Audit Report
Annex 1: Action List including opportunities for improvement and positive aspects

Order no.: 4153913022 Client no.: 537917-01
Client: Trustea Sustainable Tea Foundation.

Management Service

Comments

An audit cannot cover each and every detail of the management system. Therefore, there may still be nonconformities not addressed by the auditors in the closing meeting or the audit report. Audit results are always evaluated on the basis of the following classification:

Nonconformities (NC):	Failure to fulfil one or more requirements of the management system standard or a situation that raises significant doubt about the ability of the client's management system to achieve its intended outputs. (Classification: **Major** nonconformities). • Corrections (immediate solution) of the audit finding are to be implemented • The causes of the identified nonconformities shall be analyzed • **Corrective actions for the causes of the nonconformities shall be effectively implemented prior to the decision on certificate issue/renewal** • The auditor generally verifies the effectiveness of corrective action in an on-site re-audit unless verification is possible on the basis of submitted new documentation.
Minor nonconformities (MiN):	In individual cases some of the requirements of the management-system standard are not fulfilled completely. However, this does not jeopardize the effectiveness of the management-system element (chapter of the standard). (Classification: **Minor** nonconformities). • Corrections (immediate solution) of the audit finding are to be implemented • The causes of the identified nonconformities shall be analyzed • **The lead auditor is to be informed of the intended corrective actions for the causes of the nonconformities within 14 days prior to the decision on certificate issue/renewal** • The lead auditor evaluates the submitted corrective actions and confirms acceptance thereof. The implementation of the corrective actions will be verified in the next audit.
Opportunities for improvement (I):	Aspects that would lead to management system optimization with respect to a requirement of the standard. (Basic requirement for the identification and recording of **opportunities for improvement is** that the **requirements of the standard regarding the process element** have been fulfilled but that there are still areas for potential improvement of system effectiveness and efficiency. Implementation by the organization is recommended.)
Positive aspects (P):	Positive aspects of the management system meriting special mention

All elements of the standard in each clause of the standard were found to be "in conformity/effective" except for those elements of the standard for which this action list includes nonconformities or minor nonconformities.

Audit Report
Annex 1: Action List including opportunities for improvement and positive aspects

Order no.: 4153913022 Client no.: 537917-01
Client: Trustea Sustainable Tea Foundation.

Management Service

Action List

The following table shall be used for all findings recorded by the audit team during an audit (certification, change, repeat, sample, special or surveillance)

Nonconformities:

Clause no.	Process	Findings		Results of root cause analysis*	Intended correction and corrective action (CA)* (incl. due dates and responsible)	Evaluation of CA *(to be completed by auditor)*		
		Description *(to be completed by auditor)*	**Type** *NC/MiN*	*(to be completed by client in case of NC and MiN)*	*(to be completed by client)*	**Date**	**Effective (E) / Accepted (A)****	**Evidence provided** (only for NC findings)***
		Transfer Audit: **Findings – *NIL***			**Immediate solution for the correction of the finding:** **Corrective Action to eliminate the cause:**			
A.5.7	Threat intelligence	**Finding:** Information relating to information security threats are NOT collected and analysed to produce threat intelligence. **Supporting audit evidence:** The application servers and Database servers are being hosted at Miles Web. However, adequate threat intelligence couldn't be demonstrated by the trustea team.	MiN	As this is a new requirement, the procedure was under development stage, so the sources were not identified. That's why the mechanism was not clear to all related to information security threat intelligence. Caused by it was not found during the assessment.	**Immediate solution for the correction of the finding:** The procedure has been developed completely and sent to the top management for final approval. Date: 20.02.2024 **Corrective Action to eliminate the cause:** Hence, the procedure will be followed to identify and demonstrating threat intelligence. **Responsible Person:** Mr. Debasish Dutta	24-Feb-2024	Accepted	Effective implementation of the Corrective Action will be verified during the next assessment.

Audit Report
Annex 1: Action List including opportunities for improvement and positive aspects

Order no.: 4153913022 Client no.: 537917-01
Client: Trustea Sustainable Tea Foundation.

Management Service

Clause no.	Process	Findings		Results of root cause analysis*	Intended correction and corrective action (CA)* (incl. due dates and responsible)	Evaluation of CA (to be completed by auditor)		
		Description *(to be completed by auditor)*	**Type** *NC/MiN*	*(to be completed by client in case of NC and MiN)*	*(to be completed by client)*	**Date**	**Effective (E) / Accepted (A)****	**Evidence provided** (only for NC findings)***
A.8.32	Change management	**Finding:** Adherence to change management procedures and policy was not evident. **Supporting audit evidence:** Change Management Policy (TSTF-POL-CMP) – v1.1, dated 01.01.2024. Types: Normal Change & Emergency Change Request for Change Impact Analysis Approve/Deny Implement Change Review/Reporting Reviewed the TCMS CR Task Sheet. A number of tasks have been captured within the sheet. Approvals are taken from the Director either via email or verbally. There is no relevency between the policy established and the process followed in the organization.	MiN	As the change management procedure was not been updated as per current practice due to inadequate review, the current practice not covered under the change management policy that leads to the non-relevancy.	**Immediate solution for the correction of the finding:** Policy of change management has been updated as per current practice. Date: 20.02.2024 **Corrective Action to eliminate the cause:** hence all the policies will be review at least once in every year **Responsible Person:** Mr. Debasish Dutta	24-Feb-2024	Accepted	Effective implementation of the Corrective Action will be verified during the next assessment.

Audit Report
Annex 1: Action List including opportunities for improvement and positive aspects

Order no.: 4153913022 Client no.: 537917-01
Client: Trustea Sustainable Tea Foundation.

Management Service

Clause no.	Process	Findings		Results of root cause analysis*	Intended correction and corrective action (CA)* (incl. due dates and responsible)	Evaluation of CA (to be completed by auditor)		
		Description *(to be completed by auditor)*	**Type** *NC/MiN*	*(to be completed by client in case of NC and MiN)*	*(to be completed by client)*	**Date**	**Effective (E) / Accepted (A)****	**Evidence provided** (only for NC findings)***
A.8.21	Security of network services	**Finding:** Security mechanism, i.e., Firewall is not implemented over the network. **Supporting audit evidence:** Reviewed the Network Mapping Diagram – Trustea Sustainable Tea Foundation (tSTF NMD01 – Sep'2022). There is no firewall in the network and/or the auditee couldn't demonstrate the security of the infrastructure hosted in the MilesWeb environment.	MiN	As the network diagram was not reviewed after change in location of the organization, hence the requirement of security tools not updated in the network map which leads to the non-availability of firewall.	**Immediate solution for the correction of the finding:** Web application firewall has been implemented. Date: 20.02.2024 **Corrective Action to eliminate the cause:** The network digram will be reviewed at least once in every year, if in between there any changes occurs. During security audit the resource requirement will also be reviewed. **Responsible Person:** Mr. Debasish Dutta	24-Feb-2024	Accepted	Effective implementation of the Corrective Action will be verified during the next assessment.
A.8.12	Data leakage prevention	**Finding:** Data leakage prevention measures are NOT applied to systems and networks that process, store or transmit sensitive information. **Supporting audit evidence:** Reviewed the Data Leakage Prevention Policy (TSTF-ISMS-DLP) – v1.0, dated 01.01.2024. Policy is in place. However, the implementation of DLP was not evident on the servers, i.e. application and DB servers as well as in emails.	MiN	Due to the implementation of new requirements as per the standard requirements, the same was under progress during the audit hence not fully implemented.	**Immediate solution for the correction of the finding:** The vendor was informed through raising a ticket. Date: 20.02.2024 **Corrective Action to eliminate the cause:** DLP will be implemented through multiple appproach like end point security , role base access control and polciy will be followed & updated accordingly. **Responsible Person:** Mr. Debasish Dutta	24-Feb-2024	Accepted	Effective implementation of the Corrective Action will be verified during the next assessment.

Audit Report
Annex 1: Action List including opportunities for improvement and positive aspects

Order no.: 4153913022 Client no.: 537917-01
Client: Trustea Sustainable Tea Foundation.

Management Service

Clause no.	Process	Findings		Results of root cause analysis*	Intended correction and corrective action (CA)* (incl. due dates and responsible)	Evaluation of CA (to be completed by auditor)		
		Description *(to be completed by auditor)*	**Type** *NC/MiN*	*(to be completed by client in case of NC and MiN)*	*(to be completed by client)*	**Date**	**Effective (E) / Accepted (A)****	**Evidence provided** (only for NC findings)***
A.8.14	Redundancy of information processing facilities	**Finding:** Application and DB servers are NOT redundant sufficient to meet availability requirements. **Supporting audit evidence:** Reviewed the Redundancy Test Report – v1.0, dated 03.01.2024. Only ISP redundancy test of airtel broadband connection and a Jio Mi-Fi device is tested in office environment. However, the redundancy of the application servers, DB server, network devices hosted in the cloud environment are never tested. As confirmed by the auditee, the servers and network devices are not redundant.	MiN	As informed by the service provider, the redundancy of cloud was confirmed. Hence it was not formally documented and tested form our end.	**Immediate solution for the correction of the finding:** We have placed a request to the vendor to obtain the redundancy test report of cloud Date: 20.02.2024 **Corrective Action to eliminate the cause:** Hence, the redundancy test will be verified at yearly basis. Sr Manager IT will be responsible to do the same. **Responsible Person:** Mr. Debasish Dutta	24-Feb-2024	Accepted	Effective implementation of the Corrective Action will be verified during the next assessment.

Note 1: Root cause analysis and corrective action are only mandatory for NC or MiN findings.

* see “Guideline for Corrective Actions Acceptance” at end of document for further assistance

** The intended corrections and implemented corrective actions have to be verified. The Auditor shall evaluate “Effective” (E) in the case of NC and ”Accepted” in the case of corrections for MiN findings, if appropriate.

*** A NC requires a re-audit, during which the corrective actions are evaluated for effectiveness.

Audit Report
Annex 1: Action List including opportunities for improvement and positive aspects

Order no.: 4153913022 Client no.: 537917-01
Client: Trustea Sustainable Tea Foundation.

Management Service

Opportunities for improvement and positive aspects::

Clause no.	Process	Findings		Action for optimization *(optional for client to fill out)*		
		Description *(to be completed by auditor)*	**Type** *I/P*	**Action**	**Responsible**	**Date**
A.8.17	Clock synchronization	**Finding:** Verified Clock Synchronization in all the information processing systems within the organization. All clocks are synchronized with one time reference. However, the CCTV timings may be relooked into.	I			
A.8.13	Information backup	**Finding:** Weekly Backup copies of information, software and systems are maintained and regularly tested. However, the agreed backup policy may be adhered or modified as per the organization's actual practice. Also, the organization may evolve for a better backup solution to ensure the latest data can be restored during any adverse situations.	I			
A.8.11	Data Masking	**Finding:** Though the third-party vendor (e.g. Zoho) is doing the data masking of all the sensitive and employee PII information from their end, the data elements of PII and sensitive information may be identified.	I			
A.8.7	Protection against malware	**Finding:** Kaspersky anti-virus is installed in all the end-point devices. However, the Storage devices of the endpoints may be encrypted.	I			
A.5.26	Response to information security incidents	**Finding:** Response to information security incidents may further be improved considering the severity and criticality of the incident reported. (Ref. Incident # MW8008404, dated 07.01.2024)	I			
A.6.6	Confidentiality or non-disclosure agreements	**Finding:** Instead of relying on the vendor NDA, trustea may also impose its own NDA on the vendors or suppliers. (Ref. OnGrid BGV vendor)	I			

Order no.: 4153913022 Client no.: 537917-01
Client: Trustea Sustainable Tea Foundation.

Management Service

General

If Minor nonconformities identified in the last audit are not closed in an acceptable manner, they must be rated as Nonconformities (re-audit required).

Information on findings management in sampling and multi-site certification

The management representative of the central office must check whether systematic corrective actions to close a root cause can be applied in a preventive manner to other affected sites. This is required for findings from internal and external audits.

In sampling certification, the TMS auditor will select and audit other sites in the next audit cycle and consequently cannot verify on site the effectiveness of the corrective actions from the last audit cycle.

Given this, during the next internal audits carried out at the sites concerned, the management representative of the central office must verify on site the effectiveness/acceptance of the corrective actions taken to address **Nonconformities**, **Minor nonconformities** and **Opportunities for improvement**, if any.

The results must be recorded and submitted to the TMS auditor at the next audit to ensure the auditor can verify the effectiveness of the corrective actions initiated.

Order no.: 4153913022 Client no.: 537917-01
Client: Trustea Sustainable Tea Foundation.

Management Service

Guideline for Corrective Actions Acceptance

Objective: The purpose of this section is to provide a consistent set of criteria for the development, acceptance and implementation of corrective action responses. These guidelines apply to all standards on the basis of the ISO 17021 (i.e. QMS, EMS, AMS, ENMS). They are intended for TÜV-SÜD auditors and audited organizations to help them understand how nonconformities should be addressed.

1. Was correction to eliminate existing finding completed?

Describe corrections for NC and MiN taken under “Intended correction and corrective action”.
e.g.: Completed missing internal audits; Conducted supplier evaluations; Segregated nonconforming material, etc.
Provide evidence that actions were planned, taken and are effective.

2. Have the appropriate root causes been identified? Consider the following:

- what caused the actual nonconformity (for NC and MiN) (occurrence of systematic failure)?
- what allowed the problem to occur without being detected internally?
- which part of the organization’s processes failed to address this issue or is the organization lacking a specific process, method, etc.?
- is the nonconformity also applicable/found in other sites (in case of multi-site and sampling certification)?

The cause shall not be a repeat or a rewording of the nonconformity statement nor of the objective evidence.
e.g.: apply the 5-Why method for root cause analysis

3. Has a corrective action been determined for each identified root cause? Each root cause must have at least one identified corrective action that eliminates / addresses the specific cause(s) and prevents recurrence of the nonconformity.
In the case of multi-sites and sampling certification, verify if the corrective action can be applied in other sites as well.

4. Has appropriate evidence been provided to verify that actions taken have been implemented and are effective?

It is the responsibility of the organization to provide evidence of internal verification of the corrective action(s), or a plan to do so. The Lead Auditor will provide due dates for submitting evidence of implementation. This could vary depending on the circumstances and standards involved.