Case Study 1
IT Enabled Assurance Services

Scenario

GI Aircrafts Ltd., a Company engaged in the manufacturing of private jets and aviation accessories has implemented a newly conceptualized Firewall System over its legacy ERP Suite. The company has appointed an IS Auditor to audit the effectiveness of the Firewall system along with its interfaces with the ERP System. There were multiple Firewalls installed at the Company but the one placed in between the company intranet and internet is in question and have some issues.

Initially Firewall audit was not in the plan but included at the last moment at the request of the auditee. The IS Auditor included the same in the scope of the audit and finally agreed to conduct the audit. The audit of Router and Switch was also made part of audit scope.

The IS Auditor, while carrying out an IS Audit, was verifying a sample of Firewall Operation Logs and found that 2 users were constantly trying to access a particular external source which was denied by the Firewall system as per the security policy of the company. The Auditor immediately issued an audit finding and went to seek explanations from the management.

Moreover, while verifying the Firewall Operation Logs further, he observed that a particular site was not prevented by the Firewall which, ideally should be prevented as per the company's security policy. When, it came to the notice of IT Management, they immediately re-configured the Firewall and made it proper.

Discussion Points

1. What to do and how to audit firewall, router & switch during an audit process

2. Roles and responsibilities of an auditor during the audit process

3. Meaning of professional independence may also be discussed.

Questions

As an IS auditor performing the IS audit, respond to the following:

1. What should an IS Auditor do FIRST, when he observed that two users are constantly trying to access some external sources?

A. Issue an Audit Finding

B. Inform the management and expand the sample to get further evidences.

C. Seek Explanations from Management

D. Ask for clarification from the Firewall Vendor

2. An IS Auditor found one security loophole in the System. However, when the IT Management got to know about it, immediately corrected it. The IS Auditor should:

A. Include the same in his Audit Report.

B. Don't include in the Audit Report as the same is corrected.

C. Don't include in the Audit Report but discuss the same in Exit Interview for recommendation.

D. Don't include in the Audit Report and send a letter of appreciation to IT Management.

3. IS Auditor rightly found one weakness in the Firewall implementation and he recommended the name of technical expert to address the weakness. The IS Auditor has failed to maintain:

A. Professional Competence

B. Organizational Independence

C. Professional Independence

D. Personal Competence

Guidelines to Faculty

1. Students may be reminded with the roles and responsibilities of auditor

2. Basics of Firewall

3. Coverage Area: IS Auditor's Roles and responsibilities.

4. In all questions, explanation of each incorrect option may be given in a properly delineated form for easy understanding.

5. Relevant Standards / regulations / frameworks like COBIT 2019, ISO27001, and GDPR may be referred to and explained in the class while discussing the answers.

6. The faculty can teach some theory which s/he might not have covered during the class.

Practice Manual 1
Audit Planning

Learning Objective

To make an effective audit plan covering different aspects of IS Audit process - audit charter, audit planning, audit universe, risk-based audit approach, IS Audit standards, guidelines, regulations, procedures and audit reporting.

Scenario

A Bank data centre is manned by around 500 people out of whom 350 are from an outsourced company. There are 150 applications running including their core banking solution. Around 100 plus network devices like firewall, IDS, IPS, Router, Switches, Gateways etc. are there along with 500 plus high end servers. Appropriate communication lines with all required redundancies are present. The asset register maintained by the bank is not updated and not reviewed for the last two years. You will not get the idea of location and ownership of the asset from this information. There is a Network operation centre (NOC), a building management system (BMS) and a security operation centre (SOC) separately placed along the data centre. All infrastructures are managed by the outsourcing agency.

They are having issues with access control mechanism. The menu access was not controlled by any authorization matrices. Anybody can access any menu in the core banking systems. System of frisking is there but not regular. Bank's data centre needs a biometric access system, but the management feels that implementing biometric control to regulate entry of people in the data centre will be too costly and complex for them. Therefore, they plan to appoint extra security guard as a compensatory control who is instructed to allow only those people into DC who is having appropriate access card and also maintaining a register for entering access details which is supervised by the security officers. There are three cases of violation of logical access control happened in recent passed which was recorded in incident register but no follow-up action was made.

In the data centre, the testing team and development team share the same server and at times with the permission of the system administrator they access the production system and implement the program. There is no librarian to maintain version control. Change management system is also not application driven and done manually. User access review being done once in a year. DBA team controls the patch management system and the network management team takes care of anti-malware system. There are also issues with the management of backup tapes and blank tapes.

Activity-1: (Audit Plan)

You have to prepare an audit plan to cover the information system audit of this Bank data Centre with a specific goal of covering infrastructure audit and access control system (Physical & logical) including scope of the audit. There is a need to outline the audit methodology as well.

Purpose	:	E.g., Assurance of IT General Controls
Scope	:	Specific process/ controls being audited
Objectives	:	Gather, evaluate, adequate and relevant audit evidence to form an audit opinion on the reliability of information systems
Criteria	:	Regulatory requirement
		Legal Requirement
		Auditing Standards/ Frameworks
		Company's IT/IS policies
Audit dates	:	From (dd/mm/yyyy) to (dd/mm/yyyy)
Audit Team	:	Audit Leader, Auditor's name
Key Personnel	:	Audit committee chair, Process owner etc.
Audit Agenda	:	Detailed plan

Hardware and Software Requirements:

- Laptop with Windows 10 and MS-Office 2010 or office 365

Step-by-Step Activities:

- Activity to be performed in a group (4 or 5 groups depending on number of participants).
- Each group will present the output within 5 minutes presentation.

Case Study 2
CAAT

Scenario

The IS Auditor has been asked to perform preliminary work that will assess the readiness of the organization for a review to measure compliance with new regulatory requirements. These requirements are designed to ensure that management is taking an active role in setting up and maintaining a well-controlled environment, and accordingly will assess management's review and testing of the general IT controls. Areas to be assessed include logical and physical security, change management, operations control and network management, IT governance, and end-user computing. The IS auditor has been given six months to perform this preliminary work so that sufficient time should be available. It should be noted that in previous years, problems have been identified and reported in the areas of logical security and change management. Hence these areas would most likely require some degree of remediation. Logical security deficiencies noted include the sharing of administrator accounts and failure to enforce adequate controls over passwords. Change management deficiencies include improper segregation of incompatible duties and failure to document all changes. Additionally, the process of deploying operating systems update to servers was found to be only partially effective. Chief Information Officer directed the IS Auditor to report to him directly. CIO also instructed IT department to make changes in the process flow. Accordingly, the actions were taken and approval was made by the relevant process owners as well as the CIO, and then forwarded to the IS auditor for examination.

Discussion points

1. Various types of CAATs

2. Uses of CAATs in continuous audit

3. Change Management process.

Questions

1. What should IS auditor do first?

A. Perform an IT Risk assessment

B. Perform a survey audit of logical access control

C. Revise the Audit plan to focus on risk-based auditing

D. Begin testing controls that the IS Auditor feels are most critical

2. While auditing program change management, how the sample should be selected?

A. Change management documents should be selected at random and examined for appropriateness

B. Changes to production code should be sampled and traced to the appropriate authorizing documents

C. Change management documents should be selected based on system criticality and examined for appropriateness

D. Changes to production code should be sampled and traced back to system-produced logs indicating the date and time of the change.

3. The most appropriate CAAT tools the auditor should use to test security configuration settings for the entire application system is:

A. Generalised Audit Software (GAS)

B. Test data

C. Utility software

D. Expert system.

Guidelines to Faculty

1. Various types of CAATS may be explained again, if necessary

2. Change management process may also be explained.

3. Coverage area: Change Management and CAAT Tools

4. In all questions, explanation of each incorrect option may be given in a properly delineated form for easy understanding.

5. Relevant Standards / regulations / frameworks like COBIT 2019, ISO27001, and GDPR may be referred to and explained in the class while discussing the answers.

6. The faculty can teach some theory which s/he might not have covered during the class.

Practice Manual 2
IS Audit Report

Learning Objective

To write an IS Audit report, essential information, applicable general IT controls & application controls and maintaining quality.

Scenario

A Bank data centre is manned by around 400 people out of which 250 are from an outsourced company. There are 50 applications running including their core banking solution. Around 100 plus network devices like firewall, IDS, IPS, Router, Switches, Gateways etc. are there along with 500 plus high end servers. Appropriate communication lines with all required redundancies are present. The asset register maintained by the bank is not updated and not reviewed for the last two years. You will not get the idea of location and ownership of the asset from this information. There is a Network operation centre (NOC), a building management system (BMS) and a security operation centre (SOC) separately placed along the data centre. All infrastructures are managed by the outsourcing agency.

They are having issues with access control mechanism. The menu access was not controlled by any authorization matrices. Anybody can access any menu in the core banking systems. System of frisking is there but not regular. Bank's data centre needs a biometric access system, but the management feels that implementing biometric control to regulate entry of people in the data centre will be too costly and complex for them. Therefore, they plan to appoint extra security guard as a compensatory control who is instructed to allow only those people into DC who is having appropriate access card and also maintaining a register for entering access details which is supervised by the security officers. There are three cases of violation of logical access control happened in recent passed which was recorded in incident register but no follow-up action was made.

In the data centre, the testing team and development team share the same server and at times with the permission of the system administrator they access the production system and implement the program. There is no librarian to maintain version control. Change management system is also not application driven and done manually. User access review being done once in a year. DBA team controls the patch management system and the network management team takes care of anti-malware system. There are also issues with the management of backup tapes and blank tapes.

Activity - 2: (Audit Report)

For the same scenario as mentioned above, please prepare an IS Audit report. You should use the format given below and follow the guidelines as stated:

(a) Detailed Audit report should contain minimum of these columns mentioning control description, audit methodology, observations, impact, risk category (CIA), risk ranking (Very High / High / Medium / Low / Negligible) and recommendations.

(b) You should cover the aspect of organizational structure and IS security policy in the report.

(c) Your findings should have minimum of ten technical controls (you may consider controls based on the above scenario).

(d) You have to also consider applicable laws and regulations while preparing the audit report.

Some of the formats attached:

1. Format of the report
2. Content of the report
3. Coverage of various controls

Hardware and Software Requirements:

- Laptop with Windows 10 and MS-Office 2010 or office 365

Step-by-Step Activities:

- Activities to be performed in a group (4 or 5 groups depending on number of participants).
- Each group will present the output within 5 minutes presentation.

Sample Formats

1. Classification Criteria for Risk

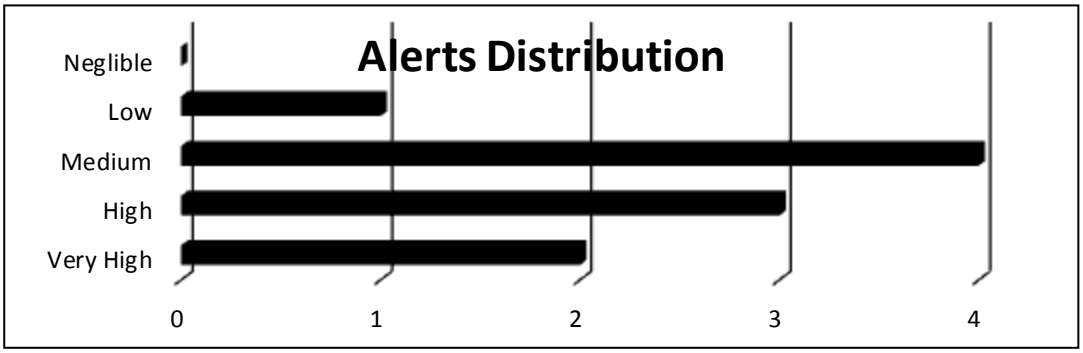
Classification	Implication
Very High	Breach could result in financial losses, or in exceptionally grave injury to individual or the organization and the business process will fail
High	Breach could result in very serious loss or injury, and the business process could fail

Medium	Breach could result in serious loss or injury, and the business process could be negatively affected
Low	Breach could result in minor loss or injury
Negligible	Breach could result in little or no loss or injury

2. Summary Table of Number of Observations classified by Risk

Audit Area / Name of Application	Very High	High	Medium	Low	Negligible	Total
Core Banking Application Name	2	4	3	1	0	10

3. Graphical Distribution of Observations



The observations have been classified into five categories based on their Risk / Implication viz., 'Very High', 'High', 'Medium', 'Low' and 'Negligible'. This classification is subjective and is based on the business criticality, desired correction timeline and on the judgment of the Business / Infosec team who performed this review.

4. Sample list of summary observations for Core Banking Application:

#	Observations	Severity
1.	Privileged access menu links were accessible from low profile user id (Junior Officer Role).	**High**
2.	There are 48 generic user available in the system with privileged access like administrator	**High**
3.	Menus could be accessed directly without any authentication.	**High**

5. Sample format of Audit Report

Sr. No.	Control Objective	Audit Procedures	Risk Ranking (VH/H/M/L/N)	Observation	Impact on C, I, A	Recommendation
1	(Issue Headings) User Access Control	(Inspection, Observations, Inquiry, Confirmation, Recalculation, re-performance, Analytical procedures)	H	It was observed that privileged access menu links for admin modules and authorization were accessible from low profile user id (e.g. clerk, Junior Officer etc.). The application doesn't validate access privileges at the server level, all the restricted pages could be accessed directly after login with low profile user id.	C I A A malicious user would gain access to privileged menus and carry out nefarious activities on the core banking application.	The application should validate the user privileges on each privileged access links before processing the requests
Evidences: <Give reference to the Screen Prints here>						

End of Document