<Organization Name>

**Gap Assessment**

|  |  |
| --- | --- |
| **Standard** | ISO/IEC 27001:2022 |
| **Version** | <Version No> |
| **Effective Date** | <Date> |
| **Reviewed Date** | <Date> |
| **Next Review Date** | <Date> |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Prepared By** | **Approved By** | **Changes/Notes** |
| <version No> | <DD/MM/YYYY> | <Name> | <Name> | *Initial Version* |

|  |  |  |
| --- | --- | --- |
| **Distribution List** | | |
| **Recipient Name** | **Department** | **Distribution Date** |
| <Name> | <Department> | <DD/MM/YYYY> |
| <Name> | <Department> | <DD/MM/YYYY> |
| <Name> | <Department> | <DD/MM/YYYY> |

# Information Security Management System (ISMS) – Requirements

The following table assesses the current state of the organization’s information security management system (ISMS) against the requirements of ISO 27001. Each clause and control will be evaluated, and gaps will be identified for future actions.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ISO 27001 Clause** | **Requirement** | **Requirements Met** | **Gap Identified** | **Action Needed** | **Priority** |
| Clause 4: Context of the Organization | Define the scope of ISMS | Yes/No | Yes/No | <Action> | High/Medium/Low |
| Clause 5: Leadership | Demonstrate leadership commitment | Yes/No | Yes/No | <Action> | High/Medium/Low |
| Clause 6: Planning | Conduct risk assessment and establish objectives | Yes/No | Yes/No | <Action> | High/Medium/Low |
| Clause 7: Support | Ensure proper resources and competence | Yes/No | Yes/No | <Action> | High/Medium/Low |
| Clause 8: Operation | Implement and operate the ISMS | Yes/No | Yes/No | <Action> | High/Medium/Low |
| Clause 9: Performance Evaluation | Monitor, measure, and audit the ISMS | Yes/No | Yes/No | <Action> | High/Medium/Low |
| Clause 10: Improvement | Continual improvement of ISMS | Yes/No | Yes/No | <Action> | High/Medium/Low |

# Controls Gap Assessment

This section evaluates the specific controls required by Annex A of ISO 27001.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ISO 27001 Control** | **Description** | **Requirements Met** | **Gap Identified** | **Action Needed** | **Priority** |
| A.5 Organizational Controls | Controls to manage and support the information security program within the organization. | Yes/No | Yes/No | <Action> | High/Medium/Low |
| A.5.1 Information Security Policies | Define and publish security policies. | Yes/No | Yes/No | <Action> | High/Medium/Low |
| A.5.2 Information Security Roles and Responsibilities | Define roles and responsibilities for security management. | Yes/No | Yes/No | <Action> | High/Medium/Low |
| A.6 People Controls | Controls to manage risks related to human resources. | Yes/No | Yes/No | <Action> | High/Medium/Low |
| A.6.1 Screening | Ensure screening and background checks for employees. | Yes/No | Yes/No | <Action> | High/Medium/Low |
| A.6.2 Information Security Awareness and Training | Employee awareness and ongoing security training programs. | Yes/No | Yes/No | <Action> | High/Medium/Low |
| A.7 Physical Controls | Controls to prevent unauthorized access to physical locations and equipment. | Yes/No | Yes/No | <Action> | High/Medium/Low |
| A.7.1 Physical Security Perimeter | Physical protection around sensitive areas. | Yes/No | Yes/No | <Action> | High/Medium/Low |
| A.8 Technological Controls | Controls to manage and secure the use of technology. | Yes/No | Yes/No | <Action> | High/Medium/Low |
| A.8.1 Identification and Authentication | Ensuring secure user authentication processes. | Yes/No | Yes/No | <Action> | High/Medium/Low |
| A.8.2 Cryptography | Controls for encryption and protection of sensitive data. | Yes/No | Yes/No | <Action> | High/Medium/Low |
| A.8.3 Access Control | Controls to ensure secure access to systems and data. | Yes/No | Yes/No | <Action> | High/Medium/Low |
| A.8.4 Secure System Development | Ensure secure software development practices. | Yes/No | Yes/No | <Action> | High/Medium/Low |
| A.8.5 Logging and Monitoring | Controls for logging and monitoring system activities. | Yes/No | Yes/No | <Action> | High/Medium/Low |
| A.8.6 Vulnerability Management | Controls to identify and remediate vulnerabilities. | Yes/No | Yes/No | <Action> | High/Medium/Low |
| A.8.7 Information Backup | Controls to ensure data backup and recovery. | Yes/No | Yes/No | <Action> | High/Medium/Low |
| A.8.8 Network Security | Ensure the security of network infrastructure. | Yes/No | Yes/No | <Action> | High/Medium/Low |
| A.8.9 Security Testing | Conduct regular security testing and assessments. | Yes/No | Yes/No | <Action> | High/Medium/Low |

# Gap Assessment Results

|  |  |  |  |
| --- | --- | --- | --- |
| **Area of Standard** | **Requirements in Section** | **No. of Requirements Met** | **Percentage Conformant** |
| 4 Context of the Organization | 4 | <Insert> | <Insert> |
| 5 Leadership | 6 | <Insert> | <Insert> |
| 6 Planning | 16 | <Insert> | <Insert> |
| 7 Support | 8 | <Insert> | <Insert> |
| 8 Operation | 4 | <Insert> | <Insert> |
| 9 Performance Evaluation | 6 | <Insert> | <Insert> |
| 10 Improvement | 2 | <Insert> | <Insert> |
| A.5 Organizational Controls | 37 | <Insert> | <Insert> |
| A.6 People Controls | 8 | <Insert> | <Insert> |
| A.7 Physical Controls | 14 | <Insert> | <Insert> |
| A.8 Technological Controls | 34 | <Insert> | <Insert> |
| Total | 139 | <Insert> | <Insert> |

# Summary of Key Gaps and Action Plan

### Major Gaps Identified

1. <Summary of gap>
2. <Summary of gap>
3. <Summary of gap>

### Action Plan

* Assign responsible persons for each identified action.
* Establish timelines for addressing gaps.
* Monitor progress and reassess gaps.

|  |  |
| --- | --- |
| **Approved By** | |
| Name | <Name> |
| Title | <title> |
| Approved Date | <date> |