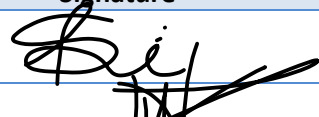


Internal Audit Programme

Version 1.0, 1.12.2020

Document Approval

The undersigned acknowledge they have reviewed the *Internal Audit Process*. The undersigned hereby give full approval to the content of the document.

Title	Name	Signature
Information Security Manager	All Si	
General Manager	High Vision	

This document is reviewed and approved by management through the company's Integrated Management System Steering Committee who is responsible to officially authorize its publication. Any change requests to this document can only be submitted to the Quality & Internal Audit department for further processing.

Document Information

Document Owner:	Information Security Manager	Issue Date:	01 December 2020
Email:	SiAll@AlphaBetaPrinting.com	Last Review Date:	
		Next Review Date:	

Document History

Version	Author	Date	Changes
0.1	Quality Manager	01/09/2020	Initial draft issued for review & comments
0.2	Quality Manager	01/10/2020	Second draft issued for review & comments
1.0	Quality Manager	30/10/2012	Issued for Implementation

Table of Contents

1	Introduction	3
1.1	Scope.....	3
1.2	Owner.....	3
1.3	Information Security and Health & Safety Aspects.....	3
1.4	Definitions and Abbreviations.....	Ошибка! Закладка не определена.
2.	Policy Statements.....	4
2	Process.....	5
3	Records	12
4	Key Performance Indicators	12

1 Introduction

This document describes roles & responsibilities and the way of conducting internal audits against the requirements of ISO 27001:2013.

The purpose of conducting internal audits is to examine and evaluate organization's processes effectiveness and efficiency, to identify areas for business improvement and to ensure compliance with regulations, standards and company's working policies and practices, including compliance with the requirements of ISO 27001:2013.

This process applies to all audits carried out within the organization, external companies, current and potential suppliers.

1.1 Scope

This document is applicable to all departments of the organization.

1.2 Owner

The Quality Manager is the owner of this document. Any changes to the document can be made only by the Quality Manager following the Control of Documents and Records Process.

1.3 Information Security and Health & Safety Aspects

Information Security: exercise care for the protection of confidentiality & integrity of the data collected and managed during the execution of this process.

Health & Safety: Observe all H&S relevant rules & guidelines when executing audit in areas which pose (or may pose) an H&S hazard. Use of personal protective equipment (PPE) may be necessary (e.g. use of safety shoes when auditing the workshops).

2. Policy Statements

The Management System has been developed to meet the requirements of ISO 27001:2013.

Information Security procedures are defined in the Manual, together with the organization's Philosophy, Vision and Mission.

As the size and requirements of the organization are constantly developing, it is essential to audit on a planned basis the organization's implemented management system to ensure its continuing suitability and effectiveness in satisfying the requirements and needs of the organization.

2 Process

S/N	Role	Responsibility	Comment
1	Internal Auditor	<p>Plan the Audits based on the annual Audit plan and/ or any other input.</p> <p>The Internal Auditor prepares the Annual Audit Plan using the respective form covering the type of audits as well as the frequency and methods of audit. The annual audit plan takes into consideration the status and importance of the processes and areas to be audited, the Risk Assessment report, as well as the results of previous audits.</p> <p>All departments and processes of the organization within the scope have to be audited once a year. As mentioned above, taking into account the risk assessment, the novelty of processes, the non conformities, the changes implemented etc, the individual audits could be implemented at a specified frequency.</p>	<p>Any type of Audit may be conducted as a result of:</p> <ul style="list-style-type: none"> ▪ The annual Audit plan ▪ External bodies Audits findings ▪ Actions agreed during Management meetings and/or any other meeting ▪ Results from surveys, suppliers questionnaires and any other KPIs ▪ Requests from organization's Departments ▪ Suppliers evaluation results and OFIs ▪ Any internal request for auditing current or potential supplier
2	Internal Auditor	<p>The Internal Auditor submits the plan to the Information Security Manager for approval.</p> <p>The Information Security Manager submits the Annual Audit Plan to the Steering Committee for final approval.</p> <p>Upon approval of the annual audit plan, the Internal Auditor communicates the plan to the interested parties (auditees).</p>	
3	Internal Auditor	<p>Notify the management of the areas to be audited regarding:</p> <ol style="list-style-type: none"> a) the objectives and the scope of the Audit b) the Audit time and c) The proposed schedule of the onsite activities and the time needed from specific teams. <p>Common consensus between the management of the audited area and the Internal Auditor must be reached in order to define the relevant representatives available for the Audit.</p> <p>In addition, further actions should be taken in order to communicate the impendent Audit to interested departments in company and to collect any other related information.</p>	<p>The discussion of the forthcoming Audit should be done with the most appropriate related management.</p>

S/N	Role	Responsibility	Comment
4	Internal Auditor	<p>Create the Audit team by selecting members with relevant experience to the area/ system to be assessed.</p> <p>The minimum competencies (education, training, experience, soft skills) for the role of the Internal Auditor for the Information Security Management System are defined in the Internal Auditor Job Description.</p> <p>Moreover, for all team members, the selection fulfils the following independence requirements:</p> <ul style="list-style-type: none"> - No internal auditor shall audit their own work. - No internal auditor shall audit their direct supervisor. - No internal auditor shall audit member of their immediate family. 	Inform other internal auditors.
5	Internal Auditor	<p>Review qualitative results before assessing any area/ process/ supplier.</p> <p>Qualitative results from quality metrics may be results from: Customers' feedback, Measurements on suppliers performance, Information security incidents, related metrics, logs, QC statistics, Projects time plans, tests results, OFIs from previous audits etc.</p>	<p>Auditors' team should review all data and/ or KPIs related to the scope of Audit:</p> <ul style="list-style-type: none"> ▪ Review of relevant existing documentation (process docs, procedures, previous Audits findings, self-Audit etc.) ▪ Qualitative results from quality metrics: Customers' feedback, Measurements on suppliers' performance, Information security incidents, related metrics, logs, QC statistics, Projects time plans, tests results, OFIs etc. ▪ Processes KPIs results ▪ Security related incidents that have occurred since last audit ▪ Security related personnel issues that have arisen since last audit ▪ Results of any risk assessment undertaken since the last audit and discussion of the proposed controls ▪ Designation of people or processes to manage risks (e.g. insurance). ▪ Proposed changes to the Security Policy ▪ Implementation progress reports of previously decided actions

S/N	Role	Responsibility	Comment
6	Internal Auditor	In case of process Audits, if the process to be assessed is not yet mapped and approved via corporate documentation workflow, a draft flowchart may be developed based on relevant documentation and/ or any other available information. Based on this draft a specific check list and interview list may be prepared.	For initial process Audits, it is recommended to the auditors' team, to prepare a desktop process flow chart, which may help them to have a holistic and integrated view of the process.
7	Internal Auditor	For each specific individual audit, Identify the areas to assess and prepare an Audit checklist, if needed.	The Internal Auditor(s) collects and studies previous audit findings and possible outstanding issues. Additionally, the team prepares any additional documents that will be needed for the realization of the audit (e.g. QMS & ISMS Audit Checklist).
8	Internal Auditor	Review of relevant existing documentation (process docs, procedures, previous Audits findings, self-Audit etc.)	
9	Internal Auditor	Create the Audit agenda including: <ul style="list-style-type: none"> objectives and the scope of the Audit the Audit time, the purpose of the Audit the list of participants and The schedule of the interviews, if needed. Audit agenda is sent at least 5 working days in advance to all parties involved in order to final confirm the Audit.	
10	Internal Auditor	Audit starts with an opening meeting with the management of the Function/ Department to be assessed in order to clearly explain the Audit purpose and process.	During this meeting the following issues should be addressed: <ol style="list-style-type: none"> 1) The objective of the Audit 2) The scope of the Audit 3) Expected Audit deliverables 4) The process to be followed during the audit 5) Previous Audit findings

S/N	Role	Responsibility	Comment
11	Internal Auditor	<p>Conduct the Audit on the predefined time frame. The Audit process includes:</p> <ul style="list-style-type: none"> ▪ Interviews with relevant employees ▪ Walkthrough of the area assessed. ▪ Collection and review of relevant documentation and/ or evidence. ▪ Observation of the systems and processes. ▪ The Internal ISMS Auditor) performs the audit and completes the pre-defined audit report. During the course of the audit the Internal Auditor tries to identify adequate evidence to ascertain that: ▪ The documented procedures are being followed (i.e. within the scope of the ISMS) and are meeting their desired objectives ▪ The agreed actions from previous audits and reviews have been implemented ▪ The ISMS are compliant with the relevant standard ▪ The security policy are still an accurate reflection of the business requirements ▪ That processes are measured for their effectiveness and efficiency. ▪ KPIs are achieved and if not relevant corrective actions are taking place. ▪ An appropriate risk assessment methodology is being used ▪ Technical controls are in place, are correctly configured and working as intended and effectively ▪ The residual risks have been assessed correctly and are still acceptable to the management of the company 	<p>Audits are conducted by a set of interviews by the auditors' team. During the interview the auditors should:</p> <ul style="list-style-type: none"> ▪ Collect evidence on everything discussed. ▪ Decide on strengths and areas that require improvement ▪ In case of process Audits, collect all necessary information and data in order to verify or update the existing process flowchart or develop a new one.

S/N	Role	Responsibility	Comment
12	Internal Auditor	<p>When Audit is completed, a closing meeting with the involved management of the audited area is conducted. During the closing meeting the following issues should be addressed and agreed:</p> <ol style="list-style-type: none">1) The results of the Audit2) The Audit findings and the areas for improvement are agreed with the management of the audited area.3) An action plan with the proposed corrective or preventive actions agreed with the local management. <p>For Audits that are for more than 1 day at the end of each day a wrap up meeting is required the management team in order to inform and agree on the findings.</p>	All Audit team should be present (if practicable) at the closing meeting.

S/N	Role	Responsibility	Comment
13	Internal Auditor	<p>Prepare an Audit report on agreed time.</p> <p>The Audit report includes the Audit findings and the corrective actions and/or opportunities for improvement (OFIs) agreed during the closing meeting and any other useful information that the Audit team would like to report.</p>	<p>Any audit finding must be labeled according to its priority level:</p> <ul style="list-style-type: none"> Audit findings that are characterized as Priority 1 are major non-conformities and must be planned for resolution in a period of 2 weeks and a follow up audit must be scheduled at the end of that period. Note that if considered critical, the resolution of certain audit findings may be required immediately. Audit findings that are characterized as Priority 2 are minor non-conformities and must be planned for resolution in a period of 3 months and a follow up audit must be scheduled at the end of that period Audit findings that are characterized as Observation must be planned for resolution in a period of 6 months and their progress must be monitored in all of the following periodic audits until resolution <p>Audit findings and their corresponding non-conformance must be communicated to the Information Security Manager at the end of each audit</p>
14	Internal Auditor	In case of process audits, all required documentation should be defined and developed, including the relevant process flowchart.	
15	Internal Auditor	<p>Distribute the Audit Report to the management of the assessed area and to other involved recipients.</p> <p>The report should be sent within 5 working days after the closing meeting.</p> <p>On exceptional cases and in case that during an internal audit a closing meeting cannot be held, a draft report including recommendations and proposed actions is sent for official comments and taking management response.</p>	If it is applicable, an updated process flowchart may be attached in the report.

S/N	Role	Responsibility	Comment
16	Internal Auditor	Record the agreed OFIs and the proposed corrective actions. The issues finding, the proposed actions, the responsible personnel, the target date, as well the status of the issue is kept in an specific action plans per department and/ or per process	According to the audit findings and the non-conformance level, an action plan (identified in the corrective/preventive actions log) must be developed.
17	Internal Auditor	Follow-up on raised OFIs/ outstanding (pending) findings. Based on the action plan the Information Security Manager coordinate activities for the implementation of the corrective actions and updates the corrective/preventive actions Log accordingly. The Information Security Manager should evaluate the effectiveness of the implemented actions (documented in the Corrective/Preventive Actions Log) and if he deems necessary he may request for a follow up audit. The scope of follow-up audits is limited to the non-conformance and the same audit mechanisms that produced the finding are used.	Project or Team Review Meetings and / or any other meeting may be scheduled on a yearly basis. During these meetings (among others) follow up of OFIs may be done. Also ad hoc follow up of the progress status could be performed if deemed necessary.
18	Steering committee	Management review	The results of internal audits must be reviewed during the annual management review

3 Records

S/N	Record Name	Record Type	Retention Time	Responsible	Location	Classification
1.	Audit records including agenda, evidences, Audit report, open issues, notes, process Audit questionnaire etc.	Electronic or physical	3 years	Internal Auditor	Relevant network areas	Confidential

4 Key Performance Indicators

KPI Name	Periodicity	Responsible	Location	Target
Management System audits performed as planned	Annually	Quality Manager	Electronic file	100% as planned
% of Non-Conformities corrected within agreed time	Quarterly	Quality Manager	Electronic file	80% on time agreed