# PROCEDURE FOR INTERNAL AUDIT

<table>
<thead>
<tr>
<th>Code:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Version:</td>
<td></td>
</tr>
<tr>
<td>Date of version:</td>
<td></td>
</tr>
<tr>
<td>Created by:</td>
<td></td>
</tr>
<tr>
<td>Approved by:</td>
<td></td>
</tr>
<tr>
<td>Confidentiality level:</td>
<td></td>
</tr>
</tbody>
</table>
Change history

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Created by</th>
<th>Description of change</th>
</tr>
</thead>
<tbody>
<tr>
<td>xx/xx/2013</td>
<td>0.1</td>
<td>Branimir Valentic</td>
<td>Basic document outline</td>
</tr>
</tbody>
</table>

Table of contents

1. PURPOSE, SCOPE AND USERS .................................................................................................................. 3
2. REFERENCE DOCUMENTS .......................................................................................................................... 3
3. INTERNAL AUDIT ......................................................................................................................................... 3
   3.1. PURPOSE OF INTERNAL AUDIT ........................................................................................................... 3
   3.2. INTERNAL AUDIT PLANNING ............................................................................................................... 3
   3.3. APPOINTING INTERNAL AUDITORS .................................................................................................... 4
   3.4. CONDUCTING INDIVIDUAL INTERNAL AUDITS .................................................................................. 4
   3.5. FOLLOW-UP ACTIVITIES .................................................................................................................... 4
4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT ............................................................... 5
5. VALIDITY AND DOCUMENT MANAGEMENT ............................................................................................... 5
6. APPENDICES ................................................................................................................................................ 5
1. Purpose, scope and users

The purpose of this procedure is to describe all audit-related activities – writing the audit program, selecting an auditor, conducting individual audits and reporting.

This procedure is applied to all activities performed within the Service Management System (SMS).

Users of this document are [members of top management] of [organization name], as well as internal auditors.

2. Reference documents

- ISO/IEC 20000-1:2011 standard, clauses 4.5.4.1., 4.5.4.2.
- Service Management System Plan
- Communication Procedure
- Management Review Minutes

3. Internal audit

3.1. Purpose of internal audit

The purpose of an internal audit is to determine whether procedures, controls, processes, arrangements and other activities within the SMS are in line with the ISO 20000 standard, applicable regulations, and the organization’s internal documentation, whether they are effectively implemented and maintained and whether they meet service requirements and SMS requirements identified by the service provider.

3.2. Internal audit planning

[role description] approves an annual program for internal audits, written as outlined in the form in Appendix “Annual Internal Audit Program.”

One or more internal audits should be conducted over the course of one year, ensuring cumulative coverage of the entire SMS scope. Internal audits are planned based on the nature and importance of the processes and areas to be audited, as well as results of previous audits, they are usually conducted before a management review.

The Annual Internal Audit Program has to contain the following information about each individual internal audit:

- period of the audit (specifying dates, or month in which the audit is planned)
- scope of the audit (departments, processes, clauses of the standard, etc.)
- objectives of the audit
- audit criteria (standards, legislation and regulations, internal documentation, corporate standards, and/or contractual obligations)
3.3. **Appointing internal auditors**

[role description] shall appoint internal auditors.

An internal auditor may be someone from the organization or a person outside the organization. Criteria for appointing internal auditors are:

- knowledge of ISO/IEC 27001 standard
- familiarity with management system auditing techniques
- knowledge of how information and communication technologies function to the extent that he/she is familiar with the purpose of individual systems as well as the impacts on processes and services

Internal auditors must be selected in such a way as to ensure objectivity and impartiality, i.e. to avoid conflict of interest, because auditors are not allowed to audit their own work.

3.4. **Conducting individual internal audits**

Persons responsible for individual internal audits are identified in the Annual Internal Audit Program. If an audit is conducted by a team consisting of several auditors, the person responsible for the audit is the one identified as Audit Team Leader.

The following must be taken into consideration during an internal audit:

- criteria laid down in the Annual Internal Audit Program
- results of previous internal or external audits
- results of risk assessment, control implementation, business impact analysis, etc.

The following must be documented as internal audit results:

- Internal Audit Report – it must be sent to [job title]
- Corrective and Preventive Action Form

3.5. **Follow-up activities**

A nonconformity is any failure to meet the requirements of the standards, internal documentation, regulations, contractual or other obligations. Nonconformities and results of internal audits shall be communicated (see Communication Procedure), prioritized (priority grade 1 is the highest priority) and responsibility allocated for actions. [role description] uses results, nonconformities and defined actions of the internal audit as input for management review (see Management Review Procedure).

The management responsible for the area being audited shall ensure that any corrections and
The person responsible for the audit must verify that actions have been implemented appropriately and within specified deadlines and report the results to [role description].

4. Managing records kept on the basis of this document

<table>
<thead>
<tr>
<th>Record name</th>
<th>Storage location</th>
<th>Person responsible for storage</th>
<th>Controls for record protection</th>
<th>Retention time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Annual Internal Audit Program (in electronic form)</td>
<td>[job title]'s computer</td>
<td>[role description]</td>
<td>Only [job title] and the internal auditor have the right to make entries into and changes to the Annual Internal Audit program.</td>
<td>Programs are stored for a period of 3 years.</td>
</tr>
<tr>
<td>Internal Audit Report (in electronic form)</td>
<td>Internal auditor’s and [job title]'s computers</td>
<td>Internal auditor</td>
<td>Reports are stored in read-only versions.</td>
<td>Reports are stored for a period of 3 years.</td>
</tr>
<tr>
<td>Corrective and Preventive Action Form</td>
<td>[name of filing folder, in which cabinet] [intranet folder name]</td>
<td>[role description]</td>
<td>After all data has been recorded, any new additions must be prevented.</td>
<td>[enter period]</td>
</tr>
</tbody>
</table>

Only [role description] can grant other employees the right to access the Annual Internal Audit Program and the Internal Audit Report.

5. Validity and document management

This document is valid as of [date].

The owner of this document is [job title], who must check and, if necessary, update the document at least once a year.

Comment [BV6]: This is only a recommendation; adjust frequency as appropriate.

6. Appendices

Appendix 1: Annual Internal Audit Program
Appendix 2: Internal Audit Report
[organization name]  [confidentiality level]

[job title]
[name]

[signature]

Comment [BV7]: Only necessary if the Procedure for Document and Record Control prescribes that paper documents must be signed.