Key steps during **risk assessment** exercise are as follows:

(i) **Determine risk assessment scope:**
Develop a brief description of the purpose of each information asset, its functionality, location, data and information criticality and sensitivity. Identify individuals using assets(s) and authentication procedures to gain access to the assets.

(ii) **Identification of threats:**
Generally, there are three general types of threats:
- **Natural** – floods, earthquakes, tornadoes, etc.
- **Human**
  - Malicious – deliberate actions such as network attacks, unauthorized access, malware upload, etc.
  - Non Malicious – unintentional acts such as data entry errors, accidental deletions, etc.
- **Environmental** – power failure, water damage, heat, etc.

(iii) **Identification of vulnerabilities:**
A vulnerability is a flaw or weakness in system security procedures, design, implementation, or internal controls that could be accidentally triggered or intentionally exploited – and result in a security breach or a violation of the system's security policy.
Generally, vulnerabilities can be classified as they relate to:
- Staff / Outsiders
- Facilities and equipment
- Applications
- Communications
- Software and operating systems

(iv) **Evaluate controls currently in place and identify gaps:**
Measures considered should combine technical, operational, and management controls to ensure adequate security.
Evaluate controls by assessing whether these are enough or appropriate to avoid the threats and vulnerabilities or at least to mitigate them as far as possible. Further gaps should be identified, otherwise.

(v) **Determine risk:**
Based on the severity and likelihood of threats, risk is determined.
Zoya Textile (ZT) should try to rank the determined risks on the basis of their significance depending upon business conditions and environment.

Key steps involved in **managing** the **above risks** are as follows:
(i) Prioritise the risk based on its impact and risk probability.
(ii) Identify controls to address the risks
(iii) Determine the cost of implementing each control and carryout a cost and benefit analysis.
(iv) Finalise the controls to be implemented.

Risks associated with outsourcing IT function and related measures:

Risks	Mitigating/avoiding measures
If the vendor leaves on short notice, the entity may not be able to cope up with the situation.	Implement a proper backup plan. Make software escrow provision. Retain key IT employees and train them to be able to continue the IT operation as per backup plan.
Entity's operations may also be affected due to inadequate business continuity planning (BCP) by the vendor.	BCP clause should be clearly defined in the SLA. The entity should periodically audit/review the BCP arrangement of the vendor.
The quality of work may not be appropriate. **OR** Inability/failure to provide agreed level of service.	Establish measurable, partnership-enacted shared goals and rewards with the vendor. Define key performance indicators, penalties on non-compliance and procedure for dispute resolution.

The deputed staff may not be as loyal, dedicated and effective as a full-time employee.	Make agreement with the vendor that : it would keep the same team of employees as far as possible. any inevitable change must be discussed and agreed with the entity before being made.
Risk of breach of confidentiality may increase.	Sign a confidentiality agreement/NDA with the vendor and all the deputed employees. Take appropriate action in case of breach of NDA. Review the controls deployed by outsourcing vendor for security and confidentiality of data.
Costs may exceed the entity's expectation.	Clear identification of costs at the start of contract. Associate payments with deliverables.

Case study: Elections of Goodland Association of Anthropologists (GAA) are due in February 2017. GAA has developed an electronic voting program (EVP) in-house. The system was developed under the supervision of its CTO. This will be the second time when EVP will be used. Previously it was used only for outstation members, who were 10% of the membership, while rest of the pooling was done manually. The system was hosted on an in-house web server which was kept live during the 8 hours of voting time. This time the local members would also be allowed to cast their votes via internet. However, in view of the suggestions received from outstation members, the voting would continue for 24 hours.

Certain up-gradation has been made in the program and the processes to meet the current needs. Members would cast their vote using their membership ID and password sent by GAA. The password will be sent to all members via email. Previously the passwords were sent through courier service.

EVP was reviewed by a reputed information security and audit firm when it was prepared before the previous elections. However no such review is planned this time because of budget constraints.

In the **absence of fresh external review**, probable **risks and their implications** are as follows:

(i) New changes made in the program might have caused some unwanted changes that may affect the processing of the program.

(ii) The programmer might have made some back door in the program to enable him to favour some candidate during result processing.

(iii) The program or the server may not be able to handle current volume of concurrent online requests and may collapse while handling peak load.

(iv) During round the clock run, there may be a period of time in which the web server will remain operational without any human monitoring or with minimum monitoring. Any malfunction of the program or server hardware during that time may prove difficult to overcome and could halt the voting process.

(v) There may be insufficient controls over members' passwords sending processes. This may lead to misuse of their passwords for fake voting.

(vi) GAA is completely transferring to online voting and apparently there is no contingency plan. If the program fails due to any reason, completion of voting process would not be possible.

Case study: Xavier Electronics Limited (XEL) has a head office and five branch offices in the country. The IT function is looked after by the CFO, with the help of programmer and two IT assistants. XEL's attendance and leave management system (ALMS) has been developed in house. The details are as follows:

- ❖ Attendance is recorded through biometric machines which are installed at each location. An employee who comes after 15 minutes of the office time is marked late by ALMS automatically. One leave is deducted against 3 late comings in a calendar month.
- ❖ ALMS allows all staff members to make a maximum of 3 time adjustments in their attendance timing in case they forget to make the attendance.
- ❖ Leaves are also applied through ALMS and are approved by departmental head through the same system.
- ❖ Each attendance machine is connected to the lane of its local office. Data recovered on each machine is transferred twice a day to a spread sheet, using a utility program provided by the attendance machine vendor.
- ❖ At head office, the data is transferred by HR manager whereas in branch offices this is done by staff designated by respective branch managers.
- ❖ Attendance data of branch offices is sent to HR manager via email next day.
- ❖ The HR manager imports the attendance data in the ALMS using another vendor provided utility program.
- ❖ Users' permissions and access rights in ALMS are set by the programmer.

Risks/weaknesses and implications	Corrective controls/measures
Data in branch offices is pulled by designated staff of the respective branch managers who may manipulate it before sending to HR Manager. Their independence is also impaired as they report to branch manager.	Data should be pulled by either designated HR staff at the branch offices or by HR Manager directly through Internet.
The designated staff keeps the data on their computers for a day before sending to HR Manager. If appropriate controls are not in place, this data may be altered by any other employee before it is sent.	Data should be transferred to HR Manager soon after it is pulled/downloaded.
The utility program stores data in a spread sheet. This makes the integrity of data extremely vulnerable as data stored in the spread sheets can be easily compromised.	The data should be stored in an un-editable or encrypted format. Preferably data should be directly transferred from the machine into the ALMS.
Three adjustments allowed under the policy could be misused and staff may use these in changing their late coming status.	Adjustments should only be allowed on the same day and with the approval of the HOD.
Users' permissions and access rights in ALMS are set by the programmer who has developed it. He may manipulate the data and erase the traces or misuse the access rights as he is the author of the program.	Users' permissions and access rights in ALMS should be set by HR Manager. The programmer should not have administrative rights with him.

Case Study: Faith Hospital is a leading healthcare provider in the city. Patients' medical records are stored on a data server which is placed in the Server Room along with application, web and backup servers. Physical access to the Server Room is controlled by biometric thumb reader. During recent IT audit of the facility, following findings have been reported:

(i) The biometric system has been deployed by Shan Technology (ST) whose owner is a friend of the IT Manager. As a gesture of goodwill, no implementation fee has been charged. ST is providing support to the hospital at a fee of Rs. 5,000 per month which was agreed in writing; however, no formal agreement exists between the hospital and ST.

(ii) The scanned thumb impressions of IT staff have been stored in the desktop system of the Network Administrator which also hosts the access control system. A copy of the thumb impressions is also stored in the laptop of the IT Manager, for backup purposes.

(iii) Access control logging is disabled on the access control system.

(iv) For providing prompt troubleshooting services, the vendor has created two IDs for its staff on the access control system. The IDs have administrative privileges and remain enabled at all times to avoid any delay in troubleshooting. Vendor's staff can remotely access the system via web interface.

(v) IT department of the hospital has 12 staff members. All of them are authorized to enter into the Server Room; however, only 10 users are registered in the access control system for accessing the Server Room.

Risk: In the absence of contractual agreement, roles and responsibilities of both sides cannot be determined clearly. Moreover, the Hospital will find it impossible to exercise its legal rights in the event that something goes wrong due to actions of the third party services provider.
Control: A formal service level agreement (SLA) should be executed between the two companies. The SLA should clearly specify roles and responsibilities of both sides.

Risk: Storage of biometric data of staff on a laptop and a desktop is highly insecure and could lead to compromise/misuse of such sensitive data. Further, any other control on the stored data is not specified. Data compromise probability would increase if it is stored in an unencrypted format.
Control: The access control system as well as biometric data should be stored on an adequately secure server within the Server Room. All such data should be secured through industry standard encryption. Moreover, the same should be removed from laptop of IT Manager. For backup purposes, copy of encrypted data may be placed in a secure place outside the Server Room, for example on a cloud, in a bank locker or in an offsite etc.

Risk: In the absence of access logs, responsibility and accountability for any untoward (Adverse) activity within Server Room cannot be fixed. Absence of such a basic control gives rise to the probability of fraudulent activity by the privileged user who is responsible for maintenance of this control.
Control: Logging should be enabled on the access control system to ensure in and out timing of all users is recorded. Periodic review of such logs should be made at an appropriate level to ensure that the logging remains enabled and detect any suspicious activity.

Risk: Continued availability of access to vendor's staff IDs is a security risk as it could be misused to manipulate access control log. Such manipulation may result in theft of an asset, concealing the access of authorized users to the facility, modifying the access log to frame some user etc. Use of these IDs through public network may also result in compromise of theses IDs and misuse by some other hacker as well.
Control: All remote access to vendor staff should either be terminated or provided through secure VPN. The IDs should be kept disabled and enabled only in case of need based on formal authorization. All vendor activities should be logged.

Risk: Since number of actual user are greater than number of registered users therefore either the door of Server Room remains open or unregistered individuals may be using the other unauthorized means of access. This also creates doubt about regular updating of the authorization.
Control: Registered IDs should be matched with current employees. Any additional ID should be deleted immediately and biometric registration of all authorized staff members should be made immediately. Periodic review of access control logs should be made at an appropriate level.

In order to carry out an **effective risk assessment for networks**, following information may be required:
(i)Detail of network topologies and network design.
(ii)Detail of significant network components (such as servers, routers, switches, hubs, firewall, modems, wireless devices etc).
(iii)Detail of interconnected boundary networks.
(iv)Network uses (including significant traffic types and main application used over the network).
(v)Network gateway to the Internet.
(vi)Names of network administrator and operator and the functions performed by them.
(vii)Names of significant groups of network users.
(viii)Procedures and standards relating to network design, support, naming conventions and data security.
(ix)Detail about network transmission media and techniques.
(x)Policies and procedures related to network risk assessment.
(xi)Helpdesk complaint log.
(xii)Detail of any potential mishap which had occurred in the past.
(xiii)Any related audit/review report.

The IT department of Boom Brokerage House (BBH) consists of five employees. BBH has a network of 100 computers. The information processing system is centralized. Internet and e-mail facility is available to selected users. You are conducting the information system audit of BBH. While interviewing users and observing various processes, you learned that:

 CEO of the company has wide experience of investment and commercial banking with working knowledge of IT.
 Sensitive data is available only to the CEO and few senior management personnel. However, only CEO has the password to open the sensitive database in edit mode. After entering the password, the necessary editing is carried out by the IT Manager.
 Domain accounts of users are created by Assistant Manager IT and their initial passwords are communicated to them verbally. Users can change their passwords whenever they want. However, they cannot repeat their last five passwords. The passwords can have a maximum of 32 characters but there is no minimum limit.
 Users can log in from any terminal and are allowed to log in from a maximum of two terminals at a time.
 Clients' data is accessible to users according to their job descriptions. Job descriptions are defined by the HR department in consultation with the relevant departmental heads and are finally approved by the CEO. Additional rights are allowed on need to have basis, on verbal instructions of the CEO.
 Administrator password of the domain is shared between IT Manager and his Assistant Manager, for maintenance and support purposes.

Risk	Consequence	Controls
Users' initial passwords are communicated to them verbally.	Passwords may be compromised and misused.	Passwords must be conveyed to the users in a sealed envelope. Users should be forced to change their passwords on their first log on.
Users can change their passwords whenever they want.	This will allow users to continue their single password by resetting five different passwords and reverting back to the old one immediately. This in turn will increase the probability of password compromise.	Users should not be allowed to change their passwords before a specified number of days. For early change of password, written request must be submitted to the system administrator.
There is no minimum limit of characters in passwords.	Users may keep blank, small or easy to guess passwords.	Minimum password length should be defined, say up to 8 characters. Passwords must meet complexity requirements.
Users are allowed to log in from two terminals at a time.	Attempts of unauthorized access to sensitive data remain undetected. Senior management users may share their passwords with their assistants/other users.	Users, specifically senior management users should not be allowed to login from more than one terminal at a time. Users should be restricted to log in from their allocated terminals only.
Additional rights are allowed to users on verbal instructions of the CEO.	Unauthorized access to sensitive data may go undetected.	Access to sensitive data in violation of defined job description should not be allowed. Changes in access rights/job description should be documented.
Only CEO has the password to open the sensitive database in edit mode.	The database may not be edited if the CEO forgets the password.	CEO should seal the database password and place it in a secure place like a bank locker. The password storage place should be known to senior management.
After entering the database password, the necessary editing is carried out by the IT Manager.	Unauthorized use of privileges by IT Manager may remain undetected.	Database log should be maintained, reviewed and signed off by a senior management member.

Domain's Administrator password is shared between IT Manager and his Assistant Manager.	Responsibility for unauthorized use of privilege may not be fixed.	□ Administrator password should not be shared under any circumstances. □ Users involve in maintenance and support may be given higher privileges to fulfill their job requirements as and when needed.
IT department is under strength.	Principle of segregation of duties may be violated.	□ Increase the strength of IT department. □ Define compensating controls where segregation of duties is not possible.

Limitations and risks associated with mobile banking services from the perspective of data and network security:

(i)Because the handset is more portable than a laptop or PC, it is also more easily lost.
(ii)The limited keypad functionality of standard handsets may effectively limit the choice of PINs, and/or resulting in PINs which can be compromised.
(iii)Encryption in mobile communication is not necessarily end-to-end, creating vulnerabilities at various points where data can be intercepted and read by third parties.
(iv)Physical access to SIM card may reveal subscriber key.
(v)Physical or logical access to Mobile Network Operator facilities by unauthorized person may give access to mobile banking user's transaction data.
(vi)Mobile station may not guarantee its communication with right recipient and is vulnerable to attacks like active identity caching and passive identity caching.
(vii)Mobile banking service may be suspended due to breakdown of telecommunication network.