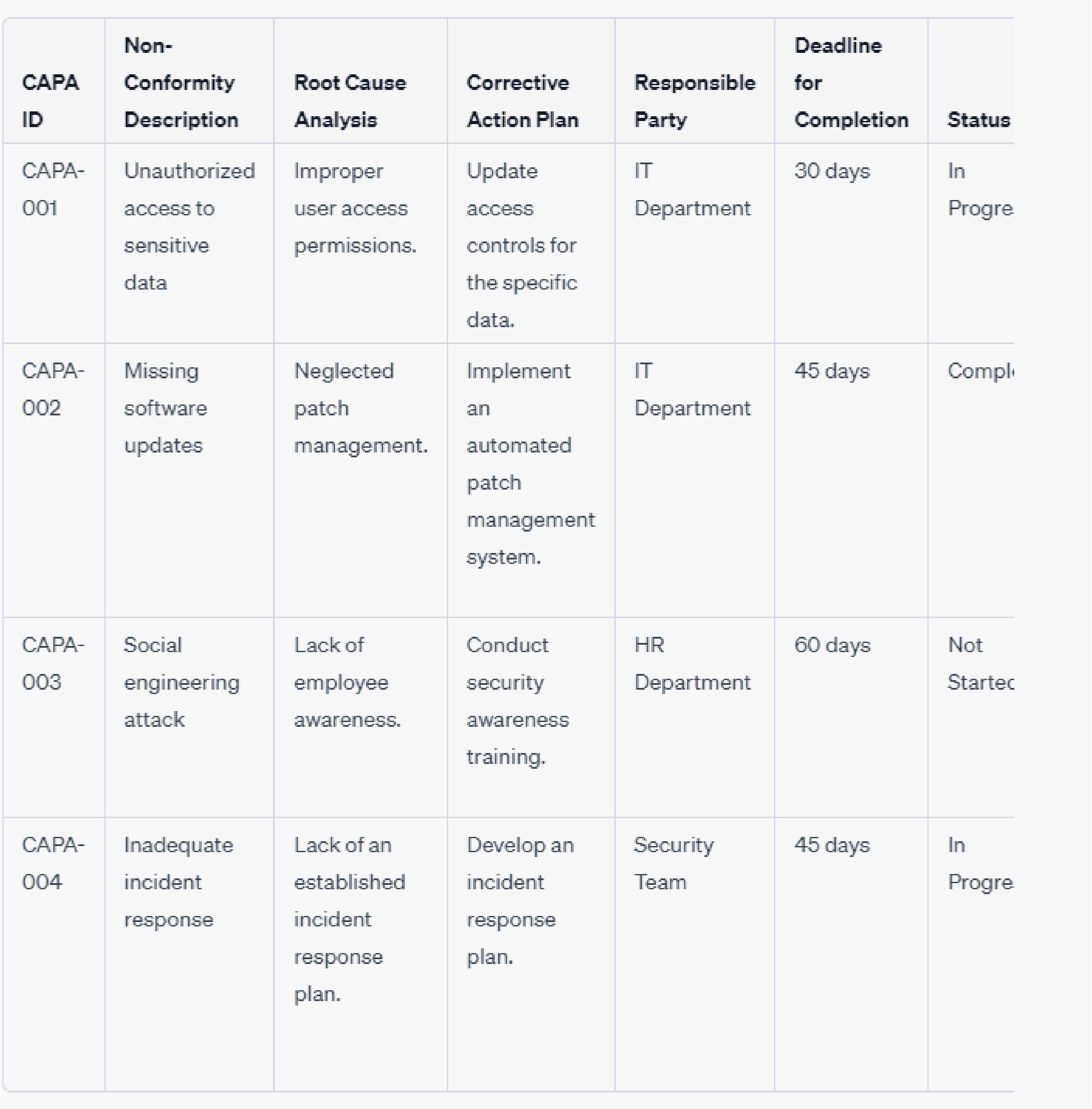
ISO 27001 LEAD IMPLEMENTER
DOWNLOADABLE TEMPLATE

Sample CAPA Table:



CAPA ID	Non-Conformity Description	Root Cause Analysis	Corrective Action Plan	Responsible Party	Deadline for Completion	Status
CAPA-001	Unauthorized access to sensitive data	Improper user access permissions.	Update access controls for the specific data.	IT Department	30 days	In Progre
CAPA-002	Missing software updates	Neglected patch management.	Implement an automated patch management system.	IT Department	45 days	Compl
CAPA-003	Social engineering attack	Lack of employee awareness.	Conduct security awareness training.	HR Department	60 days	Not Startec
CAPA-004	Inadequate incident response	Lack of an established incident response plan.	Develop an incident response plan.	Security Team	45 days	In Progre

In this sample CAPA table:

- **CAPA ID**: A unique identifier for each corrective and preventive action.

- **Non-Conformity Description**: A brief description of the non-conformity or issue.
- **Root Cause Analysis**: The analysis of the root causes or underlying factors contributing to the non-conformity.
- **Corrective Action Plan**: The specific actions to rectify the non-conformity.
- **Responsible Party**: The individual or department responsible for implementing the action.
- **Deadline for Completion**: The date by which the action should be completed.
- **Status**: The current status of the action (e.g., Not Started, In Progress, Completed).
- **Verification Plan**: The plan for verifying that the action has been effective.
- **Preventive Action Plan**: Actions taken to prevent a similar issue from occurring in the future.

This table helps organizations track and manage CAPA activities systematically, ensuring that non-conformities are addressed and future issues are prevented.

In conclusion, effective management of non-conformities and the implementation of corrective actions are integral components of ISO 27001:2022. As a Lead Implementer, mastering these processes is crucial for maintaining the effectiveness of the ISMS, preventing security incidents, and fostering a culture of