

ISO / IEC 27001:2022 Lead Implementer Course

Exercise 25:

Instructions:

- Corrective actions Process Management Review Process
- Considering your company as a case study for ISO 27001:2022 implementation
- Take a blank piece of a white paper, write (by-hand). Do not copy or review; trust your memory.
- Take a clear snapshot of the paper, create a folder on Google Drive 'ISO 27001:2022 Lead' and save the snapshot (If you did not create in Exercise A)
- Send me the link to access the snapshot file on your Google drive via Facebook Messenger.
- Facebook link: facebook.com/profile.php?id=61556175711538

Follow me on my social media platforms to learn more about ISO / IEC 27001:2022 via my posts:

- LinkedIn: linkedin.com/in/john-kimani-13831329b
- Facebook: facebook.com/profile.php?id=61556175711538
- Quora: quora.com/profile/The-Cyber-Hackers-Diary
- Pinterest: pinterest.com/hackersdiary
- YouTube: www.youtube.com/@CyberHackersDiary



@ The Cyber Hacker's Diary

Corrective Actions Process Management Review for Scoopid Boy Animations Inc.

Objective:-

Ensure effective resolution of non-conformities in our ISMS as per ISO/IEC 27001:2022

Scope:-

Applies to all departments and activities related to the ISMS non-conformities.

Procedure

1. Identification

- Sources:- Audits, incidents, risk assessments
- Report:- Non-conformity Report Form (NCRF) to Information Security Manager within 24 hours.

2. Investigation

- Lead:- Information Security Manager
- Steps:-
 - Determine scope and impact
 - Root cause analysis
 - Document Findings

3. Corrective Action Plan (CAP)

- Includes:-
 - Non-conformity description
 - Root cause
 - Actions, responsible persons, timeline resources.
- Developed by:- Information Security Manager and relevant Stakeholders.

4. Implementation

- Responsible:- Assigned individuals
- Monitored by:- Information Security Manager
- Document:- All actions recorded.

5. Verification

- Method:- Follow-up audits
- Verified by:- Internal audit team.
- Criteria:- Non-recurrence and root cause addressed.

6. Management Reviews

- Frequency:- Quarterly
- Participant:- Senior management, Information Security Manager
- Agenda:- Review non-conformities, CAP effectiveness, improvements, recommendations
- Document:- Meeting minutes

Roles & Responsibilities

- Employees:- Report non-conformities
- Information Security Manager:- Oversee process
- Department Heads:- Assist in CAP implementation.
- Internal Audit Team:- Verify corrective actions.

Records

- NCRFs
- CAPs
- Follow-up audit reports
- Management review minutes.

Conclusion:-

Stupid Boy Animations Inc. is committed to continual improvement of its ISMS through effective management of corrective actions.