

**

**MSECB Certification –ISO/IEC 27018:2019**

*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 5

1.1. Organization information 5

1.2. Audit information 5

1.3. Audit Scope 5

2. Audit preparation and methodology 6

2.1. Audit objectives 6

2.2. Audit criteria 6

2.3. Audit methodology 6

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 13

4.1. Audit finding definition 13

4.2. Major nonconformities (see also Annex A) 14

4.3. Minor nonconformities (see also Annex A) 14

4.4. Observations 14

4.5. Opportunities for improvement 14

4.6. Agreed follow-up activities 14

4.7. Uncertainty / obstacles that could affect the reliability of audit conclusions 14

4.8. Unresolved diverging opinions between the audit team & auditee 14

5. Audit conclusions and audit recommendation 15

5.1. System management conformance and capability 15

5.2. Audit conclusions 15

5.3. Recommendation 15

6. Annex A: Nonconformity report 16

6.1. Nonconformity Report 16

7. Annex B: Certification Information 17

8. Annex C: Surveillance Plan 18

Place, and Date

To Mr. John Smith (example)

Organization Name

I have audited Company ABC (Organization Name) compliance to the ISO/IEC 27018:2019 from May 12th to May 15th 2017.The main objective of this audit was to evaluate whether the organization has successfully implemented the ISO/IEC 27018:2019 requirements and the effectiveness of its implementation. Based on these audits and evaluations, a decision has been made whether or not to recommend your organization for attestation against ISO/IEC 27018:2019.

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/IEC 17021, which are accepted worldwide. Those standards require our audit team to plan and perform the audit in order to acquire reasonable assurance whether your organization has met all requirements of ISO/IEC 27018:2019.

During the audit process, the organization has proven overall conformity with the requirements of the standard. The audit team has concluded that your organization has 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 is in compliance with ISO/IEC 27018:2019.

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 within the scope** |
| 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 standard 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 ISO/IEC 27018:2019.

The specific objectives of this audit are to confirm that:

* The organization has determined the boundaries and applicability of the standard in scope;
* The organization system conforms with all the requirements of the audit standard (Clause 5 to 18 of ISO/IEC 27018:2019);
* The organization system conforms with all applicable legal and regulatory requirements;
* The organization system is capable of achieving the organization’s policies objectives;
* The organization has established, implemented, maintained and continually improved its system, including the processes needed and their interactions, in accordance with the requirements of the ISO/IEC 27018:2019*.*

## Audit criteria

The audit criteria (the set of requirements) for this are all normative clauses of ISO/IEC 27018:2019:

* Clause 5 – Information security policies
* Clause 6 – Organization of information security
* Clause 7 – Human resource security
* Clause 8 – Asset Management
* Clause 9 – Access control
* Clause 10 – Cryptography
* Clause 11 – Physical and environmental security
* Clause 12 – Operations security
* Clause 13 – Communications security
* Clause 14 – System acquisition, development and maintenance
* Clause 15 – Supplier relationships
* Clause 16 – Information security incident management
* Clause 17 – Information security aspects of business continuity management
* Clause 18 - Compliance
* 11 - Additional requirements
	+ - Use of logo and trademark
		- Documentation and processes 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 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.*

| **Control Objective and Controls** | **Status** | **Audit Evidence** | **No. of NC** |
| --- | --- | --- | --- |
|  |  | Findings/justification of findings/specifics/notes |  |
| **5 Information security policies** |
| **5.1 Management direction for information security**Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations. |
| 5.1.1 | **Policies for information security.** Control. A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties. |  |  |  |
| 5.1.2 | **Review of the policies for information security.** Control.The policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness. |  |  |  |
| **6 Organization of information security** |
| **6.1 Internal organization**Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization. |
| 6.1.1 | **Information security roles and responsibilities.** Control. All information security responsibilities should be defined and allocated. |  |  |  |
| 6.1.2 | **Segregation of duties.** Control. Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization’s assets. |  |  |  |
| 6.1.3 | **Contact with authorities.** Control. Appropriate contacts with relevant authorities should be maintained. |  |  |  |
| 6.1.4 | **Contact with special interest groups.** Control. Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained. |  |  |  |
| 6.1.5 | **Information security in project management.** Control. Information security should be addressed in project management, regardless of the type of the project. |  |  |  |
| **6.2 Mobile devices and teleworking**Objective: A policy and supporting security measures should be implemented to protect information accessed, processed or stored at teleworking sites. |
| 6.2 | **Mobile devices and teleworking** |  |  |  |
| **7 Human resource security** |
| **7.1 Prior to employment**Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered. |
| **7.2 During employment**Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities. |
| 7.2.1 | **Management responsibilities.** Control. Management should require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization. |  |  |  |
| 7.2.2 | **Information security awareness, education and training**. Control. All employees of the organization and, where relevant, contractors should receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function. |  |  |  |
| 7.2.3 | **Disciplinary process.** Control. There should be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach. |  |  |  |
| **8 Asset management** |  |
| **8 Asset management**Objective: To identify organizational assets and define appropriate protection responsibilities.  |
| 8 | **Asset management** |  |  |  |
| **9 Access control** |  |
| **9.1 Business requirements of access control**Objective: To limit access to information and information processing facilities. |  |
| 9.1 | Business requirements of access control |  |  |  |
| 9.2 User access managementObjective: To ensure authorized user access and to prevent unauthorized access to systems and services. |
| 9.2.1 | **User registration and de-registration.** Control. A formal user registration and de-registration process should be implemented to enable assignment of access rights. |  |  |  |
| 9.2.2 | **User access provisioning.** Control. A formal user access provisioning process should be implemented to assign or revoke access rights for all user types to all systems and services. |  |  |  |
| 9.2.3 | **Management of privileged access rights.** Control. The allocation and use of privileged access rights should be restricted and controlled. |  |  |  |
| 9.2.4 | **Management of secret authentication information of users.** Control. The allocation of secret authentication information should be controlled through a formal management process. |  |  |  |
| 9.2.5 | **Review of user access rights.** Control. Asset owners should review users’ access rights at regular intervals. |  |  |  |
| 9.2.6 | **Removal or adjustment of access rights.** Control. The access rights of all employees and external party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change. |  |  |  |
| **9.3 User responsibilities**Objective: To make users accountable for safeguarding their authentication information. |
| 9.3.1 | **Use of secret authentication information.** Control. Users should be required to follow the organization’s practices in the use of secret authentication information. |  |  |  |
| **9.4 System and application access control**Objective: To prevent unauthorized access to systems and applications. |
| 9.4.1 | **Information access restriction.** Control.Access to information and application system functions should be restricted in accordance with the access control policy. |  |  |  |
| 9.4.2 | **Secure log-on procedures.** Control.Where required by the access control policy, access to systems and applications should be controlled by a secure log-on procedure. |  |  |  |
| 9.4.3  | **Password management system.** Control.Password management systems should be interactive and should ensure quality passwords. |  |  |  |
| 9.4.4 | **Use of privileged utility programs.** Control.The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled. |  |  |  |
| 9.4.5 | **Access control to program source code.** Control.Access to program source code should be restricted. |  |  |  |
| **10 Cryptography** |  |
| **10.1 Cryptography controls**Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information. |  |
| 10.1.1 | **Policy on the use of cryptographic controls.** Control. A policy on the use of cryptograpghic controls for protection of information should be developed and implemented. |  |  |  |
| 10.1.2 | **Key management.** Control. A policy on the use, protection and lifetime of cryptographic keys should be developed and implemented through their whole lifecycle. |  |  |  |
| **11 Physical and environmental security** |  |
| **11.1 Secure areas**Objective: To prevent unauthorized physical access, damage and interference to the organization’s information and information processing facilities. |
| 11.1 | **Secure areas** |  |  |  |
| **11.2 Equipment**Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization’s operations. |  |
| 11.2.1 | **Equipment siting and protection.** Control. Equipment should be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. |  |  |  |
| 11.2.2 | **Supporting utilities.** Control. Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities. |  |  |  |
| 11.2.3 | **Cabling security.** Control. Power and telecommunications cabling carrying data or supporting information services should be protected from interception, interference or damage. |  |  |  |
| 11.2.4 | **Equipment maintenance.** Control. Equipment should be correctly maintained to ensure its continued availability and integrity. |  |  |  |
| 11.2.5 | **Removal of assets.** Control. Equipment, information or software should not be taken off-site without prior authorization. |  |  |  |
| 11.2.6 | **Security of equipment and assets off-premises.** Control. Security should be applied to off-site assets taking into account the different risks of working outside the organization’s premises. |  |  |  |
| 11.2.7 | **Secure disposal or re-use of equipment.** Control. All items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use. |  |  |  |
| 11.2.8 | **Unattended user equipment.** Control. Users should ensure that unattended equipment has appropriate protection. |  |  |  |
| 11.2.9 | **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 should be adopted. |  |  |  |
| **12 Operations security** |  |
| **12.1 Operational procedures and responsibilities**Objective: To ensure correct and secure operations of information processing facilities. |
| 12.1.1 | **Documented operating procedures.** Control. Operating procedures should be documented and made available to all users who need them. |  |  |  |
| 12.1.2 | **Change management.** Control. Changes to the organization, business processes, information processing facilities and systems that affect information security should be controlled. |  |  |  |
| 12.1.3 | **Capacity management.** Control. The use of resources should be monitored, tuned and projections made of future capacity requirements to ensure the required system performance. |  |  |  |
| 12.1.4 | **Separation of development, testing and operational environments.** Control. Development, testing, and operational environments should be separated to reduce the risks of unauthorized access or changes to the operational environment. |  |  |  |
| **12.2 Protection from malware**Objective: To ensure that information and information processing facilities are protected against malware. |
| 12.2 | **Protection from malware** |  |  |  |
| **12.3 Backup**Objective: To protect against loss of data |
| 12.3.1 | **Information backup.** Control.Backup copies of information, software and system images should be taken and tested regularly in accordance with an agreed backup policy. |  |  |  |
| **12.4 Logging and monitoring**Objective: To record events and generate evidence. |
| 12.4.1 | **Event logging.** Control.Event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed. |  |  |  |
| 12.4.2 | **Protection of log information.** Control.Logging facilities and log information should be protected against tampering and unauthorized access. |  |  |  |
| 12.4.3 | **Administrator and operator logs.** Control.System administrator and system operator activities should be logged and the logs protected and regularly reviewed. |  |  |  |
| 12.4.4 | **Clock synchronization. Control.** The clocks of all relevant information processing systems within an organization or security domain should be synchronized to a single reference time source. |  |  |  |
| 12.4.5 | **Control of operational software.** Control.Procedures should be implemented to control the installation of software on operational systems. |  |  |  |
| 12.4.6 | **Technical vulnerability management.** Control.Information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organization’s exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk. |  |  |  |
| 12.4.7 | **Information systems audit considerations.** Control.Audit requirements and activities involving verification of operational systems should be carefully planned and agreed to minimize disruptions to business processes. |  |  |  |
| **13 Communications security** |
| **13.1 Network security management**Objective: To ensure the protection of information in networks and its supporting information processing facilities. |
| 13.1 | **Network security management** |  |  |  |
| **13.2 Information transfer**Objective: To maintain the security of information transferred within an organization and with any external entity. |
| 13.2.1 | **Information transfer policies and procedures.** Control.Formal transfer policies, procedures and controls should be in place to protect the transfer of information through the use of all types of communication facilities. |  |  |  |
| 13.2.2 | **Agreements on information transfer.** Control.Agreements should address the secure transfer of business information between the organization and external parties. |  |  |  |
| 13.2.3 | **Electronic messaging.** Control.Information involved in electronic messaging should be appropriately protected. |  |  |  |
| 13.2.4 | **Confidentiality or non-disclosure agreements.** Control.Requirements for confidentiality or non-disclosure agreements reflecting the organization’s needs for the protection of information should be identified, regularly reviewed and documented. |  |  |  |
| **14 System acquisition, development and maintenance** |
| 14 | **System acquisition, development and maintenance** |  |  |  |
| **15 Supplier relationships** |
| 15 | **Supplier relationships**  |  |  |  |
| **16 Information security incident management** |
| **16.1 Management of information security incidents and improvements**Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.  |
| 16.1.1 | **Responsibilities and procedures.** Control. Management responsibilities and procedures should be established to ensure a quick, effective and orderly response to information security incidents. |  |  |  |
| 16.1.2 | **Reporting information security events.** Control.Information security events should be reported through appropriate management channels as quickly as possible. |  |  |  |
| 16.1.3 | **Reporting information security weaknesses.** Control.Employees and contractors using the organization’s information systems and services should be required to note and report any observed or suspected information security weaknesses in systems or services. |  |  |  |
| 16.1.4 | **Assessment of and decision on information security events.** Control.Information security events should be assessed and it should be decided if they are to be classied as information security incidents. |  |  |  |
| 16.1.5 | **Response to information security incidents.** Control.Information security incidents should be responded to in accordance with the documented procedures. |  |  |  |
| 16.1.6 | **Learning from information security incidents.** Control.Knowlegde gained from analyzing and resolving information security incidents should be used to reduce the likelihood or impact of future incidents. |  |  |  |
| 16.1.7 | **Collection of evidence.** Control.The organization should define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence. |  |  |  |
| **17 Information security aspects of business continuity management** |
| 17 | **Information security aspects of business continuity management** |  |  |  |
| **18 Compliance** |
| **18.1 Compliance with legal and contractual requirements**Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements. |
| 18.1 | **Compliance with legal and contractual requirements** |  |  |  |
| **18.2 Information security reviews**Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures. |
| 18.2.1 | **Independent review of information security.** Control.The organization’s approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) should be reviewed independently at planned intervals or when significant changes occur. |  |  |  |
| 18.2.2 | **Compliance with security policies and standards.** Control.Manager should 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. |  |  |  |
| 18.2.3 | **Technical compliance review.** Control. Information systems should be regularly reviewed for compliance with the organization’s information security policies and standards. |  |  |  |
| **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.1 Consent and choice** |
| A.1.1 | **Obligation to co-operate regarding PII principals’ rights.** Control. The public cloud PII processor should provide the cloud service customer with the means to enable them to fulfil their obligation to facilitiate the exercise of PII principals’ rights to access, correct and/or erase PII pertaining to them |  |  |  |
| **A.2 Purpose legitimacy and specification** |
| A.2.1 | **Public cloud PII processor’s purpose.** Control. PII to be processed under a contract should not be processed for any purposes independent of the instructions of the cloud service customer |  |  |  |
| A.2.2 | **Public cloud PII processor’s commercial use.** Control. PII processed under a contract should not be used by the public cloud PII processor for the purposes of marketing and advertising without express consent. Such consent should not be a condition of receiving the service. |  |  |  |
| **A.3 Collection limitation** |
| **No additional controls are relevant to this privacy principle**. |
| **A.4 Data minimization** |
| A.4.1 | **Secure erasure of temporary files.** Control. Temporary files and documents should be erased or destroyed within a specified, documented period. |  |  |  |
| **A.5 Use, retention and disclosure limitation** |
| A.5.1 | **PII disclosure notification.** Control. The contract between the public cloud PII processor and the cloud service customer should require the public cloud PII processor to notify the cloud service customer, in accordance with any procedure and time periods agreed in the contract, of any legally binding request for disclosure of PII by a law enforcement authority, unless such a disclosure is otherwise prohibited. |  |  |  |
| A.5.2 | **Recording of PII disclosures.** Control.Disclosures of PII to third parties should be recorded, including what PII has been disclosed, to whom and at what time. |  |  |  |
| **A.6 Accuracy and quality** |
| **No additional controls are relevant to this privacy principle.** |
| **A.7 Opennes, transparency and notice** |
| A.7.1 | **Disclosure of sub-contracted PII processing.** Control.The use of sub-contractors by the public cloud PII processor to process PII should be disclosed to the relevant cloud service customers before their use. |  |  |  |
| **A.8 Individual participation and access** |
| **No additional controls are relevant to this privacy principle.** |
| **A.9 Accountability** |
| A.9.1 | **Notification of a data breach involving PII.** Control. The public cloud PII processor should promptly notify the relevant cloud service customer in the eventof any unauthorized access to PII or unauthorized access to processing equipment or facilities resulting in loss, disclosure or alteration of PII. |  |  |  |
| A.9.2 | **Retention period for administrative security policies and guidelines.** Control. Copies of security policies and operating procedures should be retained for a specified, documented period upon replacement (including updating). |  |  |  |
| A.9.3 | **PII return, transfer and disposal.** Control. The public cloud PII processor should have a policy in respect of the return, transfer and/or disposal of PII and should make this policy available to the cloud service customer. |  |  |  |
| **A.10 Information security** |
| A.10.1 | **Confidentiality or non-disclosure agreements.** Control. Individuals under the public cloud PII processor’s with access to PII should be subject to a confidentiality obligation. |  |  |  |
| A.10.2 | **Restriction of the creation of hardcopy material.** Control. The creation of hardcopy material displaying PII should be restricted. |  |  |  |
| A.10.3 | **Control and logging of data restoration.** Control. There should a procedure for, and a log of, data restoration efforts. |  |  |  |
| A.10.4 | **Protecting data on storage media leaving the premises.** Control. PII on media leaving the organization’s premises should be subject to an authorization procedure and should not be accessible to anyone other than authorized personnel (e.g. by encrypting the data concerned). |  |  |  |
| A.10.5 | **Use of unencrypted portable storage media and devices.** Control. Portable physical media and portable devices that do not permit encryption should not be used except where it is unavoidable, and any use of such portable media and devices should be documented. |  |  |  |
| A.10.6 | **Encryption of PII transmitted over public data-transmission networks.** Control. PII that is transmitted over public data-transmission networks should be encrypted prior to transmission. |  |  |  |
| A.10.7 | **Secure disposal of hardcopy materials.** Control. Where hardcopy materials are destroyed, they should be destroyed securely using mechanisms such as cross-cutting, shredding, incinerating, pulping, etc. |  |  |  |
| A.10.8 | **Unique use of user IDs.** Control. If more than one individual has access to stored PII, then they should each have a distinct user ID for identification, authentication and authorization purposes. |  |  |  |
| A.10.9 | **Records of authorized users.** Control. An up-to-date record of the users or profiles of users who have authorized access to the information system should be maintained. |  |  |  |
| A.10.10 | **User ID management.** Control. De-activated or expired user IDs should not be granted to other individuals. |  |  |  |
| A.10.11 | **Contract measures.** Control. Contracts between the cloud service customer and the public cloud PII processor should specify minimum technical and organizational measures to ensure that the contracted security arrangements are in place and that data are not processed for any purpose independent of the instructions of the controller. Such measures should not be subject to unilateral reduction by the public cloud PII processor. |  |  |  |
| A.10.12 | **Sub-contracted PII processing.** Control. Contracts between the public cloud PII processor and any sub-contractors that process PII should specify minimum technical and organizational measures that meet the information security and PII protection obligations of the public cloud PII processor. Such measures should not be subject to unilateral reduction by the sub-contractor. |  |  |  |
| A.10.13 | **Access to data on pre-used data storage space.** Control. The public cloud PII processor should ensure that whenever data storage space is assigned to a cloud service customer, any data previously residing on that storage space is not visible to that cloud service customer. |  |  |  |
| **A.11 Privacy compliance** |
| A.11.1 | **Geographical location of PII.** Control. The public cloud PII processor should specify and document the countries in which PII might possibly be stored. |  |  |  |
| A.11.2 | **Intended destination of PII.** Control. PII transmitted using a data-transmission network should be subject to appropriate controls designed to ensure that data reaches its intended destination. |  |  |  |

# 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 quality 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 quality 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 quality system relative to a requirement; or
* A single observed lapse in following one item of a company’s quality 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 organization system has proven conformity with the requirements of the audit standard and provided adequate structure to support implementation and maintenance of the system*

*i.e:*

* *demonstration of effective implementation and maintenance of the organization system*
* *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 system since last audit took place? (If yes, please list the significant changes) | Yes [ ]  No [ ]  N/A [ ]  |
| Are there any unresolved issues affecting the 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 system is designed to achieve the organization’s policy objectives | Yes [ ]  No [ ]  |
| The 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 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 27018:2019 |
| **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.  |  |
| **Excluded clauses in the audited Management System** (to be put in the certificate) |  |
| **DELIVERY ADDRESS** *(Note\* This shall be 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 PlanISO/IEC 27018:2019** |
| **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 27018:2019 requirements** |
| **Control objectives and controls** |
| **5** | Information security policies |  |  |  |  |
| **6** | Organization of information security |  |  |  |  |
| **7** | Human resource security |  |  |  |  |
| **8** | Asset management |  |  |  |  |
| **9** | Access control |  |  |  |  |
| **10** | Cryptography |  |  |  |  |
| **11** | Physical and environmental security |  |  |  |  |
| **12** | Operations security |  |  |  |  |
| **13** | Communications security |  |  |  |  |
| **14** | System acquisition, development and maintenance |  |  |  |  |
| **15** | Supplier relationships |  |  |  |  |
| **16** | Information security incident management |  |  |  |  |
| **17** | Information security aspects of business continuity management |  |  |  |  |
| **18** | Compliance |  |  |  |  |
| **Use of Logo** |  |  |  |  |
| **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.*