



**MSECB Certification – ISO/IEC 27001:2022, ISO/IEC 27701:2019 and ISO/IEC 27017:2015**

*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 5

1.1. Organization information 5

1.2. Audit information 5

1.3. Audit Scope 6

2. Audit preparation and methodology 6

2.1. Audit objectives 6

2.2. Audit criteria 6

2.3. Audit methodology 7

2.4. Previous audit results 7

2.5. Audit planning 7

2.6. Key people interviewed 8

2.7. MSECB complaint and appeal process 8

3. Significant audit trails followed 9

4. Audit findings 43

4.1. Audit finding definition 43

4.2. Major nonconformities (see also Annex A) 44

4.3. Minor nonconformities (see also Annex A) 44

4.4. Observations 44

4.5. Opportunities for improvement 44

4.6. Agreed follow-up activities 44

4.7. Uncertainty / obstacles that could affect the reliability of audit conclusions 44

4.8. Unresolved diverging opinions between the audit team & auditee 44

5. Audit conclusions and audit recommendation 45

5.1. System management conformance and capability 45

5.2. Audit conclusions 45

5.3. Recommendation 45

6. Annex A: Nonconformity report 46

6.1. Nonconformity Report 46

7. Annex B: Certification Information 47

8. Annex C: Surveillance Plan 48

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, 2022.The main objective of this audit was to assess if the MS has been successfully implemented and effective, as well as to evaluate the conformance of the organization to the ISO/IEC 27001:2022, ISO/IEC 27701:2019, and ISO/IEC 27017:2015 requirements. Based on these assessments and evaluations, a decision has been made whether to recommend your organization for certification against ISO/IEC 27001:2022, ISO/IEC 27701:2019, and ISO/IEC 27017:2015.

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/IEC 17021, which are accepted worldwide. Those standards require our audit team to plan and perform the audit to acquire reasonable assurance whether your company’s management system is effective and all requirements of ISO/IEC 27001:2022, ISO/IEC 27701:2019, and ISO/IEC 27017:2015 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 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 27001:2022, ISO/IEC 27701:2019, and ISO/IEC 27017:2015.

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 Security Management (PIMS) including evaluation of conformity to the requirements of ISO/IEC 27001:2022, ISO/IEC 27701:2019, and ISO/IEC 27017:2015.

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 standard (Clause 4 to 10 of ISO/IEC 27001:2022 and ISO/IEC 27701:2019).

The management system conforms with all applicable legal and regulatory requirements.

The management system is capable of achieving the objectives of the organization’s policies.

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 27001:2022, ISO/IEC 27701:2019, and ISO/IEC 27017:2015.

## Audit criteria

The audit criteria (the set of requirements) for this audit are all normative clauses of ISO/IEC 27001:2022, ISO/IEC 27701:2019, and ISO/IEC 27017:2015:

Clause 4 – Context of the organization

Clause 5 – Leadership

Clause 6 – Planning

Clause 7 – Support

Clause 8 – Operation

Clause 9 – Performance evaluation

Clause 10 – Improvement

Annex A – Information security controls reference

Additional requirements

Use of logo and trademark

Documentation and processes defined in the management system developed by the client.

## 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 preparation for this audit 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 ISMS 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: [www.msecb.com](http://www.msecb.com)

# 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/IEC 27001 requirements/PIMS specific requirements related to ISO/IEC 27001:2022** | | | |  |
| **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 ISMS\*\* |  |  |  |
| 4.4/5.2.4 | Information security 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 |  |  |  |
| 6.1.1/5.4.1.1 | General |  |  |  |
| 6.1.2/5.4.1.2 | Information security risk assessment\*\* |  |  |  |
| 6.1.3/5.4.1.3 | Information security risk treatment\*\* |  |  |  |
| 6.2/5.4.2 | Information security objectives and planning to achieve them |  |  |  |
| 6.3 | Planning of changes |  |  |  |
| **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 |  |  |  |
| 7.5.1/5.5.5.1 | General |  |  |  |
| 7.5.2/5.5.5.2 | Creating and updating |  |  |  |
| 7.5.3/5.5.5.3 | Control of documented information |  |  |  |
| **8/5.6 Operation** | | | | |
| 8.1/5.6.1 | Operational planning and control |  |  |  |
| 8.2/5.6.2 | Information security risk assessment |  |  |  |
| 8.3/5.6.3 | Information security risk treatment |  |  |  |
| **9/5.7 Performance evaluation** | | | | |
| 9.1/5.7.1 | Monitoring, measurement, analysis and evaluation |  |  |  |
| 9.2/5.7.2 | Internal audit |  |  |  |
| 9.2.1 | General |  |  |  |
| 9.2.2 | Internal audit program |  |  |  |
| 9.3/5.7.3 | Management review |  |  |  |
| 9.3.1 | General |  |  |  |
| 9.3.2 | Management review inputs |  |  |  |
| 9.3.3 | Management review results |  |  |  |
| **10/5.8 Improvement** | | | | |
| 10.1/5.8.2 | Continual improvement |  |  |  |
| 10.2/5.8.1 | Nonconformity and corrective action |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **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 |  |
| **A.5 Organizational controls** | | | | |
| A 5.1/6 2.1.1/6.3.2.1 | **Policies for information security\*\*.** Control. Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur. |  |  |  |
| Control 5.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. Sector-specific guidance also applies: - Cloud service customer - Cloud service provider - Other information for cloud services  (27017). |
| A 5.2/6.3.1.1 | **Information security roles and responsibilities\*\*.**  Control. Information security roles and responsibilities shall be defined and allocated according to the organization needs. |  |  |  |
| Control 6.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. Sector-specific guidance also applies: - Cloud service customer - Cloud service provider - Other information for cloud services (27017) |
| A 5.3/6.3.1.2 | **Segregation of duties\*\***  Control. Conflicting duties and conflicting areas of responsibility shall be segregated. |  |  |  |
| A 5.4/6.3.2.1 | **Management responsibilities**  Control. Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization. |  |  |  |
| A 5.5 /6.3.1.3 | **Contact with authorities\*\***  Control. The organization shall establish and maintain contact with relevant authorities. |  |  |  |
| Control 6.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. Sector-specific guidance also applies: - Cloud service customer - Cloud service provider - Other information for cloud services (27017) |
| A 5.6/6.3.1.4 | **Contact with special interest groups\*\***  Control. The organization shall establish and maintain contact with special interest groups or other special security forums and professional associations. |  |  |  |
| A 5.7 | **Threat intelligence**  Control. Information relating to information security threats shall be collected and analyzed to produce threat intelligence. |  |  |  |
| A 5.8/6.3.1.5 | **Information security in project management\*\***  Control. Information security shall be integrated into project management. |  |  |  |
| A 5.9 | **Inventory of information and other associated assets**  Control. An inventory of information and other associated assets, including owners, shall be developed and maintained. |  |  |  |
| Control 8.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. Sector-specific guidance also applies: -Cloud service customer -Cloud service provider -Other information for cloud services (27017) |
| A 5.10 | **Acceptable use of information and other associated assets**  Control. Rules for the acceptable use and procedures for handling information and other assets shall be identified, documented and implemented. |  |  |  |
| A 5.11 | **Return of assets**  Control. Personnel and other interested parties as appropriate shall return all the organization’s assets in their possession upon change or termination of their employment, contract or agreement. |  |  |  |
| A 5.12/6.5.2.1 | **Classification of information\*\***  Control. Information shall be classified according to the information security needs of their organization based on confidentiality, integrity, availability and relevant interested party requirements. |  |  |  |
| A 5.13/6.5.2.2 | **Labelling of information\*\***  Control. An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization. |  |  |  |
| Control 8.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. Sector-specific guidance also applies: -Cloud service customer -Cloud service provider (27017) |
| A 5.14/6.5.3.3/ 6.10.2.1 | **Information transfer\*\***  Control. Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties. |  |  |  |
| A 5.15 | **Access control**  Control. Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements. |  |  |  |
| **CLD.9.5** Access control of cloud service customer data in shared virtual environment. |
| A 5.16 | **Identity management**  Control. The full life cycle of identities shall be managed. |  |  |  |
| A 5.17 | **Authentication information**  Control. Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information. |  |  |  |
| Control 9.2.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. Sector-specific guidance also applies: - Cloud service customer - Cloud service provider - Other information for cloud services (27017) |
| A 5.18 | **Access rights**  Control. Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization’s topic-specific policy on and rules for access control. |  |  |  |
| Control 9.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.  - Cloud service customer - Cloud service provider  (27017) |
| Control 9.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.  - Cloud service customer - Cloud service provider  (27017) |
| Control 9.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.  - Cloud service customer - Cloud service provider - Other information for cloud services (27017) |
| A 5.19 | **Information security in supplier relationships**  Control. Processes and procedures shall be defined and implemented to manage the information security risk associated with the use of supplier’s products or services. |  |  |  |
| Control 15.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. Sector-specific guidance also applies: - Cloud service customer - Cloud service provider  (27017) |
| A 5.20/6.12.1.2 | **Addressing information security within supplier agreements\*\***  Control. Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship. |  |  |  |
| Control 15.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. Sector-specific guidance also applies: - Cloud service customer - Cloud service provider  (27017) |
| A 5.21 | **Managing information security in the information and communication technology (ICT) supply chain**  Control. Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain. |  |  |  |
| Control 15.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. Sector-specific guidance also applies: - Cloud service customer - Cloud service provider  (27017) |
| A 5.22 | **Monitoring, review and change management of supplier services.**  Control. The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery. |  |  |  |
| A 5.23 | **Information security for use of cloud services**  Control. Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization’s information security requirements. |  |  |  |
| A 5.24/6.13.1.1 | **Information security incident management planning and preparation\*\***  Control. The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities. |  |  |  |
| Control 16.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.  Sector-specific guidance also applies: - Cloud service customer - Cloud service provider  (27017) |
| A 5.25 | **Assessment and decision on information security events**  Control. The organization shall assess information security events and decide if they are to be categorized as information security incidents. |  |  |  |
| A 5.26/6.13.1.5 | **Response to information security incidents\*\***  Control. Information security incidents shall be responded to in accordance with the documented procedures. |  |  |  |
| A 5.27 | **Learning from information security incidents**  Control. Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls. |  |  |  |
| A 5.28 | **Collection of evidence**  Control. The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events. |  |  |  |
| Control 16.1.7 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. Sector-specific guidance also applies: - Cloud service customer - Cloud service provider (27017) |
| A 5.29 | **Information security during disruption**  Control. The organization shall plan how to maintain information security at an appropriate level during disruption. |  |  |  |
| A 5.30 | **ICT refines for business continuity.**  Control. ICT Readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements. |  |  |  |
| A 5.31/6.15.1.1 | **Legal, statutory, regulatory and contractual requirements\*\***  Control. Legal, statutory, regulatory and contractual requirements related to information security and the organization’s approach to meet these requirements shall be identified, documented and kept up to date. |  |  |  |
| Control 18.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. Sector-specific guidance also applies: - Cloud service customer - Cloud service provider  - Other information for cloud services (27017) |
| A 5.32 | **Intellectual property rights**  Control. The organization shall implement appropriate procedures to protect intellectual property rights. |  |  |  |
| Control 18.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. Sector-specific guidance also applies: - Cloud service customer - Cloud service provider  (27017) |
| A 5.33/6.15.1.3 | **Protection of records\*\***  Control. Record shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release. |  |  |  |
| Control 18.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. Sector-specific guidance also applies: - Cloud service customer - Cloud service provider  (27017) |
| A 5.34 | **Privacy protection of personal identifiable information (PII)**  Control. The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements. |  |  |  |
| A 5.35/6.15.2.1 | **Independent review of information security\*\***  Control. The organization’s approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur. |  |  |  |
| Control 18.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. Sector-specific guidance also applies: - Cloud service customer - Cloud service provider  (27017) |
| A 5.36/6.15.2.3 | **Compliance with policies, rules and standards for information security\*\***  Control. Compliance with the organization’s information security policy, topic-specific policies, rules and standards shall be regularly reviewed. |  |  |  |
| A 5.37 | **Documented operating procedures.**  Control. Operating procedures for information processing facilities shall be documented and made available to personnel who need them. |  |  |  |
| CLD 8.1.5 | **Removal of cloud service customer assets.** Assets of the cloud service customer that are on the cloud service provider’s premises should be removed, and returned if necessary, in a timely manner upon termination of the cloud service agreement.  (ISO 27017) |  |  |  |
| **A.6 People controls** | | | | |
| A 6.1 | **Screening**  Control. Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks. |  |  |  |
| A 6.2 | **Terms and conditions of employment**  Control. The employment contractual agreements shall state the personnel’s and the organization’s responsibilities for information security. |  |  |  |
| A 6.3/6.4.2.2 | **Information security awareness education and training\*\***  Control. Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization’s information security policy, topic-specific policies and procedures, as relevant for their job function. |  |  |  |
| Control 7.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. Sector-specific guidance also applies: - Cloud service customer - Cloud service provider (27017) |
| A 6.4 | **Disciplinary process**  Control. A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation. |  |  |  |
| A 6.5 | **Responsibilities after termination or change of employment.**  Control. Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties. |  |  |  |
| A 6.6/6.10.2.4 | **Confidentiality or non-disclosure agreements\*\***  Control. Confidentiality or non-disclosure agreements reflecting the organization’s needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties. |  |  |  |
| A 6.7 | **Remote working**  Control. Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization’s premises. |  |  |  |
| A 6.8 | **Information security event reporting**  Control. The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in timely manner. |  |  |  |
| Control 16.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. Sector-specific guidance also applies: - Cloud service customer - Cloud service provider  - Other information for cloud services (27017) |
| CLD 6.3.1 | **Cloud service customer:**  The cloud service customer should define or extend its existing policies and procedures in accordance with its use of cloud services, and make cloud service users aware of their roles and responsibilities in the use of the cloud service.  **Cloud service provider:**  The cloud service provider should document and communicate its information security capabilities, roles, and responsibilities for the use of its cloud service, along with the information security roles and responsibilities for which the cloud service customer would need to implement and manage as part of its use of the cloud service.  (ISO 27017) |  |  |  |
| **A.7 Physical controls** | | | | |
| A 7.1 | **Physical security perimeters**  Control. Security perimeters shall be defined and used to protect areas that contain information and other associated assets. |  |  |  |
| A 7.2 | **Physical entry**  Control. Secure areas shall be protected by appropriate entry controls and access points. |  |  |  |
| A 7.3 | **Securing offices, rooms and facilities**  Control. Physical security for offices, rooms and facilities shall be designed and implemented. |  |  |  |
| A 7.4 | **Physical security monitoring**  Control. Premises shall be continuously monitored for unauthorized physical access. |  |  |  |
| A 7.5 | **Protecting against physical and environmental threats**  Control. Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented. |  |  |  |
| A 7.6 | **Working in secure areas**  Control. Security measures for working in secure areas shall be designed and implemented. |  |  |  |
| A 7.7/6.5.3.1/ 6.8.2.9 | **Clear desk and clear screen\*\***  Control. Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced. |  |  |  |
| A 7.8 | **Equipment siting and protection**  Control. Equipment shall be sited securely and protected. |  |  |  |
| A 7.9 | **Security of assets off-premises**  Control, Off-site assets shall be protected. |  |  |  |
| A 7.10/6.5.3.2 | **Storage media\*\***  Control. Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization’s classification scheme and handling requirements. |  |  |  |
| A 7.11 | **Supporting utilities**  Control. Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities. |  |  |  |
| A 7.12 | **Cabling security**  Control. Cables varying power, data or supporting information services shall be protected from interception, interference or damage. |  |  |  |
| A 7.13 | **Equipment maintenance**  Control. Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information. |  |  |  |
| A 7.14 | **Secure disposal or re-use of equipment**  Control. 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. |  |  |  |
| Control 11.2.7 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. Sector-specific guidance also applies: - Cloud service customer - Cloud service provider - Other information for cloud services (27017) |
| **A.8 Technological Controls** | | | | |
| A 8.1 | **User end point devices**  Control. Information stored on, processed by or accessible via user end point devices shall be protected. |  |  |  |
| A 8.2 | **Privileged access rights**  Control. The allocation and use of privileged access rights shall be restricted and managed. |  |  |  |
| Control 9.2.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies:  - Cloud service customer - Cloud service provider - Other information for cloud services (27017) |
| A 8.3 | **Information access restriction**  Control. Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control. |  |  |  |
| Control 9.4.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. Sector-specific guidance also applies: - Cloud service customer - Cloud service provider - Other information for cloud services (27017) |
| A 8.4 | **Access to source code**  Control. Read and write access to source code, development tools and software libraries shall be appropriately managed. |  |  |  |
| A 8.5 | **Secure authentication**  Control. Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control. |  |  |  |
| A 8.6 | **Capacity management**  Control. The use of resources shall be monitored and adjusted in line with current and expected capacity requirements. |  |  |  |
| Control 12.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. Sector-specific guidance also applies: - Cloud service customer - Cloud service provider - Other information for cloud services  (27017) |
| A 8.7 | **Protection against malware**  Control. Protection against malware shall be implemented and supported by appropriate user awareness. |  |  |  |
| A 8.8 | **Management of technical vulnerabilities**  Control. Information about technical vulnerabilities of information systems in use shall be obtained, the organization’s exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken. |  |  |  |
| Control 12.6.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. Sector-specific guidance also applies: - Cloud service customer - Cloud service provider (27017) |
| A 8.9 | **Configuration management**  Control. Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed. |  |  |  |
| CLD.13.1.4 **Alignment of security management for virtual and physical networks.** Upon configuration of virtual networks, consistency of configurations between virtual and physical networks should be verified based on the cloud service provider’s network security policy. |
| A 8.10 | **Information deletion**  Control. Information stored in information systems, devices or in any other storage media shall be deleted when no longer required. |  |  |  |
| A 8.11 | **Data masking**  Control. Data masking shall be used in accordance with the organization’s topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration. |  |  |  |
| A 8.12 | **Data leakage prevention**  Control. Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information. |  |  |  |
| A 8.13 | **Information backup**  Control. Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup. |  |  |  |
| Control 12.3.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. Sector-specific guidance also applies: - Cloud service customer - Cloud service provider - Other information for cloud services  (27017) |
| A 8.14 | **Redundancy of information processing facilities**  Control. Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements. |  |  |  |
| A 8.15 | **Logging**  Control. Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analyzed. |  |  |  |
| Control 12.4.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. Sector-specific guidance also applies: - Cloud service customer - Cloud service provider - Other information for cloud services  (27017) |
| Control 12.4.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. Sector-specific guidance also applies: - Cloud service customer - Cloud service provider - Other information for cloud services  (27017) |
| A 8.16 | **Monitoring activities**  Control. Networks, systems and applications shall be monitored for anomalous behavior and appropriate actions taken to evaluate potential information security incidents. |  |  |  |
| CLD 12.4.5 **Monitoring of Cloud Services.** The cloud service customer should have the capability to monitor specified aspects of the operation of the cloud service that the cloud service customer uses.  (ISO 27017) |
| A 8.17 | **Clock synchronization**  Control. The clock of information processing systems used by the organization shall be synchronized to approved time sources. |  |  |  |
| Control 12.4.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. Sector-specific guidance also applies: - Cloud service customer - Cloud service provider - Other information for cloud services  (27017) |
| A 8.18 | **Use of privileged utility programs**  Control. The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled. |  |  |  |
| Control 9.4.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. Sector-specific guidance also applies: - Cloud service customer - Cloud service provider (27017) |
| A 8.19 | **Installation of software on operational systems**  Control. Procedures and measures shall be implemented to securely manage software installation on operational systems. |  |  |  |
| A 8.20 | **Networks security**  Control. Networks and network devices shall be secured, managed and controlled to protect information in systems and applications. |  |  |  |
| A 8.21 | **Security of network services**  Control. Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored. |  |  |  |
| A 8.22 | **Segregation of networks**  Control. Groups of information services, users and information systems shall be segregated in the organization’s networks. |  |  |  |
| Control 13.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. Sector-specific guidance also applies: - Cloud service customer - Cloud service provider - Other information for cloud services  (27017) |
| CLD.9.5.1 **Segregation in virtual computing environments.** A cloud service customer’s virtual environment running on a cloud service should be protected from other cloud service customer and unauthorized persons.  (ISO 27017) |
| A 8.23 | **Web filtering**  Control. Access to external websites shall be managed to reduce exposure to malicious content. |  |  |  |
| A 8.24 | **Use of cryptography**  Control. Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented. |  |  |  |
| Control 10.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. Sector-specific guidance also applies. - Cloud service customer - Cloud service provider - Other information for cloud services (27017) |
| Control 10.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. Sector-specific guidance also applies: - Cloud service customer - Cloud service provider  (27017) |
| Control 18.1.5 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. Sector-specific guidance also applies: - Cloud service customer - Cloud service provider  (27017) |
| A 8.25 | **Secure development life cycle**  Control. Rules for the secure development of software and systems shall be established and applied. |  |  |  |
| Control 14.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. Sector-specific guidance also applies: - Cloud service customer - Cloud service provider - Other information for cloud services  (27017) |
| A 8.26 | **Application security requirements**  Control. Information security requirements shall be identified, specified and approved when developing or acquiring applications. |  |  |  |
| A 8.27 | **Secure system architecture and engineering principles**  Control. Principles for engineering secure systems shall be established, documented, maintained, and applied to any information system development activities. |  |  |  |
| Control 14.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. Sector-specific guidance also applies. - Cloud service customer - Cloud service provider - Other information for cloud services  (27017) |
| A 8.28 | **Secure coding**  Control. Secure coding principles shall be applied to software development. |  |  |  |
| A 8.29 | **Security testing in development and acceptance**  Control. Security testing processes shall be defined and implemented in development life cycle. |  |  |  |
| A 8.30 | **Outsourced development**  Control. The organization shall direct, monitor and review the activities related to outsourced system development |  |  |  |
| A 8.31 | **Separation of development, test and production environments**  Control. Development, testing and production environments shall be separated and secured. |  |  |  |
| A 8.32 | **Change management**  Control. Changes to information processing facilities and information systems shall be subject to change management procedures. |  |  |  |
| Control 12.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. Sector-specific guidance also applies: - Cloud service customer - Cloud service provider - Other information for cloud services  (27017) |
| A 8.33 | **Test information**  Control. Test information shall be appropriately selected, protected and managed. |  |  |  |
| A 8.34 | **Protection of information systems during audit testing**  Control. Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management. |  |  |  |
| CLD 9.5.2 | **Virtual machine hardening.** Virtual machines in a cloud computing environment should be hardened to meet business needs.  (ISO 27017) |  |  |  |
| CLD 12.1.5 | **Administrator’s operation security.** Procedures for administrative operations of a cloud computing environment should be defined, documented and monitored.  (ISO 27017) |  |  |  |

**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 27001:2022 | | | | |
| **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\***  Scope Statement should be concise and shall indicate **only** the processes and procedures within the management system that were assessed during the audit.  Company’s name or address should not be written in this statement as they are mentioned in dedicated spaces.  For ISO 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** | | |
| 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 27001:2022, ISO/IEC 27701:2019 and ISO/IEC 27017:2015** | | | | | | |
| **1**: Initial Audit  **2:** Surveillance 1 Audit  **3**: Surveillance 2 Audit  **4**: Recertification Audit | | | **Plan** | | | |
| **1**  **(202X)** | **2**  **(202X)** | **3**  **(202X)** | **4**  **(202X)** |
| **Clauses and Controls** | | | | | | |
| **4 Context of the organization** | | | | | | |
| **4.1** | Understanding the organization and its context | |  |  |  |  |
| **4.2** | Understanding the needs and expectations of interested parties | |  |  |  |  |
| **4.3** | Determining the scope of the information security management system | |  |  |  |  |
| **4.4** | Information security management system | |  |  |  |  |
| **5 Leadership** | | | | | | |
| **5.1** | Leadership and commitment | |  |  |  |  |
| **5.2** | Policy | |  |  |  |  |
| **5.3** | Organizational roles, responsibilities and authorities | |  |  |  |  |
| **6 Planning** | | | | | | |
| **6.1** | Actions to address risks and opportunities | |  |  |  |  |
| **6.2** | Information security objectives and planning to achieve them | |  |  |  |  |
| **6.3** | Planning of changes | |  |  |  |  |
| **7 Support** | | | | | | |
| **7.1** | Resources | |  |  |  |  |
| **7.2** | Competence | |  |  |  |  |
| **7.3** | Awareness | |  |  |  |  |
| **7.4** | Communication | |  |  |  |  |
| **7.5** | Documented information | |  |  |  |  |
| **8 Operation** | | | | | | |
| **8.1** | Operational planning and control | |  |  |  |  |
| **8.2** | Information security risk assessment | |  |  |  |  |
| **8.3** | Information security risk treatment | |  |  |  |  |
| **9 Performance Evaluation** | | | | | | |
| **9.1** | Monitoring, measurement, analysis and evaluation | |  |  |  |  |
| **9.2** | Internal audit | |  |  |  |  |
| **9.3** | Management review | |  |  |  |  |
| **10 Improvement** | | | | | | |
| **10.1** | Continual improvement | |  |  |  |  |
| **10.2** | Nonconformity and corrective action | |  |  |  |  |
| **Control objectives and controls** | | | | | | |
| **A.5** | Organizational controls | |  |  |  |  |
| **A.6** | People controls | |  |  |  |  |
| **A.7** | Physical Controls | |  |  |  |  |
| **A.8** | Technological controls | |  |  |  |  |
| **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 esach clause/process to be covered.*