



**MSECB Certification – ISO/IEC 27001:2013\_ISO/IEC 27701:2019**

*Management System Audit Report*

*of* **Company ABC**



**DISTRIBUTION**

The content of this report must not be disclosed to a third party without the agreement of the MSECB Client.

**DISCLAIMER**

This report has been prepared by MSECB in respect of a Client's application for assessment by MSECB. The purpose of the report is to verify the Client's conformance with the management system standard(s) or other criteria specified. The content of this report applies only to matters, which were evident to MSECB at the time of the audit within the audit scope. MSECB does not warrant or otherwise comment upon the suitability of the contents of the report or the certificate for any particular purpose or use. MSECB accepts no liability whatsoever for consequences to, or actions taken by, third parties as a result of or in reliance upon information contained in this report or certificate.

This audit is based on a sampling process of the available information and the auditors nor MSECB can guarantee that all, if any, non-conformities have been discovered.

1. Audit information 4

1.1. Organization information 4

1.2. Audit information 4

1.3. Audit Scope 4

2. Audit preparation and methodology 4

2.1. Audit objectives 4

2.2. Audit criteria 4

2.3. Audit methodology 4

2.4. Previous audit results 4

2.5. Audit planning 4

2.6. Key people interviewed 4

2.7. MSECB complaint and appeal process 4

3. Significant audit trails followed 4

4. Audit findings 4

4.1. Audit finding definition 4

4.2. Major nonconformities (see also Annex A) 4

4.3. Minor nonconformities (see also Annex A) 4

4.4. Observations 4

4.5. Opportunities for improvement 4

4.6. Agreed follow-up activities 4

4.7. Uncertainty / obstacles that could affect the reliability of audit conclusions 4

4.8. Unresolved diverging opinions between the audit team & auditee 4

5. Audit conclusions and audit recommendation 4

5.1. System management conformance and capability 4

5.2. Audit conclusions 4

5.3. Recommendation 4

6. Annex A: Nonconformity report 4

6.1. Nonconformity Report 4

7. Annex B: Certification Information 4

8. Annex C: Surveillance Plan 4

Place, and Date

To Mr. John Smith (example)

Organization Name

I have audited the Management System (MS) of Company ABC (Organization Name) from May 12th to May 15th 2017. The main objective of this audit was to assess if the MS has been successfully implemented and effecticve, as well as to evaluate the conformance of the organization to the ISO/IEC 27001:2013 and ISO/IEC 27701:2019 requirements. Based on these assessments and evaluations, a decision has been made whether or not to recommend your organization for certification against ISO/IEC 27001:2013 and ISO/IEC 27701:2019.

The audit team has conducted the audit based on the organization’s defined processes in correspondence with the audit plan. The audit conducted by a professional team was a process-based audit with a focus on the significant aspects, risks and objectives. The audit was conducted in accordance with the ISO 19011 and ISO 17021 standards, which are accepted worldwide. Those standards require our audit team to plan and perform the audit in order to acquire reasonable assurance whether your company’s management system is effective and all requirements of ISO/IEC 27001:2013 and ISO/IEC 27701:2019 have been met.

During the course of the audit process, the management system has proven overall conformity with the requirements of the standard. The audit team has concluded that your organization has established and preserved its management system according to the requirements of the standard and proved the ability of the system to consistently achieve the approved requirements for the services within the scope of your organization and also on your organization’s policy and objectives.

The conformance level with the standard can still be improved despite the fact that no nonconformities or only one nonconformity has been found during the audit. This was a sample based audit. Nonconformities and other opportunities for improvement can still be found in the audited and non-audited areas.

Referring to the results of the audit process and the demonstration of the organization’s development and maturity, the audit team recommends that your organization’s management system should be certified to ISO/IEC 27001:2013 and ISO/IEC 27701-2019.

Name Surname

Audit team Leader

# Audit information

## Organization information

|  |  |
| --- | --- |
| Company name: |  |
| Contract number: |  |
| Phone number: |  |
| Website: |  |
| Total number of employees: |  |
| Total number of employees within the scope:  Please provide justification for the employees that are not included in the certification scope. |  |
|  | |
| Contact name: |  |
| Contact email: |  |
| Contact phone: |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Sites: | | | | | |
| **Site #** | **Street Address** | **City** | **State, Province, Country** | **Zip Code** | **# of Employees** |
| 1 (main) |  |  |  |  |  |
| 2 |  |  |  |  |  |
| 3 |  |  |  |  |  |
| 4 |  |  |  |  |  |

## Audit information

|  |  |  |
| --- | --- | --- |
| Audit standard(s): |  | |
| Audit type: | Initial Audit | Surveillance 1 |
| Recertification | Surveillance 2 |
| Other: | |
| Date(s) of audit(s): |  | |
| Duration: |  | |
| Audit team leader: |  | |
| Additional team member(s): |  | |
| Additional attendees and roles: |  | |

|  |  |
| --- | --- |
| **Site #** | **Sites Audited** |
| 1 (main) |  |
| 2 |  |
| 3 |  |
| 4 |  |

## Audit Scope

|  |  |
| --- | --- |
| Certification audit scope: |  |
| Date and version of scope statement: |  |
| Has scope changed since last audit? |  |
| All scope exclusions are appropriate and justified:  Important Note\* Excluded clauses in the audited Management System shall be put in the certificate |  |

# Audit preparation and methodology

## Audit objectives

The main purpose of this audit is to evaluate the implementation and effectiveness of the Information Security Management (ISMS) and Privacy Information Management including evaluation of conformity to the requirements of ISO/IEC 27001:2013 and ISO/IEC 27701-2019.

The specific objectives of this audit are to confirm that:

* The organization has determined the boundaries and applicability of the MS in scope;
* The management system conforms with all the requirements of the audit standards (Clause 4 to 10 of ISO/IEC 27001:2013 and clause 5 to 8 of ISO/IEC 27701-2019);
* The management system conforms with all applicable legal and regulatory requirements;
* The management system is capable of achieving the organization’s policies objectives
* The organization has established, implemented, maintained and continually improved its MS, including the processes needed and their interactions, in accordance with the requirements of the ISO/IEC 27001:2013 and ISO/IEC 27701-2019*.*

## Audit criteria

The audit criteria (set of requirements) for this audit are all normative clauses of ISO/IEC 27001:2013 and ISO/IEC 27701-2019.

* Clause 4 – Context of the organization
* Clause 5 – Leadership/PIMS-specific requirements related to ISO/IEC 27001
* Clause 6 – Planning/PIMS-specific guidance related to ISO/IEC 27002
* Clause 7 – Support/Additional ISO/IEC 27002 guidance for PII controllers
* Clause 8 – Operation/Operation of the service management system/Additional ISO/IEC 27002 guidance for PII processors
* Clause 9 – Performance Evaluation
* Clause 10 – Improvement
* Annex A – Control objectives and controls/PIMS-specific reference control objectives and controls (PII Controllers)
* Annex B – PIMS-specific reference control objectives and controls (PII Processors)
* 11 – Additional requirements
  + Use of logo and trademark
  + List of documents included in the audited MS

## Audit methodology

[Please explain the methodology used by the audit team to perform this audit, similar to the sample below]

The audit team has conducted a process-based audit focusing on the significant aspects, risks and objectives. The auditors have used audit procedures to collect evidence in sufficient quantity and quality to validate the conformity of the management system of the organization. The use of audit procedures in a systematic way reduces the audit risk and reinforces the objectivity of the audit conclusions.

The audit team has used a combination of evidence collection procedures to create their audit test plan. The audit methods used consisted of interviews, observations of activities, review of documentation and records, technical tests and analysis of sampling.

The analysis procedure allows the audit team to draw conclusions concerning a whole by examining a part. It allows the auditor to estimate characteristics of a population by directly observing a part of the whole population. The sampling method used during this audit was a systematic sampling (or interval sampling) technique with a margin error of 3 to 5 %.

Technical tests, including testing of the effectiveness of a process or control have not been performed by the auditors themselves. The operations have always been performed by the personnel of the auditee.

## Previous audit results

The results of the last audit of this system have been reviewed, in particular to assure appropriate correction and corrective action have been implemented to address any nonconformity identified. This review has concluded that:

any nonconformity identified during previous audits has been corrected and the corrective action continues to be effective

any nonconformity identified during previous audits hasn’t been addressed adequately and the specific issue has been re-defined in the nonconformity section of this report

N/A (no previous audits or no nonconformities during the previous audit)

## Audit planning

[Please describe how the audit was planned by the audit team. Please check the example below]

*The team leader of the audit has established an initial contact with the auditee to make arrangement for this audit, including scheduling the dates. The team leader has validated the feasibility of the audit, the audit objectives, the audit scope, the location and the audit criteria.*

*The audit plan was sent to the auditee and it was confirmed before the opening meeting between the audit team and the auditee.*

*The onsite audit was started with an opening meeting which has been attended by the general manager and the BCMS, ISMS and ITSMS responsible. The MSECB profile, audit purpose, methodology, reporting system, appeal process and confidentiality were briefly presented to the client during the opening meeting.*

## Key people interviewed

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Title** | **Department / Process** | **Opening Meeting (Yes or No)** | **Closing Meeting (Yes or No)** | **Date of interviewing** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## MSECB complaint and appeal process

Any client may appeal any decision made by the audit team. Appeals must be in writing and are addressed using MSECB’ procedure for handling appeals and disputes. If MSECB fails to resolve the appeal to the organization’s satisfaction, the appeal can be escalated to MSECB Advisory Board.

MSECB Complaint and Appeal Procedure: [https://MSECB-ms.com/en/complaintAndAppealProcedure](https://pecb-ms.com/en/complaintAndAppealProcedure)

# Significant audit trails followed

**Notes on usage by the auditor:**

*Under the column “Status”, please use the following key to record your assessment result for each clause:*

***A*** *= Acceptable,*

***N/A*** *= Not Applicable (Out of Scope),*

***MaNC*** *= Major Nonconformity*

***MiNC*** *= Minor Nonconformity*

***OBS*** *= Observation*

***OFI*** *= Opportunity for improvement*

*nonconformities are explained in “Section 4: Audit Findings”.*

*Evidence should be provided also for ‘Acceptable’ clauses.*

*If nonconformity is identified (Minor or Major), please include the number of the nonconformity in the column “No. of NC”. Detailed description of the nonconformity should be provided in Annex A – Nonconformity Report.*

*If OBS or OFI is identified, please explain in details the finding(s) in section 4.4 and 4.5.*

| **Clause**  **Requirement** | | **Status** | **Audit Evidence** | **No. of NC** |
| --- | --- | --- | --- | --- |
|  | |  | Findings/justification of findings/specifics/notes |  |
| **ISO 27001 requirements/PIMS specific requirements related to ISO/IEC 27001** | | | | |
| **4/5.2 Context of the organization** | | | |  |
| 4.1/5.2.1 | Understanding the organization and its context\*\* |  |  |  |
| 4.2/5.2.2 | Understanding the needs and expectations of interested parties\*\* |  |  |  |
| 4.3/5.2.3 | Determining the scope of the information security and privacy management system\*\* |  |  |  |
| 4.4/5.2.4 | Information security and privacy management system\*\* |  |  |  |
| **5/5.3 Leadership** | | | |  |
| 5.1/5.3.1 | Leadership and commitment |  |  |  |
| 5.2/5.3.2 | Policy |  |  |  |
| 5.3/5.3.3 | Organizational roles, responsibilities and authorities |  |  |  |
| **6/5.4 Planning** | | | |  |
| 6.1/5.4.1 | Actions to address risks and opportunities\*\* |  |  |  |
| 6.2/5.4.2 | Information security and privacy objectives and planning to achieve them |  |  |  |
| **7/5.5 Support** | | | |  |
| 7.1/5.5.1 | Resources |  |  |  |
| 7.2/5.5.2 | Competence |  |  |  |
| 7.3/5.5.3 | Awareness |  |  |  |
| 7.4/5.5.4 | Communication |  |  |  |
| 7.5/5.5.5 | Documented information |  |  |  |
| **8/5.6 Operation** | | | |  |
| 8.1/5.6.1 | Operational planning and control |  |  |  |
| 8.2/5.6.2 | Information security and privacy risk assessment |  |  |  |
| 8.3/5.6.3 | Information security and privacy risk treatment |  |  |  |
| **9/5.7 Performance evaluation** | | | |  |
| 9.1/5.7.1 | Monitoring, measurement, analysis and evaluation |  |  |  |
| 9.2/5.7.2 | Internal audit |  |  |  |
| 9.3/5.7.3 | Management review |  |  |  |
| **10/5.8 Improvement** | | | |  |
| 10.1/5.8.1 | Nonconformity and corrective action |  |  |  |
| 10.2/5.8.2 | Continual improvement |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **11. Additional requirements** | | |  |
| Use of logo and trademark |  |  |  |
| List of documents included in the audited MS |  |  |  |

| **Control Objective and Controls** | | **Status** | **Audit Evidence** | **No. of NC** |
| --- | --- | --- | --- | --- |
|  | |  | Findings/justification of findings/specifics/notes |  |
| **Information security control objectives and controls /PIMS**  **specific guidance related to ISO/IEC 27002** | | | | |
| **A.5/6.2 Information security and privacy policies** | | | | |
| **A.5.1/6.2.1 Management direction for information security and privacy**  Objective: To provide management direction and support for information security and privacy in accordance with business requirements and relevant laws and regulations. | | | | |
| A 5.1.1/6.2.1.1 | **Policies for information security and privacy\*\*** Control. A set of policies for information security and privacy shall be defined by management, published and communicated to all employees and relevant external parties. |  |  |  |
| A 5.1.2/6.2.1.2 | **Review of the policies for information security and privacy** Control. The policies for information security and privacy shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness. |  |  |  |
| **A.6/6.3 Organization of information security and privacy** | | | | |
| **A.6.1/6.3.1 Internal organization**  Objective: To establish a management framework to initiate and control the implementation and operation of information security and privacy within the organization. | | | | |
| A 6.1.1/6.3.1.1 | **Information security and privacy roles and responsibilities\*\*** Control. All information security and privacy responsibilities shall be defined and allocated. |  |  |  |
| A 6.1.2/6.3.1.2 | **Segregation of duties**. Control. Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets. |  |  |  |
| A 6.1.3/6.3.1.3 | **Contact with authorities.** Control. Appropriate contacts with relevant authorities shall be maintained. |  |  |  |
| A 6.1.4/6.3.1.4 | **Contact with special interest groups.** Control. Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained. |  |  |  |
| A 6.1.5/6.3.1.5 | **Information security and privacy in project management.** Control. Information security and privacy shall be addressed in project management, regardless of the type of project. |  |  |  |
| **A.6.2/6.3.2 Mobile devices and teleworking**  Objective: To ensure the security and privacy of teleworking and use of mobile devices. | | | | |
| A 6.2.1/6.3.2.1 | **Mobile device policy\*\***. Control. A policy and supporting security and privacy measures shall be adopted to manage the risks introduced by using mobile devices. |  |  |  |
| A 6.2.2/6.3.2.2 | **Teleworking.** Control. A policy and supporting measures shall be implemented to protect information accessed, processed or stored at teleworking sites. |  |  |  |
| **A.7/6.4 Human resource security** | | | | |
| **A.7.1/6.4.1 Prior to employment**  Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered | | | | |
| A 7.1.1/6.4.1.1 | **Screening.** Control. Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks. |  |  |  |
| A 7.1.2/6.4.1.2 | **Terms and conditions of employment.** Control. The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security. |  |  |  |
| **A.7.2/6.4.2 During employment**  Objective: To ensure that employees and contractors are aware of and fulfil their information security and privacy responsibilities. | | | | |
| A 7.2.1/6.4.2.1 | **Management responsibilities.** Control. Management shall require all employees and contractors to apply information security and privacy in accordance with the established policies and procedures of the organisation. |  |  |  |
| A 7.2.2/6.4.2.2 | **Information security and privacy awareness, education and training.\*** Control. All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function. |  |  |  |
| A 7.2.3/6.4.2.3 | **Disciplinary process.** Control. There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security and privacy breach. |  |  |  |
| **A.7.3/6.4.3 Termination and change of employment**  Objective: To protect the organization’s interests as part of the process of changing or terminating employment. | | | | |
| A 7.3.1/6.4.3.1 | **Termination or change of employment responsibilities.** Control. Information security and privacy responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced. |  |  |  |
| **A.8/6.5 Asset management** | | | | |
| **A.8.1/6.5.1 Responsibility for assets**  Objective: To identify organizational assets and define appropriate protection responsibilities. | | | | |
| A 8.1.1/6.5.1.1 | **Inventory of assets**. Control. Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained. |  |  |  |
| A 8.1.2/6.5.1.2 | **Ownership of assets.** Control. Assets maintained in the inventory shall be owned. |  |  |  |
| A 8.1.3/6.5.1.3 | **Acceptable use of assets.** Control. Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented. |  |  |  |
| A 8.1.4/6.5.1.4 | **Return of assets.** Control. All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement. |  |  |  |
| **A.8.2/6.5.2 Information classification**  Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization. | | | | |
| A 8.2.1/6.5.2.1 | **Classification of information.\*\*** Control. Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification. |  |  |  |
| A 8.2.2/6.5.2.2 | **Labeling of information.\*\*** Control. An appropriate set of procedures for information labeling shall be developed and implemented in accordance with the information classification scheme adopted by the organization. |  |  |  |
| A 8.2.3/6.5.2.3 | **Handling of assets.** Control. Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization. |  |  |  |
| **A.8.3/6.5.3 Media handling**  Objective: To prevent unauthorized disclosure, modification, removal or destruction of information stored on media. | | | | |
| A 8.3.1/6.5.3.1 | **Management of removable media.\*\*** Control. Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization. |  |  |  |
| A 8.3.2/6.5.3.2 | **Disposal of media.\*\***  Control. Media shall be disposed of securely when no longer required, using formal procedures. |  |  |  |
| A 8.3.3/6.5.3.3 | **Physical media transfer.\*\***  Control. Media containing information shall be protected against unauthorised access, misuse or corruption during transportation. |  |  |  |
| **A.9/6.6 Access control** | | | | |
| **A.9.1/6.6.1 Business requirements of access control**  Objective: To limit access to information and information processing facilities. | | | | |
| A 9.1.1/6.6.1.1 | **Access control policy.**  Control. An access control policy shall be established, documented and reviewed based on business and information security and privacy requirements. |  |  |  |
| A 9.1.2/6.6.1.2 | **Access to networks and network services.**  Control. Users shall only be provided with access to the network and network services that they have been specifically authorized to use. |  |  |  |
| **A.9.2/6.6.2 User access management**  Objective: To ensure authorized user access and to prevent unauthorized access to systems and services. | | | | |
| A 9.2.1/6.6.2.1 | **User registration and deregistration.\*\*** Control. A formal user registration and de-registration process shall be implemented to enable assignment of access rights. |  |  |  |
| A 9.2.2/6.6.2.2 | **User access provisioning.\*\*** Control. A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services. |  |  |  |
| A 9.2.3/6.6.2.3 | **Management of privileged access rights**. Control. The allocation and use of privileged access rights shall be restricted and controlled. |  |  |  |
| A 9.2.4/6.6.2.4 | **Management of secret authentication information of users.** Control. The allocation of secret authentication information shall be controlled through a formal management process. |  |  |  |
| A 9.2.5/6.6.2.5 | **Review of user access rights.**  Control. Asset owners shall review users' access rights at regular intervals. |  |  |  |
| A 9.2.6/6.6.2.6 | **Removal or adjustment of access rights.** Control. The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change. |  |  |  |
| **A.9.3/6.6.3 User Responsibilities**  Objective: To make users accountable for safeguarding their authentication information. | | | | |
| A 9.3.1/6.6.3.1 | **Use of secret authentication information.** Control. Users shall be required to follow the organization's practices in the use of secret authentication information. |  |  |  |
| **A.9.4/6.6.4 System and application access control**  Objective: To prevent unauthorized access to systems and applications. | | | | |
| A 9.4.1/6.6.4.1 | **Information access restriction.** Control. Access to information and application system functions by users shall be restricted in accordance with the access control policy. |  |  |  |
| A 9.4.2/6.6.4.2 | **Secure Log-on procedures.\*\*** Control. Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure. |  |  |  |
| A 9.4.3/6.6.4.3 | **Password Management system.** Control. Password management systems shall be interactive and shall ensure quality passwords. |  |  |  |
| A 9.4.4/6.6.4.4 | **Use of privileged utility programs.** Control. The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled. |  |  |  |
| A 9.4.5/6.6.4.5 | **Access control to program source code.** Control. Access to program source code shall be restricted. |  |  |  |
| **A.10/6.7 Cryptography** | | | | |
| **A.10.1/6.7.1 Cryptographic controls**  Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information. | | | | |
| A 10.1.1/6.7.1.1 | **Policy on the use of cryptographic controls.\*\***  Control. A policy on the use of cryptographic controls for protection of information shall be developed and implemented. |  |  |  |
| A 10.1.2/6.7.1.2 | **Key Management.**  Control. A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle. |  |  |  |
| **A.11/6.8 Physical and environmental security** | | | | |
| **A.11.1/6.8.1 Secure areas**  Objective: To prevent unauthorized physical access, damage and interference to the organization’s information and information processing facilities. | | | | |
| A 11.1.1/6.8.1.1 | **Physical security perimeter.**  Control. Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities. |  |  |  |
| A 11.1.2/6.8.1.2 | **Physical entry controls** Control. Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. |  |  |  |
| A 11.1.3/6.8.1.3 | **Securing offices, rooms and facilities.** Control. Physical security for offices, rooms, and facilities shall be designed and applied. |  |  |  |
| A 11.1.4/6.8.1.4 | **Protecting against external and environmental threats.** Control. Physical protection against natural disasters, malicious attack or accidents shall be designed and applied. |  |  |  |
| A 11.1.5/6.8.1.5 | **Working in secure areas.**  Control. Procedures for working in secure areas shall be designed and applied. |  |  |  |
| A 11.1.6/6.8.1.6 | **Delivery and loading areas**. Control. Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. |  |  |  |
| **A.11.2/6.8.2 Equipment**  Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations. | | | | |
| A 11.2.1/6.8.2.1 | **Equipment siting and protection.** Control. Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. |  |  |  |
| A 11.2.2/6.8.2.2 | **Supporting utilities.**  Control. Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities. |  |  |  |
| A 11.2.3/6.8.2.3 | **Cabling security.**  Control. Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage. |  |  |  |
| A 11.2.4/6.8.2.4 | **Equipment maintenance.** Control. Equipment shall be correctly maintained to ensure its continued availability and integrity. |  |  |  |
| A 11.2.5/6.8.2.5 | **Removal of assets.**  Control. Equipment, information or software shall not be taken off-site without prior authorization. |  |  |  |
| A 11.2.6/6.8.2.6 | **Security of equipment and assets off-premises.** Control. Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises. |  |  |  |
| A 11.2.7/6.8.2.7 | **Secure disposal or re-use of equipment.**\*\* Control. All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use. |  |  |  |
| A 11.2.8/6.8.2.8 | **Unattended user equipment.**  Control. Users shall ensure that unattended equipment has appropriate protection. |  |  |  |
| A 11.2.9/6.8.2.9 | **Clear Desk and Clear Screen Policy.\*\*** Control. A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted. |  |  |  |
| **A.12/6.9 Operations security** | | | | |
| **A.12.1/6.9.1 Operational procedures and responsibilities**  Objective: To ensure correct and secure operations of information processing facilities. | | | | |
| A 12.1.1/6.9.1.1 | **Documented operating procedures.**  Control. Operating procedures shall be documented and made available to all users who need them. |  |  |  |
| A 12.1.2/6.9.1.2 | **Change management.**  Control. Changes to the organization, business processes, information processing facilities and systems that affect information security and privacy shall be controlled. |  |  |  |
| A 12.1.3/6.9.1.3 | **Capacity management.**  Control. The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance. |  |  |  |
| A 12.1.4/6.9.1.4 | **Separation of development, testing and operational environments.** Control. Development, testing and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment. |  |  |  |
| **A.12.2/6.9.2 Protection from malware**  Objective: To ensure that information and information processing facilities are protected against malware. | | | | |
| A 12.2.1/6.9.2.1 | **Controls against malware.**  Control. Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness. |  |  |  |
| **12.3/6.9.3 Backup**  Objective: To protect against loss of data. | | | | |
| A 12.3.1/6.9.3.1 | **Information backup.\*\***  Control. Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy. |  |  |  |
| **A.12.4/6.9.4 Logging and monitoring**  Objective.To log events and generate evidence. | | | | |
| A 12.4.1/6.9.4.1 | **Event logging.\*\*** Control. Event logs recording user activities, exceptions, faults and information security and privacy events shall be produced, kept and regularly reviewed. |  |  |  |
| A 12.4.2/6.9.4.2 | **Protection of log information.\*\***  Control. Logging facilities and log information shall be protected against tampering and unauthorized access. |  |  |  |
| A 12.4.3/6.9.4.3 | **Administrator and operator logs.** Control. System administrator and system operator activities shall be logged and the logs protected and regularly reviewed. |  |  |  |
| A 12.4.4/6.9.4.4 | **Clock synchronization.** Control. The clocks of all relevant information processing systems within an organization or security domain shall be synchronized to a single reference source. |  |  |  |
| **A.12.5/6.9.5 Control of operational software**  Objective: To ensure the integrity of operational systems. | | | | |
| A 12.5.1/6.9.5.1 | **Installation of software on operational systems.** Control. Procedures shall be implemented to control the installation of software on operational systems. |  |  |  |
| **A.12.6/6.9.6 Technical Vulnerability Management**  Objective: To prevent exploitation of technical vulnerabilities. | | | | |
| A 12.6.1/6.9.6.1 | **Management of technical vulnerabilities.**  Control. Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk. |  |  |  |
| A 12.6.2/6.9.6.2 | **Restrictions on software installation.** Control. Rules governing the installation of software by users shall be established and implemented. |  |  |  |
| **A.12.7/6.9.7 Information systems audit considerations**  Objective: To minimize the impact of audit activities on operational systems. | | | | |
| A 12.7.1/6.9.7.1 | **Information System Audit controls.**  Control. Audit requirements and activities involving verifications of operational systems shall be carefully planned and agreed to minimize disruptions to business processes. |  |  |  |
| **A.13/6.10 Communications security** | | | | |
| **A.13.1/6.10.1 Network security management**  Objective: To ensure the protection of information in networks and its supporting information processing facilities. | | | | |
| A 13.1.1/6.10.1.1 | **Network controls.**  Control. Networks shall be managed and controlled to protect information in systems and applications. |  |  |  |
| A 13.1.2/6.10.1.2 | **Security of network services.** Control. Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced. |  |  |  |
| A 13.1.3/6.10.1.3 | **Segregation in networks.**  Control. Groups of information services, users and information systems shall be segregated on networks. |  |  |  |
| **A.13.2/6.10.2 Information transfer**  Objective: To maintain the security of information transferred within an organization and with any external entity. | | | | |
| A 13.2.1/6.10.2.1 | **Information transfer policies and procedures.\*\*** Control. Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities. |  |  |  |
| A 13.2.2/6.10.2.2 | **Agreements on information transfer.** Control. Agreements shall address the secure transfer of business information between the organization and external parties. |  |  |  |
| A 13.2.3/6.10.2.3 | **Electronic messaging.** Control. Information involved in electronic messaging shall be appropriately protected. |  |  |  |
| A 13.2.4/6.10.2.4 | **Confidentiality or nondisclosure agreements.\*\***  Control. Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented. |  |  |  |
| **A.14/6.11 System acquisition, development and maintenance** | | | | |
| **A.14.1/6.11.1 Security requirements of information systems**  Objective: To ensure that information security and privacy is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks. | | | | |
| A 14.1.1/6.11.1.1 | **Information security requirements analysis and specification.** Control. The information security and privacy related requirements shall be included in the requirements for new information systems or enhancements to existing information systems. |  |  |  |
| A 14.1.2/6.11.1.2 | **Securing application services on public networks.\*\*** Control. Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification. |  |  |  |
| A 14.1.3/6.11.1.3 | **Protecting application services transactions.**  Control. Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay. |  |  |  |
| **A.14.2/6.11.2 Security in development and support processes**  Objective: To ensure that information security and privacy is designed and implemented within the development lifecycle of information systems. | | | | |
| A 14.2.1/6.11.2.1 | **Secure development policy.\*\*** Control. Rules for the development of software and systems shall be established and applied to developments within the organization. |  |  |  |
| A 14.2.2/6.11.2.2 | **System change control procedures.** Control. Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures. |  |  |  |
| A 14.2.3/6.11.2.3 | **Technical review of applications after operating platform changes.** Control. When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security. |  |  |  |
| A 14.2.4/6.11.2.4 | **Restrictions on changes to software packages.** Control. Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled. |  |  |  |
| A 14.2.5/6.11.2.5 | **Secure systems engineering principles.\*\*** Control. Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts. |  |  |  |
| A 14.2.6/6.11.2.6 | **Secure development environment.** Control. Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle. |  |  |  |
| A 14.2.7/6.11.2.7 | **Outsourced development.\*\***  Control. The organization shall supervise and monitor the activity of out sourced system development. |  |  |  |
| A 14.2.8/6.11.2.8 | **System security testing.**  Control. Testing of security functionality shall be carried out during development. |  |  |  |
| A 14.2.9/6.11.2.9 | **System acceptance testing.** Control. Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions. |  |  |  |
| **A.14.3/6.11.3 Test data**  Objective: To ensure the protection of data used for testing. | | | | |
| A 14.3.1/6.11.3.1 | **Protection of test data.\*\***  Control. Test data shall be selected carefully, protected and controlled. |  |  |  |
| **A.15/6.12 Supplier relationships** | | | |  |
| **A.15.1/6.12.1 Information security and privacy in supplier relationships**  Objective: To ensure protection of the organization’s assets that is accessible by suppliers. | | | | |
| A 15.1.1/6.12.1.1 | **Information security and privacy policy for supplier relationships.** Control. Information security and privacy requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented. |  |  |  |
| A 15.1.2/6.12.1.2 | **Addressing security within supplier agreements.\*\*** Control. All relevant information security and privacy requirements shall be established and agreed with each supplier that may access, process, store, communicated, or provide IT infrastructure components for, the organization's information. |  |  |  |
| A 15.1.3/6.12.1.3 | **Information and communication technology supply chain.** Control. Agreements with suppliers shall include requirements to address the information security and privacy risks associated with information and communications technology services and product supply chain. |  |  |  |
| **A.15.2/6.12.2 Supplier service delivery management**  Objective: To maintain an agreed level of information security and privacy and service delivery in line with supplier agreements. | | | | |
| A 15.2.1/6.12.2.1 | **Monitoring and review of supplier services.**  Control. Organizations shall regularly monitor, review and audit supplier service delivery. |  |  |  |
| A 15.2.2/6.12.2.2 | **Managing changes to supplier services.**  Control. Changes to the provision of services by suppliers, including maintaining and improving existing information security and privacy policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks. |  |  |  |
| **A.16/6.13 Information security and privacy incident management** | | | | |
| **A.16.1/6.13.1 Management of information security and privacy incidents and improvements**  Objective: To ensure a consistent and effective approach to the management of information security and privacy incidents, including communication on security events and weaknesses. | | | |  |
| A 16.1.1/6.13.1.1 | **Responsibilities and procedures.\*\*** Control. Management of responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security and privacy incidents. |  |  |  |
| A 16.1.2/6.13.1.2 | **Reporting information security and privacy events.**  Control. Information security and privacy events shall be reported through appropriate management channels as quickly as possible. |  |  |  |
| A 16.1.3/6.13.1.3 | **Reporting information security and privacy weaknesses.**  Control. Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security and privacy weaknesses in systems or services. |  |  |  |
| A 16.1.4/6.13.1.4 | **Assessment of and decision on information security and privacy events.** Control. Information security and privacy events shall be assessed and it shall be decided if they are to be classified as information security and privacy incidents. |  |  |  |
| A 16.1.5/6.13.1.5 | **Response to information security and privacy incidents.\*\***  Control. Information security incidents shall be responded to in accordance with the documented procedures. |  |  |  |
| A 16.1.6/6.13.1.6 | **Learning from information security and privacy incidents.** Control. Knowledge gained from analyzing and resolving information security and privacy incidents shall be used to reduce the likelihood or impact of future incidents. |  |  |  |
| A 16.1.7/6.13.1.7 | **Collection of evidence.** Control. The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence. |  |  |  |
| **A.17/6.14 Information security aspects of business continuity management** | | | | |
| **A.17.1/6.14.1 Information security continuity**  Objective: Information security continuity shall be embedded in the organization’s business continuity management systems. | | | |  |
| A 17.1.1/6.14.1.1 | **Planning information security continuity.** Control. The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster. |  |  |  |
| A 17.1.2/6.14.1.2 | **Implementing information security continuity.** Control. The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information securityduring an adverse situation. |  |  |  |
| A 17.1.3/6.14.1.3 | **Verify, review and evaluate information security continuity.**  Control. The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations. |  |  |  |
| **A.17.2/6.14.2 Redundancies**  Objective:To ensure availability of information processing facilities. | | | | |
| A 17.2.1/6.14.2.1 | **Availability of information processing facilities.**  Control. Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements. |  |  |  |
| **A.18/6.15 Compliance** | | | | |
| **A.18.1/6.15.1 Compliance with legal and contractual requirements**  Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and privacy and of any security requirements. | | | |  |
| A 18.1.1/6.15.1.1 | **Identification of applicable legislation and contractual requirements.\*\*** Control. All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization. |  |  |  |
| A 18.1.2/6.15.1.2 | **Intellectual property rights.** Control. Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products. |  |  |  |
| A 18.1.3/6.15.1.3 | **Protection of records.\*\*** Control. Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements. |  |  |  |
| A 18.1.4/6.15.1.4 | **Privacy and protection of personally identifiable information.** Control. Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable. |  |  |  |
| A 18.1.5/6.15.1.5 | **Regulation of cryptographic controls.**  Control. Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations. |  |  |  |
| **A.18.2/6.15.2 Information security and privacy reviews**  Objective: To ensure that information security and privacy is implemented and operated in accordance with the organizational policies and procedures. | | | | |
| A 18.2.1/6.15.2.1 | **Independent review of information security and privacy.\*\***  Control. The organization's approach to managing information security and privacy and its implementation (i.e. control objectives, control, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur. |  |  |  |
| A 18.2.2/6.15.2.2 | **Compliance with security policies and standards**. Control. Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements. |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| A 18.2.3/6.15.2.3 | **Technical compliance review.\*\*** Control. Information systems shall be regularly reviewed for compliance with the organization's information security and privacy policies and standards. |  |  |  |

**Annex A – PIMS-specific reference control objectives and controls (PII Controllers)**

| **Control Objective and Controls** | | **Status** | **Audit Evidence** | **No. of NC** |
| --- | --- | --- | --- | --- |
|  | |  | Findings/justification of findings/specifics/notes |  |
| **A.7.2 Conditions for collection and processing** | | | | |
| Objective: To determine and document that processing is lawful, with legal basis as per applicable jurisdictions, and with clearly defined and legitimate purposes. | | | | |
| A 7.2.1 | **Identify and document purpose** Control. The organization shall identify and document the specific purposes for which the PII will be processed. |  |  |  |
| A 7.2.2 | **Identify lawful basis**  Control. The organization shall determine, document and comply with the relevant lawful basis for the processing of PII for the identified purposes. |  |  |  |
| A 7.2.3 | **Determine when and how consent is to be obtained**  Control.The organization shall determine and document a process by which it can demonstrate if, when and how consent for the processing of PII was obtained from PII principals. |  |  |  |
| A 7.2.4 | **Obtain and record consent**  Control.The organization shall obtain and record consent from PII principals according to the documented processes. |  |  |  |
| A 7.2.5 | **Privacy impact assessment**  Control.The organization shall assess the need for, and implement where appropriate, a privacy impact assessment whenever new processing of PII or changes to existing processing of PII is planned. |  |  |  |
| A 7.2.6 | **Contract with PII processors**  Control.The organization shall have a written contract with any PII processor that it uses, and shall ensure that their contracts with PII processors address the implementation of the appropriate controls in Annex B. |  |  |  |
| A 7.2.7 | **Joint PII controller**  Control.The organization shall determine respective roles and responsibilities for the processing of PII (including PII protection and security requirements) with any joint PII controller. |  |  |  |
| A 7.2.87 | **Records related to processing PII**  Control.The organization shall determine and securely maintain the necessary records in support of its obligations for the processing of PII. |  |  |  |
| **A.7.3 Obligations to PII principals** | | | | |
| Objective: To ensure that PII principals are provided with appropriate information about the processing of their PII and to meet any other applicable obligations to PII principals related to the processing of their PII. | | | | |
| A 7.3.1 | **Determining and fulfilling obligations to PII principals**  Control. The organization shall determine and document their legal, regulatory and business obligations to PII principals related to the processing of their PII and provide the means to meet these obligations. |  |  |  |
| A 7.3.2 | **Determining information for PII principals**  Control. The organization shall determine and document the information to be provided to PII principals regarding the processing of their PII and the timing of such a provision. |  |  |  |
| A 7.3.3 | **Providing information to PII principals**  Control. The organization shall provide PII principals with clear and easily accessible information identifying the PII controller and describing the processing of their PII. |  |  |  |
| A 7.3.4 | **Providing mechanism to modify or withdraw consent**  Control. The organization shall provide a mechanisms for PII principals to modify or withdraw their consent. |  |  |  |
| A 7.3.5 | **Providing mechanism to object to PII processing**  Control. The organization shall provide a mechanism for PII principals to object to the processing of their PII. |  |  |  |
| A 7.3.6 | **Access, correction and/or erasure**  Control.The organization shall implement policies, procedures and/or mechanisms to meet their obligations to PII principals to access, correct and/or erase their PII. |  |  |  |
| A 7.3.7 | **PII controllers’ obligations to inform third parties**  Control.The organization shall inform third parties with whom PII has been shared of any modification, withdrawal or objectionspertaining to the shared PII, and implement appropriate policies, procedures and/or mechanisms to do so. |  |  |  |
| A 7.3.8 | **Providing copy of PII processed**  Control.The organization shall be able to provide a copy of the PII that is processed when requested by the PII principal |  |  |  |
| A 7.3.9 | **Handling requests**  Control.The organization shall define and document policies and procedures for handling and responding to legitimate requests from PII principals. |  |  |  |
| A 7.3.10 | **Automated decision making**  Control.The organization shall identify and address obligations, including legal obligations, to the PII principals resulting from decisions made by the organization which are related to the PII principal based solely on automated processing of PII. |  |  |  |
| **A.7.4 Privacy by Design and privacy by default** | | | | |
| Objective: To ensure that processes and systems are designed such that the collection and processing (including use, disclosure, retention, transmission and disposal) are limited to what is necessary for the identified purpose. | | | | |
| A 7.4.1 | **Limit collection**  Control. The organization shall limit the collection of PII to the minimum that is relevant, proportional and necessary for the identified purposes. |  |  |  |
| A 7.4.2 | **Limit processing**  Control. The organization shall limit the processing of PII to that which is adequate, relevant and necessary for the identified purposes. |  |  |  |
| A 7.4.3 | **Accuracy and quality**  Control. The organization shall ensure and document that PII is as accurate, complete and up-to-date as is necessary for the purposes for which it is processed, throughout the life-cycle of the PII. |  |  |  |
| A 7.4.4 | **PII minimization objectives**  Control. The organization shall define and document data minimization objectives and what mechanisms (such as de-identification) are used to meet those objectives. |  |  |  |
| A 7.4.5 | **PII de-identification and deletion at the end of processing**  Control. The organization shall either delete PII or render it in a form which does not permit identification or re-identification of PII principals, as soon as the original PII is no longer necessary for the identified purposes(s). |  |  |  |
| A 7.4.6 | **Temporary files**  Control. The organization shall ensure that temporary files created as a result of the processing of PII are disposed of (e.g. erased or destroyed) following documented procedures within a specified, documented period. |  |  |  |
| A 7.4.7 | **Retention**  Control.The organization shall not retain PII for longer than is necessary for the purposes for which the PII is processed. |  |  |  |
| A 7.4.8 | **Disposal**  Control.The organization shall have documented policies, procedures and/or mechanisms for the disposal of PII. |  |  |  |
| A 7.4.9 | **PII transmission controls**  Control.The organization shall subject PII transmitted (e.g. sent to another organization) over a data-transmission network to appropriate controls designed to ensure that the data reaches its intended destination. |  |  |  |
| **A.7.5 PII sharing, transfer and disclosure** | | | | |
| Objective: To determine whether and document when PII is shared, transferred to other jurisdictions or third parties and/or disclosed in accordance with applicable obligations. | | | | |
| A 7.5.1 | **Identify basis for PII transfer between jurisdictions**  Control. The organization shall identify and document the relevant basis for transfers of PII between jurisdictions. |  |  |  |
| A 7.5.2 | **Countries and international organizations to which PII can be transferred**  Control. The organization shall specify and document the countries and international organizations to which PII can possibly be transferred. |  |  |  |
| A 7.5.3 | **Records of transfer of PII**  Control. The organization shall record transfers of PII to or from third party and ensure cooperation with those parties to support future requests related to obligations to the PII principals. |  |  |  |
| A 7.5.4 | **Records of PII disclosure to third parties**  Control. The organization shall record disclosures of PII to third parties, including what PII has been disclosed, to whom and at what time. |  |  |  |

**Annex B – PIMS-specific reference control objectives and controls (PII Processors)**

| **Control Objective and Controls** | | **Status** | **Audit Evidence** | **No. of NC** |
| --- | --- | --- | --- | --- |
|  | |  | Findings/justification of findings/specifics/notes |  |
| **B.8.2 Conditions for collection and processing** | | | | |
| Objective: To determine and document that processing is lawful, with legal basis as per applicable jurisdictions, and with clearly defined and legitimate purposes. | | | | |
| B 8.2.1 | **Customer agreement** Control. The organization shall ensure, where relevant, that the contract to process PII addresses the organization’s role in providing assistance with the customer’s obligations, (taking into account the nature of processing and the information available to the organization). |  |  |  |
| B 8.2.2 | **Organization’s purposes**  Control. The organization shall ensure that PII processed on behalf of a customer are only processed for the purposes expressed in the documented instructions of the customer. |  |  |  |
| B 8.2.3 | **Marketing and advertising use**  Control.The organization shall not use PII processed under a contract for the purposes of marketing and advertising without establishing that prior consent was obtained from the appropriate PII principal. The organization shall not make providing such consent a condition for receiving the service. |  |  |  |
| B 8.2.4 | **Infringing instruction**  Control.The organization shall inform the customer if, in its opinion, a processing instruction infringes applicable legislation and/or regulation. |  |  |  |
| B 8.2.5 | **Customer obligations**  Control.The organization shall provide the customer with the appropriate information such that the customer can demonstrate compliance with their obligations. |  |  |  |
| B 8.2.6 | **Records related to processing PII**  Control.The organization shall determine and maintain the necessary records in support of demonstrating compliance with its obligations (as specified in the applicable contract) for the processing of PII carried out on behalf of a customer. |  |  |  |
| **B.8.3 Obligations to PII principals** | | | | |
| Objective: To ensure that PII principals are provided with appropriate information about the processing of their PII, and to meet any other applicable obligations to PII principals related to the processing of their PII. | | | | |
| B 8.3.1 | **Obligations to PII principals**  Control. The organization shall provide the customer with the means to comply with its obligations related to PII principals. |  |  |  |
| **B.8.4 Privacy by Design and privacy by default** | | | | |
| Objective: To ensure that processes and systems are designed such that the collection and processing of PII (including use, disclosure, retention, transmission and disposal) are limited to what is necessary for the identified purpose. | | | | |
| B 8.4.1 | **Temporary files**  Control. The organization shall ensure that temporary files created as a result of the processing of PII are disposed of (e.g. erased or destroyed) following documented procedures within a specified, documented period. |  |  |  |
| B 8.4.2 | **Return, transfer or disposal of PII**  Control. The organization shall provide the ability to return, transfer and/or disposal of PII in a secure manner. It shall also make its policy available to the customer. |  |  |  |
| B 8.4.3 | **PII transmission controls**  Control. The organization shall subject PII transmitted over a data-transmission network to appropriate controls designed to ensure that the data reaches its intended destination. |  |  |  |
| **B.8.5 PII sharing, transfer and disclosure** | | | | |
| Objective: To determine whether and document when PII is shared, transferred to other jurisdictions or third parties and/or disclosed in accordance with applicable obligations. | | | | |
| B 8.5.1 | **Basis for PII transfer between jurisdictions**  Control. The organization shall inform the customer in a timely manner of the basis for PII transfers between jurisdictions and of any intended changes in this regard, so that the customer has the ability to object to such changes or to terminate the contract. |  |  |  |
| B 8.5.2 | **Countries and international organizations to which PII can be transferred**  Control. The organization shall specify and document the countries and international organizations to which PII can possibly be transferred. |  |  |  |
| B 8.5.3 | **Records of PII disclosure to third parties**  Control. The organization shall record disclosures of PII to third parties, including what PII has been disclosed, to whom and when. |  |  |  |
| B 8.5.4 | **Notification of PII disclosure requests**  Control. The organization shall notify the customer of any legally binding requests for disclosure of PII. |  |  |  |
| B 8.5.5 | **Legally binding PII disclosures**  Control.The organization shall reject any requests for PII disclosures that are not legally binding, consult the corresponding customer before making any PII disclosures and accepting any contractually agreed requests for PII disclosures that are authorized by the corresponding customer. |  |  |  |
| B 8.5.6 | **Disclosure of subcontractors used to process PII**  Control.The organization shall disclose any use of subcontractors to process PII to the customer before use. |  |  |  |
| B 8.5.7 | **Engagement of a subcontractor to process PII**  Control.The organization shall only engage a subcontractor to process PII according to the customer contract |  |  |  |
| B 8.5.8 | **Change of subcontractor to process PII**  Control.The organization shall, in the case of having general written authorization, inform the customer of any intended changes concerning the addition or replacement of subcontractors to process PII, thereby giving the customer the opportunity to object such changes. |  |  |  |

# Audit findings

The audit findings were communicated to the senior management of the organization during the closing meeting. The final conclusion of the audit results and recommendation by the audit team was also communicated to the management during the meeting.

## Audit finding definition

The evaluation of the audit findings is based on the following definitions:

**Major Nonconformities (MaNC)**

The **absence** or **total failure** of a **system** to meet a requirement. It may be either:

* A number of minor nonconformities against one requirement can represent a total failure of the system and thus be considered a major nonconformance; or
* Any nonconformance that would result in the probable shipment of a nonconforming product. A condition that may result in the failure or materially reduce the usability of the products or services for their intended purpose; or
* A nonconformance that judgment and experience indicate is likely either to result in the failure of the ISMS system or to materially reduce its ability to assure controlled processes and products.

**Minor Nonconformities (MiNC)**

A **nonconformance** that judgment and experience **indicate is not likely to result in the failure** of the ISMS system or **reduce its ability** to assure controlled processes or products. It may be either:

* A failure in some part of the supplier's documented ISMS system relative to a requirement; or
* A single observed lapse in following one item of a company’s ISMS system.

**Observations (OBS)**

Any issues which are **likely to become a NC,** if not treated until the next audit are marked as observations (OBS). No response is required.

**Opportunities for Improvement (OFI)**

If **certain aspects** which generally comply with the requirements of the standard should be improved, then they are marked as opportunities for improvement (OFI). These OFIs help to **improve the management system** as a whole or named processes. No response is required.

## Major nonconformities (see also Annex A)

Please explain if there are major non-conformities found during the audit.

## Minor nonconformities (see also Annex A)

Please explain if there are minor non-conformities found during the audit.

## Observations

Please list any noted observations or issues that can possibly turn to non-conformities.

## Opportunities for improvement

*Please list any noted opportunities for improvement without any specific recommendations for correction.*

## Agreed follow-up activities

Nonconformities detailed here need to be addressed through the organization’s corrective action process, in accordance with the relevant corrective action requirements of the audit standard, including actions to analyze the cause of the nonconformity, prevent recurrence, and complete the maintained records.

Corrective actions to address the identified major nonconformities, shall be carried out immediately and MSECB shall be notified of the actions taken within 30 days. To confirm the actions taken, evaluate their effectiveness, and determine whether certification can be granted or continued, a MSECB auditor will perform a follow up visit within 90 days.

Corrective actions to address the identified minor nonconformities shall be documented on an action plan and be sent for review by the client to the auditor within 30 days. If the actions are deemed to be satisfactory, they will be followed up during the next scheduled visit.

Nonconformities shall be addressed through the client’s corrective action process, including:

* Actions taken to determine the extent of and contain the specific nonconformance.
* Root Cause (results of an investigation to determine the most basic cause(s) of the nonconformance.).
* Actions taken to correct the nonconformance and, in response to the root cause, to eliminate recurrence of the nonconformance.
* Corrective action response shall be submitted to the MSECB Lead Auditor.
* Client must maintain corrective action records, including objective evidence, for at least three (3) years.

## Uncertainty / obstacles that could affect the reliability of audit conclusions

Please specify.

## Unresolved diverging opinions between the audit team & auditee

Please specify.

# Audit conclusions and audit recommendation

## System management conformance and capability

*[Please describe if the management system has proven conformity with the requirements of the audit standard and provided adequate structure to support implementation and maintenance of the management system*

*i.e:*

* *demonstration of effective implementation and maintenance of MS*
* *demonstration of established and tracking of proper key performance objectives and targets*
* *implementation of internal audit programme etc. ]*

## Audit conclusions

|  |  |
| --- | --- |
| Has there been any serious deviation from the audit plan? (If yes, please specify) | Yes  No |
| Are there any significant issues impacting the audit program? (If yes, please specify) | Yes  No |
| Are there any significant changes affecting the management system since last audit took place? (If yes, please list the significant changes) | Yes  No  N/A |
| Are there any unresolved issues affecting the management system since last audit took place? (If yes, please list the unresolved issues) | Yes  No  N/A |
| The verification of the effectiveness of the corrective action taken regarding previously identified nonconformities has been performed and is satisfactory (please list any comments if needed) | Yes  No  N/A |
| The management system is designed to achieve the organization’s policy objectives | Yes  No |
| The management system is designed to meet statutory, regulatory and contractual requirements | Yes  No |
| The internal audit and management review processes are in place and adequate | Yes  No |
| The audit was successful in meeting the stated objectives | Yes  No |

## Recommendation

*Lead Auditor Recommendation:*

*[Please recommend whether the management system of the organization being audited, should be certified or not certified)*



# Annex A: Nonconformity report

## Nonconformity Report

Note: If more than one nonconformity identified, please add additional nonconformity reports

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **NON CONFORMITY REPORT** | | | | | | | | | | |
| **TO BE COMPLETED BY AUDITOR** | | **DATE** | **ORGANIZATION** | | | | | **NC ID** | | |
|  |  | | | | |  | | |
| **STANDARD:** ISO/IEC 27001:2013 | | | | |
| **NON CONFORMITY OBSERVED IN PROCESS/ AREA** | | |  | | | | | |
| **REQUIREMENT OF THE STANDARD:** | | | | | | **CLAUSE:** | | |
| **NON CONFORMITY – DESCRIPTION OF OBJECTIVE EVIDENCE** | | | | | | | | |
|  | | | | | | | | |
| **GRADE (Major/ Minor)** | | **LEAD AUDITOR** | | **AUDITOR** | | | **BUSINESS PROCESS REP.** | |
|  | |  | |  | | |  | |
| **TO BE COMPLETED BEFORE** | |
|  | |
| **TO BE COMPLETED BY THE ORGANIZATION** | | **ROOT CAUSE ANALYSIS (What failed in the system to allow this NC to occur ?)** | | | | | | | | |
|  | | | | | | | | |
| **CORRECTION & CORRECTIVE ACTION (What is done to solve this problem and to prevent recurrence)** | | | | | | | | |
| CORRECTION:  CORRECTIVE ACTION: | | | | | | | | |
| **VERIFICATION OF CORRECTIVE ACTIONS** | | **DATE OF COMPLETION** | |  | | | | |
| **ORGANIZATION REPRESENTATIVE** | |  | | | | |
| **TO BE COMPLETED BY AUDITOR** | | **VERIFICATION OF CORRECTIONS / CORRECTIVE ACTIONS** | | **DATE** | | **STATUS** | **LEAD AUDITOR** | | | |
|  | |  |  | | | |
| **AUDITOR COMMENTS (including evidences verified to accept the corrections/ correcive actions)** | |  | | | | | | |
| **NON CONFORMITY REPORT** | | | | | | | | | | | | |
| **TO BE COMPLETED BY AUDITOR** | | **DATE** | | **ORGANIZATION** | | | | | **NC ID** | | |
|  | |  | | | | |  | | |
| **STANDARD:** ISO/IEC 27701-2019 | | | | |
| **NON CONFORMITY OBSERVED IN PROCESS/ AREA** | | | |  | | | | | |
| **REQUIREMENT OF THE STANDARD:** | | | | | | | **CLAUSE:** | | |
| **NON CONFORMITY – DESCRIPTION OF OBJECTIVE EVIDENCE** | | | | | | | | | |
|  | | | | | | | | | |
| **GRADE (Major/ Minor)** | | | **LEAD AUDITOR** | | **AUDITOR** | | | **BUSINESS PROCESS REP.** | |
|  | | |  | |  | | |  | |
| **TO BE COMPLETED BEFORE** | | |
|  | | |
| **TO BE COMPLETED BY THE ORGANIZATION** | | **ROOT CAUSE ANALYSIS (What failed in the system to allow this NC to occur ?)** | | | | | | | | | |
|  | | | | | | | | | |
| **CORRECTION & CORRECTIVE ACTION (What is done to solve this problem and to prevent recurrence)** | | | | | | | | | |
| CORRECTION:  CORRECTIVE ACTION: | | | | | | | | | |
| **VERIFICATION OF CORRECTIVE ACTIONS** | | | **DATE OF COMPLETION** | |  | | | | |
| **ORGANIZATION REPRESENTATIVE** | |  | | | | |
| **TO BE COMPLETED BY AUDITOR** | | **VERIFICATION OF CORRECTIONS / CORRECTIVE ACTIONS** | | | **DATE** | | **STATUS** | **LEAD AUDITOR** | | | |
|  | |  |  | | | |
| **AUDITOR COMMENTS (including evidences verified to accept the corrections/ correcive actions)** | | |  | | | | | | |

# Annex B: Certification Information

|  |  |  |
| --- | --- | --- |
| **GENERAL INFORMATION** | | |
| **Number of Certificates** (for hardcopy) |  | |
| **Languages** | English | French |
| **Name of the company** (to be put in the certificate) |  | |
| **Address** (to be put in the certificate) |  | |
| **Certification Scope Statement** (to be put in the certificate)  **Important Note\***  Certification Statement shall be precise and include **only** the audited sites and processes..  For ISO/IEC 27001, it is obligatory to put SoA version as well. |  | |
| **Excluded clauses in the audited Management System** (to be put in the certificate) |  | |
| **DELIVERY ADDRESS** *(Note\* This shall be the client’s address only)* | | |
| Title (Mr., Ms.) |  | |
| First name |  | |
| Last name |  | |
| Address |  | |
| City |  | |
| Country |  | |
| Province/State/Region |  | |
| ZIP/Postal code |  | |
| Email address |  | |

# Annex C: Surveillance Plan

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Surveillance Plan ISO/IEC 27001:2013/27701:2019** | | | | | | |
| **1**: Initial Audit  **2:** Surveillance 1 Audit  **3**: Surveillance 2 Audit  **4**: Recertification Audit | | | **Plan** | | | |
| **1**  **(202X)** | **2**  **(202X)** | **3**  **(202X)** | **4**  **(202X)** |
| **ISO/IEC 27001:2013/27701:2019 Clauses** | | | | | | |
| **4/5.2 Context of the organization** | | | | | | |
| **4.1/5.2.1** | Understanding the organization and its context | |  |  |  |  |
| **4.2/5.2.2** | Understanding the needs and expectations of interested parties | |  |  |  |  |
| **4.3/5.2.3** | Determining the scope of the information security and privacy management system | |  |  |  |  |
| **4.4/5.2.4** | Information security and privacy management system | |  |  |  |  |
| **5/5.3 Leadership** | | | | | | |
| **5.1/5.3.1** | Leadership and commitment | |  |  |  |  |
| **5.2/5.3.2** | Policy | |  |  |  |  |
| **5.3/5.3.3** | Organizational roles, responsibilities and authorities | |  |  |  |  |
| **6/5.4 Planning** | | | | | | |
| **6.1/5.4.1** | Actions to address risks and opportunities | |  |  |  |  |
| **6.2/5.4.2** | Information security and privacy objectives and planning to achieve them | |  |  |  |  |
| **7/5.5 Support** | | | | | | |
| **7.1/5.5.1** | Resources | |  |  |  |  |
| **7.2/5.5.2** | Competence | |  |  |  |  |
| **7.3/5.5.3** | Awareness | |  |  |  |  |
| **7.4/5.5.4** | Communication | |  |  |  |  |
| **7.5/5.5.5** | Documented information | |  |  |  |  |
| **8/5.6 Operation** | | | | | | |
| **8.1/5.6.1** | Operational planning and control | |  |  |  |  |
| **8.2/5.6.2** | Information security and privacy risk assessment | |  |  |  |  |
| **8.3/5.6.3** | Information security and privacy risk treatment | |  |  |  |  |
| **9/5.7 Performance evaluation** | | | | | | |
| **9.1/5.7.1** | Monitoring, measurement, analysis and evaluation | |  |  |  |  |
| **9.2/5.7.2** | Internal audit | |  |  |  |  |
| **9.3/5.7.3** | Management review | |  |  |  |  |
| **10/5.8 Improvement** | | | | | | |
| **10.1/5.8.1** | Nonconformity and corrective action | |  |  |  |  |
| **10.2/5.8.2** | Continual improvement | |  |  |  |  |
| **Control objectives and controls ISMS/PIMS** | | | | | | |
| **A.5/6.2** | Information security and privacy policies | |  |  |  |  |
| **A.6/6.3** | Organization of information security and privacy | |  |  |  |  |
| **A.7/6.4** | Human resource security | |  |  |  |  |
| **A.8/6.5** | Asset management | |  |  |  |  |
| **A.9/6.6** | Access control | |  |  |  |  |
| **A.10/6.7** | Cryptography | |  |  |  |  |
| **A.11/6.8** | Physical and environmental security | |  |  |  |  |
| **A.12/6.9** | Operations security | |  |  |  |  |
| **A.13/6.10** | Communications security | |  |  |  |  |
| **A.14/6.11** | System acquisition, development and maintenance | |  |  |  |  |
| **A.15/6.12** | Supplier relationships | |  |  |  |  |
| **A.16/6.13** | Information security and privacy incident management | |  |  |  |  |
| **A.17/6.14** | Information security aspects of business continuity management | |  |  |  |  |
| **A.18/6.15** | Compliance | |  |  |  |  |
| **Annex A – PIMS-specific reference control objectives and controls** | | | | | | |
| **A.7.2** | Conditions for collection and processing | |  |  |  |  |
| **A.7.3** | Obligations to PII principals | |  |  |  |  |
| **A.7.4** | Privacy by design and privacy by default | |  |  |  |  |
| **A.7.5** | PII sharing, transfer and disclosure | |  |  |  |  |
| **Annex B – PIMS-specific reference control objectives and controls** | | | | | | |
| **B.8.2** | Conditions for collection and processing | |  |  |  |  |
| **B.8.3** | Obligations to PII principals | |  |  |  |  |
| **B8.4** | Privacy by design and privacy by default | |  |  |  |  |
| **B.8.5** | PII sharing, transfer and disclosure | |  |  |  |  |
| **11. Additional requirements** | | | | | | |
|  | Use of Logo | |  |  |  |  |
|  | List of documents included in the audited MS | |  |  |  |  |
| **Notes and comments:** | |  | | | | |

*For completed visits, mark “X” in the box for each clause/process covered.*

*For planned visits, mark “O” in the box for each clause/process to be covered.*