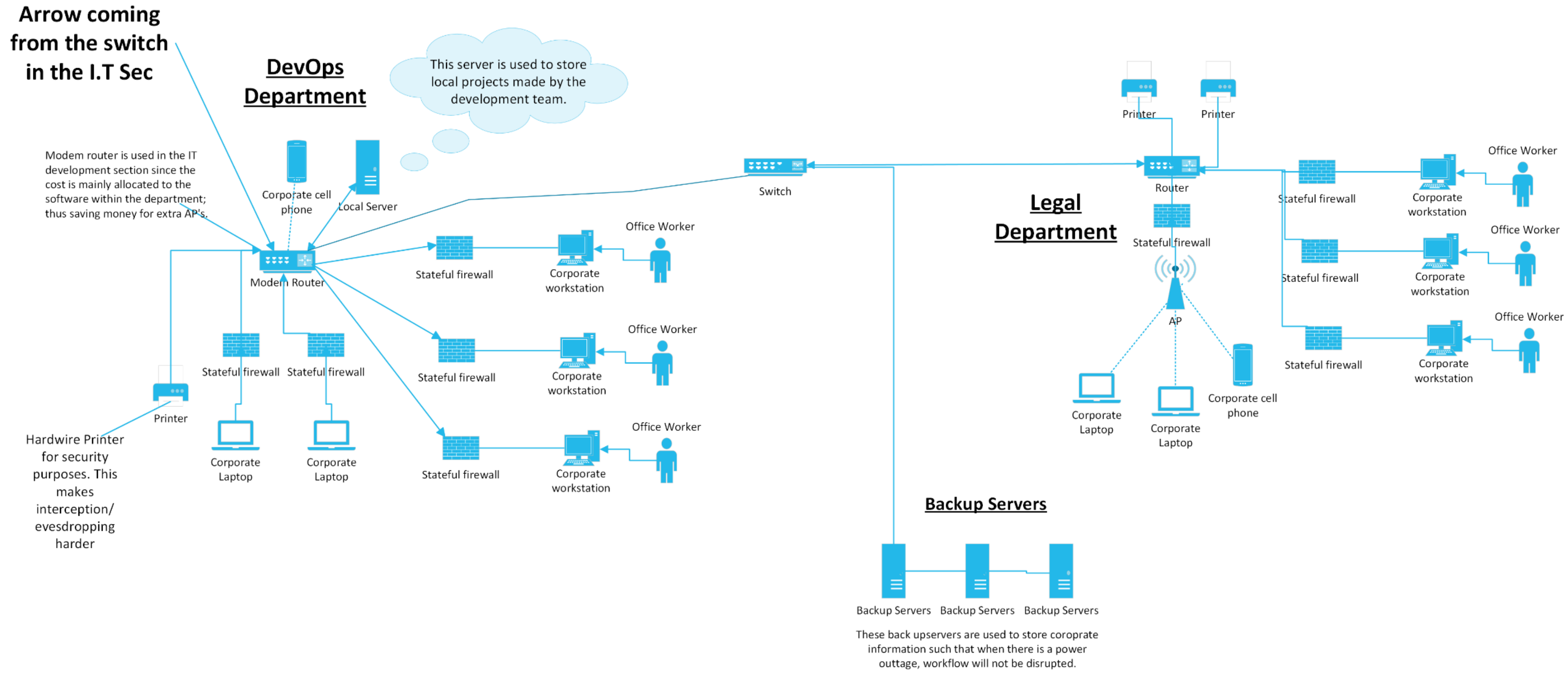
INFO 30004-18223 P01

April 14, 2023

Part 1



INFO30004 Office Network Plan (Project Part 1)



Arrow coming from the switch in the I.T Sec

DevOps Department

This server is used to store local projects made by the development team.

Modem router is used in the IT development section since the cost is mainly allocated to the software within the department; thus saving money for extra AP's.

Hardwire Printer for security purposes. This makes interception/ evesdropping harder

Legal Department

Backup Servers

These back upservers are used to store coroprate information such that when there is a power outtage, workflow will not be disrupted.

Part 2

A.10.1 Operational Procedures and Responsibilities

A.10.1.2 Change Management

Control: Changes to information processing facilities and systems should be controlled.

Control: Specific policies will be established to handle system changes, which should include complete documentation about what changes were made and who was responsible.

Testing: Changes to business systems should be made only after the necessary testing has been conducted and formal approval has been granted. Auditors should check that all changes made must be fully documented, including audit logs with all necessary information.

A.10.1.3 Segregation of Duties

Control: Duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

Control: Multiple employees or departments should be assigned to oversee critical processes.

Testing: Conduct a risk assessment to determine whether any one person in an organization is responsible for critical processes. Check to make sure that logs are stored in an un-modifiable format and that individuals of the organization cannot alter or delete these logs.

A.10.1.4 Separation of Development, Test, and Operational Facilities

Control: Development, test, and operational facilities should be separated to reduce the risks of unauthorized access or changes to the operational system.

Control: Proper software should be installed that lets users test untrusted code in a sandbox environment.

Testing: Test how separation and authorization processes are implemented to make sure that untested software is run in a controlled space. If the untested software must run on the same systems as operational facilities, ensure that there are at lease different domains in place that restrict access controls.

A.10.4 Protection Against Malicious and Mobile Code

A.10.4.1 Controls Against Malicious Code

Control: Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures should be implemented.

Control: Schedules will be put in place to ensure that software package and library versions are always up to date.

Testing: Check that software packages and library versions are updated. Test whether updates are made when needed, for example automatic updates or notifications of important updates. Make sure that users are aware of the correct ways of using web applications safely. Additionally, utilise more that one type of antivirus to increase the number of detections.

A.10.4.2 Controls Against Mobile Code

Control: Where the use of mobile code is authorized, the configuration should ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code should be prevented from executing.

Control: Establish a security policy that outlines specific configuration so that mobile code cannot execute outside of its permissions. Segregate the network to properly contain code within its needed departments.

Testing: Test that additional security settings in web browsers and other applications are in place that prevent the mobile code from executing outside of its permissions.

A.10.6 Network Security Management

A.10.6.1 Network Controls

Control: Networks should be adequately managed and controlled, in order to be protected from threats and to maintain security for the systems and applications using the network, including information in transit.

Control: Establish security controls for the network, such as data encryption, access control techniques, restricted routing per user, etc.

Testing: Test to make sure that monitoring systems are in place that can identify and alert the organization of potential breaches. Make sure that the company has sufficient incident reporting procedures for breach scenario. Make sure that protective mechanisms are in place where internal networks are exposed to public networks.

A.10.6.2 Security of Network Services

Control: Security features, service levels, and management requirements of all network services should be identified and included in any network services agreement, whether these services are provided in-house or outsourced.

Control: Establish proper failover procedures in the event of a service failure.

Testing: Test that security features from network service providers have been integrated into the company's operational procedures and security controls. Make sure that there are policies in place to regularly review and verify security features. Ensure that the organization has assessed the risks and needs of all security services.

A.10.7 Media Handling

A.10.7.1 Management of Removable Media

Control: There should be procedures in place for the management of removable media.

Control: Establish procedures for handling and managing removable media. The procedures can be general and apply to the entire network topology.

Testing: Test whether the strategies for transporting different media have acceptable protection. Check that there is a method to authorize the removal of media from the premises for transport. This authorization process should also be documented thoroughly. A risk assessment should also be done to determine the limit of the controls.

A.10.7.2 Disposal of Media

Control: Media should be disposed of securely and safely when no longer required, using formal procedures.

Control: Establish a proper procedure and policy outlining when to dispose of media, how, and whether to repair it or not.

Testing: Ensure that there are formal procedures in place for the destruction and disposal of any media that is no longer useful. Check whether there is a different policy in place for external contractors, and that there is a logging process for the media that is being disposed. Check if there is a procedure to decide whether damaged media should be destroyed or sent for repair.

A.10.7.3 Information Handling Procedures

Control: Procedures for the handling and storage of information should be established to protect this information from unauthorized disclosure or misuse.

Control: Establish proper procedures for the handling and storage of sensitive information. Ensure that employees are aware of the policy.

Testing: Test whether there are procedures in place to protect sensitive information. The procedures may depend on whether the information is recorded in video, in documents, etc. Make sure that the person responsible for the information is logged and that the information is only distributed on a need-to-know basis.

A.10.7.4 Security of System Documentation

Control: System documentation should be protected against unauthorized access.

Control: Create security controls that limit user access to system documentation either by role or department.

Testing: Test whether there are proper procedures in place for determining who is authorized to view system documentation. This may be arranged according to clearance level or role within the organization. Make sure that there is also a proper logging mechanism which records who accessed system documentation and when.

A.10.8 Exchange of Information

A.10.8.3 Physical Media in Transit

Control: Media containing information should be protected against unauthorized access, misuse, or corruption during transportation beyond an organization's physical boundaries.

Control: Establish a proper procedure detailing how physical media should be transported and protected. Ensure that the needed materials are available and that employees are trained on the process.

Testing: Test transport arrangements for physical media. For example, that tamper-proof containers are being used to transport the media, that secure postal services are used. Conduct a risk assessment of critical information and whether they should be encrypted or other protections should be used to ensure that they are tamper-safe, for example digital signatures. Finally, test that all transport activities are recorded.

A.10.8.4 Electronic Messaging

Control: Information involved in electronic messaging should be appropriately protected.

Control: Establish a policy that covers all forms of electronic messaging. Implement encryption in messaging services.

Testing: Ensure that the organization has a clear communications policy that covers all forms of electronic messaging. For example, email and instant messaging, voice calls, etc. Check whether external messaging services are allowed, and that the organization has security arrangements to handle external messages.

A.10.10 Monitoring

A.10.10.1 Audit Logging

Control: Audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring.

Control: Depending on the operating system, configure audit logging, logging schedule, and where log files are saved. Also when log files are archived.

Testing: Test that auditing logs are reviewed when necessary and that there are procedures in place for corrective actions if they need to be taken. Check that there is a schedule in place for logs to be reviewed, and that the responsibility of reviewing audit logs is rotated between multiple people.

A.10.10.2 Monitoring System Use

Control: Procedures for monitoring use of information processing facilities should be established and the results of the monitoring activities reviewed regularly.

Control: Create a well documented procedure for how monitoring activities should be implemented. This will include a list of the network's key critical areas, where more monitoring activities should be established.

Testing: Test what monitoring activities are used by the system to alert for potential breaches. Make sure that incident reporting procedures cover monitoring activities.

A.10.10.3 Protection of Log Information

Control: Logging facilities and log information should be protected against tampering and unauthorized access.

Control: Configure logging settings to prevent unauthorized access and alterations from happening.

Testing: Test that logs are stored and maintained properly, and that they cannot be altered or deleted. Make sure that no one can maliciously change the types of information recorded in the logs. Check that proper restrictions are in place to protect log information, such as prohibiting: overwriting logs without generating an alert, editing logs without authorization, and modifying the type of information that logs store.

A.10.10.4 Administrator and Operator Logs

Control: System administrator and system operator activities should be logged.

Control: Configure logging for users with system administrator or system operator privileges.

Testing: Test that the logs contain enough information and are protected from unauthorized changes and deletion. Test the mechanisms used to automatically or manually archive logs, how they can be retrieved, and how they're protected from unauthorized viewing.

A.10.10.5 Fault Logging

Control: Faults should be logged, analyzed, and appropriate action taken.

Control: Configure logging settings to detect faults.

Testing: Test that all faults are logged and that there is a process in place for handling reported faults. Make sure that there is also a process for reviewing fault logs.

A.11.2 User Access Management

A.11.2.1 User Registration

Control: There should be a formal user registration and deregistration procedure in place for granting and revoking access to all information systems and services.

Control: Establish a procedure for user registration and removal, and what information systems and services need to be configured to grant/revoke access.

Testing: Test that the process of creating and deleting User IDs is documented. Check that if employees decide to leave the company, their user IDs are immediately removed. Additionally, check to see if there is a system to track individual user IDs at any time.

A.11.2.2 Privilege Management

Control: The allocation and use of privileges should be restricted and controlled.

Control: Establish permissions for users by role. Ensure that this policy operates on a *least privilege* basis.

Testing: Test especially system administrators and engineers and those who have “super user” access. Make sure that the level of access provided to users of these rules aligns with their job purpose – meaning that they should have the bare amount of privileges needed to do their job.

A.11.2.3 User Password Management

Control: The allocation of passwords should be controlled through a formal management process.

Control: Establish a policy that covers password restrictions. Encrypt passwords and store them on a protected server.

Testing: Test that there is a policy in place that covers the use of appropriate passwords. It should cover the following: length of passwords, frequency of password changes, how common passwords between users or the same user is handled, the secure storage of passwords, and changing default passwords.

A.11.2.4 Review of User Access Rights

Control: Management should review users' access rights at regular intervals using a formal process.

Control: Establish a schedule where users' access rights are reviewed by management. This review will automatically trigger if a user's employee status changes. Create a proper procedure to revoke access rights if a user is deregistered.

Testing: Test that there are procedures regarding user access rights if a user's employment status with the organization changes. Change of employment status should trigger a review of all the access rights related to that specific user, and that any shared password with that user is changed.

A.11.3 User Responsibilities

A.11.3.1 Password Use

Control: Users should be required to follow good security practices in the selection and use of passwords.

Control: Passwords throughout the corporation especially consultants or the financial department. Additionally, we can also evaluate our servers were data is stored.

Testing: To test if users are following good security practices with passwords, we can interview managers or directors and see if they are implementing strong passwords within their departments. We can also test this by having the I.T service desk monitor any password related issues since they will get the most calls regarding this issue. Finally, we can test this by verifying that passwords are stored and transmitted correctly by checking our internal servers and doing test runs.

A.11.3.2 Unattended User Equipment

Control: Users should ensure that unattended equipment has appropriate protection.

Control: We can do a risk assessment within the HR department first, then move throughout the company.

Testing: The assessment will be to monitor and analyze how many equipment are left out on the table and who does it belong to (checking laptop number that was assignment to the individual). This way, the auditing team can gage as to how much of a loss would they take if that particular equipment was stolen (hardware & software such as sensitive information).

A.11.4 Network Access Control

A.11.4.2 User Authentication for External Connections

Control: Appropriate authentication methods should be used to control access by remote users.

Control: Check if individuals are using MFA and that their accounts are properly adjusted to conform with company policies.

Testing: To test this, we can make sure that each user is using up-to-date RSA equipment such as a software token or a hardware token by having managers call in I.T service desk (if need be) or have the employee manually check. Another step is to login employee profile portal to check MFA. This is crucial to consultants or even DevOp team within our company as those two departments contain sensitive data and is a huge risk when compromised.

A.11.4.3 Equipment Identification in Networks

Control: Automatic equipment identification should be considered as a means to authenticate connections from specific locations and equipment.

Control: The server rooms and the equipment rooms are a key candidate.

Testing: The reason being is that, some network engineers/technicians take shortcuts when setting up networks and this could mean using equipment that are either outdate, not certified, etc. To test this, the best is to review the equipment, network inventory and checking device naming convention. Additionally, performing risk assessment on all the servers are a great way to confirm if it's following properly policies and procedures as this will mitigate the potential impact of unauthorized access, data leakage, or network disruptions.

A.11.4.4 Remote Diagnostic and Configuration Port Protection

Control: Physical and logical access to diagnostic and configuration ports should be controlled.

Control: A precise way to check the server rooms and all other ported location such as ethernet hubs

Test: To test this, we have to make sure that first identify remote diagnostic and configuration ports that require protection. These include but not limited to network devices, servers, applications, etc. We should then assess the risk involved with the different types of ports that are implemented within the company and the potential impact of unauthorized access. This assessment is done company wide and configuration of the servers.

A.11.4.5 Segregation in Networks

Control: Groups of information services, users, and information systems should be segregated on networks.

Control: The area that should be looked at are the guest hotspots and enterprise users.

Test: To test this, networks between enterprise users and hotspot users (such as guests) should be separate from each other. To test this, we can try to sign into corporate hotspots and see if guests can access internal weblinks. If they can, then it will be a clear that segregation was not setup properly. Other configurations to check are if firewall rules, VLANs and ACLs are put in place by going on “blocked” sites such as pornography or malicious weblinks.

A.11.4.6 Network Connection Control

Control: For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network should be restricted, in line with the access control policy and requirements of the business applications (see 11.1).

Control: A way to test this is to make sure VPN is securely configured to conform with ISO 27001 within our organization.

Test: This is especially for the C-suite as they are always targets most of the time. We can risk assessments on remote connections by having a team that will work at a coffee shop that tries to connect back to our network or better, any third-party networks. From there we can make further analysis of the situation.

A.11.5 Operating System Access Control

A.11.5.1 Secure Log-on Procedures

Control: Access to operating systems should be controlled by a secure log-on procedure.

Control: We can implement a companywide account lockout policy.

Test: To test this, we can include, lockout duration, lockout counts (how many bad tries before account gets locked out), password expiry dates, etc. We can also review how the information is stored on the server. Once a user has securely logged on, is the information or in other words, the transmission of data are secure and follows company policies? Moreover, do they adhere to ISO 27001?

A.11.5.2 User Identification and Authentication

Control: All users should have a unique identifier (user ID) for their personal use only, and a suitable authentication technique should be chosen to substantiate the claimed identity of a user.

Control: We can check if there exists at least 1 user within the corporation that does not have a unique ID. This can be done within AD hence our I.T department will be the target for this section.

Test: One of the best and easiest way to test this is implementing MFA. MFA can come in the form of any authentication applications such as Microsoft Authenticator and Google Authenticator. We can also test this by checking in with the IT service desk to make sure that everyone has a unique ID within the company by checking for duplicates on active directory.

A.11.5.3 Password Management System

Control: Systems for managing passwords should be interactive and should ensure quality passwords.

Control: The I.T service desk department within our organization will be evaluated as they are the main department/team that does passwords resets.

Test: To test this, we must ensure that the people who are handling passwords know what to do. To conduct this test, we randomly select members on that team and ask them a few questions on secure password handling and the procedures for passwords resets. This can include, assessing employees on how to use AD to manage password resets as well as applications such as MS Azure. Other test we can perform are penetration testing or password audits to check for weak and insecure passwords. Finally, we can conduct application testing on applications that handle the password like checking if the 3rd party companies are even following ISO 27001 and maintaining up to date software.

A.11.5.4 Use of System Utilities

Control: The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled.

Control: This would be done with applications used within the HR department or accounting.

Test: Due to the sensitive nature of money, this is the best place to start since bad actors can go in and elevate privileges to change an individual’s paycheck. We need to make sure that the correct individual will get the correct access rights by using the principle of least privilege. Another check we can perform is logging and monitoring the utility applications itself. This ensures that the system logs capture necessary details, such as user identification, time and date and the utility used.

A.11.6 Application and Information Access Control

A.11.6.1 Information Access Restriction

Control: Access to information and application system functions by users and support personnel should be restricted in accordance with the defined access control policy.

Control: Each department must have a system in place to limit the amount of access. Hence the way to test would be to go department-to-department and see if anyone has more access than needed.

Test: In general, this should be tested throughout company wide as it is important to implement the correct access control policy. Our company should include role-based access control (RBAC) within every role and department as this ensures that people are not able to grant themselves elevated privileges. To test this, we can have an employee attempt to access resources or perform actions outside of their assigned role.

A.11.6.2 Sensitive System Isolation

Control: Sensitive systems should have a dedicated (isolated) computing environment.

Control: We can test this on our internal servers.

Test: We want to make sure that those systems (especially ones that contain money, or user passwords) should be hardened and secure. To do the test we must first verify that proper segmentation is in place and then check if sensitive systems are on separate subnets or if possible, create them on VLAN's. Firewalls are another great way to ensure that only necessary traffics are allowed and assess strict rules are in place. Finally, we can check that the data being transmitted are encrypted properly with industry standard encryption algorithms such as AES.

A.13 Information Security Incident Management

A.13.1.1 Reporting Information Security Events

Control: Information security events should be reported through appropriate management channels as quickly as possible.

Control: The department will be testing I.T service desk especially SLA and response times.

Test: There are several things to test here and one of them would be incident report. The focus should be mainly on the I.T service desk for our company as most people would call into that hotline. We can evaluate the SLA timings and how long it takes for a situation from start to end to be resolved. We can also conduct simulated drills such as checking if employees are able to recognize any threats and documentation and reporting skills regarding those threats. Finally, we can also evaluate the availability of reporting channels such as email, telephone lines or incident reporting systems.

A.13.1.2 Reporting Security Weaknesses

Control: All employees, contractors, and third-party users of information systems and services should be required to note and report any observed or suspected security weaknesses in systems or services.

Control: To conduct the test, we will make sure that our operations/office management/facilities/physical security are complying to company policies.

Test: These include checking in with all employees, contractors, and third-party users of information systems and that documents are signed prior to any work done so each and everyone knows what is expected of them. Each individual should review our organizations procedures and have been trained to follow the procedures. They should understand and recognize security weaknesses and the appropriate procedures for reporting them.

References

1. ISO 27001 controls – A guide to implementing and auditing by Bridget Kenyon, Published by IT Governance Publishing, ISO 27001, 2019: https://learning.oreilly.com/library/view/iso-27001-controls/9781787781467/