ISO/IEC 27001 – Annex A Control Review (Mock)

Prepared by: James Gladden
Objective: To review the design and implementation status of selected Annex A controls for audit readiness.

A.5.1 – Information Security Policies

Control Objective: Management direction and support for information security.
Observed State: Policy drafted and communicated informally.
Implementation Status: Partially Implemented
Gap Identified: Formal approval and periodic review not documented.

A.6.1 – Information Security Roles and Responsibilities

Control Objective: Defined roles and responsibilities for information security.
Observed State: Responsibilities understood but not formally assigned.
Implementation Status: Partially Implemented
Gap Identified: Lack of documented role ownership.

A.8.2 – Privileged Access Management

Control Objective: Restriction and management of privileged access rights.
Observed State: Privileged access exists with limited review.
Implementation Status: Partially Implemented
Gap Identified: No periodic access review process.

A.12.1 – Operational Procedures and Responsibilities

Control Objective: Documented operating procedures for IT operations.
Observed State: Procedures followed but not formally documented.
Implementation Status: Partially Implemented
Gap Identified: Operational procedures not standardized.

A.16.1 – Information Security Incident Management

Control Objective: Consistent and effective handling of security incidents.
Observed State: Incident handling informal and undocumented.
Implementation Status: Not Implemented
Gap Identified: No formal incident response documentation.

Overall Assessment

The review identified foundational awareness of information security requirements; however, formal documentation, ownership, and periodic review processes require improvement to meet ISO/IEC 27001 expectations.

Recommendations

Recommendations include formalizing information security policies, assigning control ownership, documenting operational and incident response procedures, and establishing periodic control reviews.