



**MSECB Certification –ISO/IEC 27034:2011**

*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 6

2.4. Previous audit results 7

2.5. Audit planning 7

2.6. Key people interviewed 7

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 27034:2011 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 27034:2011 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 27034:2011.

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 27034:2011.

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 27034:2011.

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 27034:2011.

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 6 to 8 of ISO/IEC 27034:2011);
* The implementation system conforms with all applicable legal and regulatory requirements;
* The implementation 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 27034:2011*.*

## Audit criteria

The audit criteria (the set of requirements) for this are all normative clauses of ISO/IEC 27034:2011:

* Clause 6 – Introduction to application security
* Clause 7 – ISO/OIEC 27034 Overall Processes
* Clause 8 – Concepts
* 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 | |  | |
| **6 Introduction to Application Security** | | | | | | | | |
| 6.3 | | Application security scope | |  |  | |  | |
| 6.3.1 | | General | |  |  | |  | |
| 6.3.2 | | Business context | |  |  | |  | |
| 6.3.3 | | Regulatory context | |  |  | |  | |
| 6.3.4 | | Application life cycle processes | |  |  | |  | |
| 6.3.5 | | Processes involved with the application | |  |  | |  | |
| 6.3.6 | | Technological context | |  |  | |  | |
| 6.3.7 | | Application specifications | |  |  | |  | |
| 6.3.8 | | Application data | |  |  | |  | |
| 6.3.9 | | Organization and user data | |  |  | |  | |
| 6.3.10 | | Roles and permissions | |  |  | |  | |
| 6.4.1 | | Applications ecurity requirements sources | |  |  | |  | |
| 6.4.2 | | Application security requirements engineering | |  |  | |  | |
| 6.4.3.1 | | Organization ISMS | |  |  | |  | |
| 6.4.3.2 | | Application security in the context of an ISMS | |  |  | |  | |
| 6.5.1 | | Application security risk | |  |  | |  | |
| 6.5.2 | | Application vulnerabilities | |  |  | |  | |
| 6.5.3 | | Threats to applications | |  |  | |  | |
| 6.5.4 | | Impact on applications | |  |  | |  | |
| 6.5.5 | | Risk management | |  |  | |  | |
| 6.6 | | Security costs | |  |  | |  | |
| 6.7 | | Target environment | |  |  | |  | |
| 6.8 | | Controls and their objectives | |  |  | |  | |
| **7 ISO/IEC 27034 overall processes** | | | | | | | | |
| 7.1 | | Components, processes and frameworks | |  |  | |  | |
| 7.2 | | ONF Management Process | |  |  | |  | |
| 7.3.1 | | General | |  |  | |  | |
| 7.3.2 | | Specifying the application requirements and environment | |  |  | |  | |
| 7.3.3 | | Assessing application security risks | |  |  | |  | |
| 7.3.4 | Creating and maintaining the Application Normative Framework | | |  | |  |  | |
| 7.3.5 | Provisioning and operating the application | | |  | |  |  | |
| 7.3.6 | Auditing the security of the application | | |  | |  |  | |
| **8 Concepts** | | | | | | | | |
| 8.1.1 | | General | |  |  | |  | |
| 8.1.2 | | Components (8.1.2.1 – 8.1.2.8) | |  |  | |  | |
| 8.1.3 | | Processes related to the Organization Normative Framework (8.1.3.1 – 8.1.3.3) | |  |  | |  | |
| 8.2 | | Application security risk assessment (8.2.1 – 8.2.5) | |  |  | |  | |
| 8.3 | | Application Normative Framework (8.3.1 – 8.3.5) | |  |  | |  | |
| 8.4 | | Provisioning and operating the application (8.4.1 – 8.4.4) | |  |  | |  | |
| 8.5 | | Application Security Audit (8.5.1 – 8.5.2) | |  |  | |  | |
| **Additional requirements** | | | | | | | | |
| Use of logo and trademark | | |  |  | | | |  |
| List of documents included in the audited MS | | |  |  | | | |  |

# 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 27034:2011 | | | | |
| **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 Plan ISO/IEC 27018:2014** | | | | | | |
| **1**: Initial Audit  **2:** Surveillance 1 Audit  **3**: Surveillance 2 Audit  **4**: Recertification Audit | | | **Plan** | | | |
| **1**  **(201X)** | **2**  **(201X)** | **3**  **(201X)** | **4**  **(201X)** |
| **ISO/IEC 27018:2014 requirements** | | | | | | |
| **6 Introduction to application security** | | | | | | |
| **6.3** | Application security scope | |  |  |  |  |
| **6.3.1** | General | |  |  |  |  |
| **6.3.2** | Business context | |  |  |  |  |
| **6.3.3** | Regulatory context | |  |  |  |  |
| **6.3.4** | Application life cycle processes | |  |  |  |  |
| **6.3.5** | Processes involved with the application | |  |  |  |  |
| **6.3.6** | Technological context | |  |  |  |  |
| **6.3.7** | Application specifications | |  |  |  |  |
| **6.3.8** | Application data | |  |  |  |  |
| **6.3.9** | Organization and user data | |  |  |  |  |
| **6.3.10** | Roles and permissions | |  |  |  |  |
| **6.4** | Application security requirements | |  |  |  |  |
| **6.4.1** | Application security requirements sources | |  |  |  |  |
| **6.4.2** | Application security requirements engineering | |  |  |  |  |
| **6.4.3** | ISMS | |  |  |  |  |
| **6.5** | Risk | |  |  |  |  |
| **6.5.1** | Application security risk | |  |  |  |  |
| **6.5.2** | Application vulnerabilities | |  |  |  |  |
| **6.5.3** | Threats to applications | |  |  |  |  |
| **6.5.4** | Impact on applications | |  |  |  |  |
| **6.5.5** | Risk management | |  |  |  |  |
| **6.6** | Security costs | |  |  |  |  |
| **6.7** | Target environment | |  |  |  |  |
| **6.8** | Controls and their objectives | |  |  |  |  |
| **7 ISO/IEC 27034 overall processes** | | | | | | |
| **7.1** | Components, processes and frameworks | |  |  |  |  |
| **7.2** | ONF management process | |  |  |  |  |
| **7.3** | Application security management process | |  |  |  |  |
| **7.3.1** | General | |  |  |  |  |
| **7.3.2** | Specifying the application requirements and environment | |  |  |  |  |
| **7.3.3** | Assessing application security risks | |  |  |  |  |
| **7.3.4** | Creating and maintaining the Application Normative Framework | |  |  |  |  |
| **7.3.5** | Provisioning and operating the application | |  |  |  |  |
| **7.3.6** | Auditing the security of the application | |  |  |  |  |
| **8 Concepts** | | | | | | |
| **8.1** | Organization normative framework | |  |  |  |  |
| **8.1.1** | General | |  |  |  |  |
| **8.1.2** | Components | |  |  |  |  |
| **8.1.3** | Processes related to the Organization Normative Framework | |  |  |  |  |
| **8.2** | Application security risk assessment | |  |  |  |  |
| **8.2.1** | Risk assessment vs risk management | |  |  |  |  |
| **8.2.2** | Application risk analysis | |  |  |  |  |
| **8.2.3** | Risk evaluation | |  |  |  |  |
| **8.2.4** | Application’s Targeted Level of Trust | |  |  |  |  |
| **8.2.5** | Application owner acceptation | |  |  |  |  |
| **8.3** | Application normative framework | |  |  |  |  |
| **8.3.1** | General | |  |  |  |  |
| **8.3.2** | Components | |  |  |  |  |
| **8.3.3** | Processes related to the security of the application | |  |  |  |  |
| **8.3.4** | Application’s life cycle | |  |  |  |  |
| **8.3.5** | Processes | |  |  |  |  |
| **8.4** | Provisioning and operating the application | |  |  |  |  |
| **8.4.1** | General | |  |  |  |  |
| **8.4.2** | Impact of ISO/IEC 27034 on an application project | |  |  |  |  |
| **8.4.3** | Components | |  |  |  |  |
| **8..4** | Processes | |  |  |  |  |
| **8.5** | Application security audit | |  |  |  |  |
| **8.5.1** | General | |  |  |  |  |
| **8.5.2** | Components | |  |  |  |  |
| **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.*