Incident 6
In the design department of organisation XYZ Ltd., the auditor reviewed the list of five information security risks identified for that department. Auditor asked if the methods to treat these risks were documented. The design director replied that such documents were not prepared, as he believed that it would suppress the creativity of his people.

Incident 7
The auditor noticed a new software is being used in the Customer service department of organisation ABC Ltd. The software tracks and analyzes customer complaints. The auditor had previously reviewed the procedure on the introduction of new software in the organisation. The procedure states that "No software must be used within the organization without the approval of the IT Manager".

Incident 8
The auditor was checking the terms and conditions of the personnel employment contracts employed with organisation PQR Ltd. He noticed that the work contract with the Joe Kleen, the office cleaner, did not contain any responsibilities for information security nor was there any other document stipulating it. When asked, the auditor is told that the Joe Kleen is the brother-in-law of the General Manager of the company and they were good friends at primary school.

Incident 9
In the Statement of Applicability documented by Medical Laboratory ASD Ltd. which specializes in blood testing, the auditor notices that the control on outsourcing is identified as non-applicable by them. The auditor is told that the medical waste is collected by the Municipality once a week.

Incident 10
In the Information Security Department of ABC Ltd., the auditor reviewed 10 audit reports that contained a total of 24 non-conformances raised in the audit. None of the Non conformances raised had any annotation to indicate the identified cause of non-conformance. The auditor also noted that the actions proposed for 21 non-conformances, dealt with the symptoms only and did not address the causes of nonconformance. 8 of the non-conformances were recurrences of previously identified problems. The procedures covering corrective actions and audit activity did not require conducting an investigation into the causes for nonconformances and recording the results thereof, nor did they clearly require that corrective actions needed to eliminate the cause of nonconformances.

The auditor discussed his observations with the Security Manager and realised that the latter did not quite understand the difference between 'curative measures' and 'corrective actions' and believed in a 'quick fix' remedy.

CORRECTIVE ACTION REQUEST				
Company: XYZ Ltd.	Date:		NCR Number: 1	
Auditor: A U Ditor	Auditee: A U Ditee			
Standard & Clause : ISO 27001:2013 A 11.1.1	Major:		Minor	

Auditors Report of non-conformance

ISO 27001:2013 clause A.11.1.1 requires Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.

While auditing the Server room, it was discovered that two personnel were in the room, were not issued the required card keys for entry into this area. Further investigation showed that they did not have the clearance to be in this room.

Signed: A U Ditor
Date:

Cause & Proposed Corrective Action:

Cause : Personnel were not aware of the requirements to be followed when accessing the server room.

Corrective Action : Personnel will be reminded of the importance of checking security clearances of personnel for activities being done in secure areas.

Proposed by : Security Manager

Proposed Completion Date:

DATE: **SIGNATURE**

Corrective Action Review:

Signed:

CORRECTIVE ACTION REQUEST				
Company: XYZ Ltd		Date:		NCR Number: 3
Auditor: A U Ditor		Auditee: A U Ditee		
Standard & Clause ISO 27001:2013 A 12.3.1	Major:		Minor	

Auditors Report of non-conformance

ISO 27001:2013 clause A.12.3.1 requires "Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy."

Whilse auditing the IT Department it was found that although backup copies of information were being taken and kept, they were never tested.

Signed: A U Ditor
Date:

Cause & Proposed Corrective Action:

Root cause : IT Department was not aware of the requirement of testing the backup copies being taken. The procedure for taking backups did not cover testing of the backups

Corrective Action : The backup procedure has been revised to include the requirement of testing the backups on a defined frequency. From now on all backups will be regularly tested in accordance with the backup procedure, once a month and records will be created of all backup testing being done.

Proposed by : IT Manager

Proposed Completion Date:

DATE: **SIGNATURE**

Corrective Action Review:

Signed:
Date:

CORRECTIVE ACTION REQUEST				
Company: XYZ Ltd.		Date:		NCR Number: 5
Auditor: A U Ditor	Auditee: A U Ditee			
Standard & Clause ISO 27001:2013 Clause 7.2	Major:		Minor	

Auditors Report of non-conformance

ISO27001:2013 Clause 7.2 requires

"The organization shall:

a) determine the necessary competence of person(s) doing work under its control that affects its information security performance;

b) ensure that these persons are competent on the basis of appropriate education, training, or experience;

c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken

During the audit of Human Resources it was discovered that several personnel had been recommended for training in various aspects of information processing, but that the training had been refused by top management.

Signed:
Date:

Cause & Proposed Corrective Action:

Cause : Due to unavailability of funds, top management deferred the trainings

Corrective action : As soon as funds are available, the identified training will be provided.

Proposed by : Security Manager

Proposed Completion Date:

DATE: **SIGNATURE**

Corrective Action Review:

Signed:
Date:

CORRECTIVE ACTION REQUEST				
Company: XYZ Ltd.		Date:		NCR Number: 6
Auditor: A U Ditor	Auditee: A U Ditee			
Standard & Clause ISO 27001:2013 A 9.3	Major:		Minor	

Auditors Report of non-conformance

ISO 27001:2013 clause A.9.3 requires "Users shall be required to follow the organization's practices in the use of secret authentication information."

During the audit of the main data processing area, it was discovered that the passwords for several accounts were written on notes found around work stations.

Signed:
Date:

Cause & Proposed Corrective Action:

Cause : Due to various passwords required to be maintained for different softwares, employees were writing their passwords on notes for easy reference. Employees were not aware of the risks in writing their passwords on notes.

Corrective action : All the notes containing passwords will be removed and destroyed. All personnel will be warned that it is a disciplinary offence to write down passwords, and action will be taken over any future breach of security in this area.

Proposed by : Security Manager

Proposed Completion Date:

DATE: **SIGNATURE**

Corrective Action Review:

Signed:
Date:

CORRECTIVE ACTION REQUEST				
Company: XYZ Ltd.		Date:		NCR Number: 7
Auditor: A U Ditor	Auditee: A U Ditee			
Standard & Clause ISO 27001:2013 A 12.2.1	Major:		Minor	

Auditors Report of non-conformance

ISO 27001:2013 clause A.12.2.1 requires "Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness."

During the audit of the IT department, it was discovered that the anti-virus software in place had not been updated for at least 6 months, may be even longer. The latest version of the antivirus software is also not updated in the end users machines.

Signed:
Date:

Cause & Proposed Corrective Action:

Cause : As the license with the antivirus software provider has expired, the anti-virus software definitions were not being updated.

Corrective Action : The contract with the service provider is extended for the next year. The virus protection software will be updated immediately on all the end user machines.

Proposed by : Security Manager

Proposed Completion Date:

DATE: **SIGNATURE**

Corrective Action Review:

Signed:
Date:

CORRECTIVE ACTION REQUEST				
Company: XYZ Ltd.		Date:		NCR Number: 8
Auditor: A U Ditor	Auditee: A U Ditee			
Standard & Clause ISO 27001:2013 clause 10.1	Major:		Minor	

Auditors Report of non-conformance

ISO 27001:2013 clause 10.1 requires "When a nonconformity occurs, the organization shall

b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by:

1) reviewing the nonconformity;

2) determining the causes of the nonconformity; and

3) determining if similar nonconformities exist, or could potentially occur;

c) implement any action needed "

During review of the internal audit program, the auditor noted, in many cases, actions taken in response to nonconformities only corrected the immediately identified symptom(s) without removing the cause of the problem.

Signed:
Date:

Cause & Proposed Corrective Action:

Cause : The procedure for internal audit did not require conducting an investigation into the root cause of the non conformities. The audit team and the department managers were not aware of root cause analysis.

Corrective Action : The security manager will review and amend the procedures for internal audits and corrective actions to make it clear that root cause analysis is necessary and that corrective actions must address the root causes of the problems. She will also support implementation of the revised procedures by conducting additional training for the audit team and department manager to cover the nonconformity investigation, root cause analysis, developing of corrective actions and evaluation-of-effectiveness of corrective action.

Proposed Completion Date:

Corrective Action Review:

Signed:
Date:

CORRECTIVE ACTION REQUEST				
Company: XYZ Ltd.	Date:		NCR Number: 9	
Auditor : A U Ditor	Auditee: A U Ditee			
Standard & Clause ISO 27001:2013 A 6.1.1	Major:		Minor	

Auditors Report: of non-conformance

ISO 27001:2013 clause A.6.1.1 requires "All information security responsibilities shall be defined and allocated."

During the audit it was discovered that information security roles and responsibilities were well documented for employees, but did not exist at all for contractors or third party users.

Signed:
Date:

Cause & Proposed Corrective Action:

Cause : Not aware of requirement of roles and responsibilities to be documented for contractors and third party users.

Corrective Action : Top management shall define the roles and responsibilities for contractors and third party users if and when a security breach associated with this lack of control is identified.

Proposed Completion Date:

DATE: **SIGNATURE**

Corrective Action Review:

Signed:
Date:

CORRECTIVE ACTION REQUEST				
Company: XYZ Ltd.		Date:	NCR Number: 10	
Auditor: A U Ditor	Auditee: A U Ditee			
Standard & Clause ISO 27001:2005 A 11.2.5	Major:		Minor	

Auditors Report: of non-conformance (requirement & evidence)

ISO 27001:2013 clause A.11.2.5 requires "Equipment, information or software shall not be taken off-site without prior authorization".

During the audit, some items of equipment identified on the assets register (laptops - 3 nos) could not be located. It was later discovered that they had been taken by a sales team visiting a prospective customer. None of the team had prior permission to take the laptops off-site.

Signed: A U Ditor
Date:

Cause & Proposed Corrective Action:

Cause : Ignorance of the sales team of the requirement.

Corrective Action : The sales team will be informed of the requirement to get prior permission to take equipment off-site. The requirement shall be reinforced for all employees, and it will now be a disciplinary offence not to comply with this requirement.

Proposed by : Security Manager

Proposed Completion Date:

DATE: **SIGNATURE**

Corrective Action Review:

Signed:
Date: