callwell

complete lead control

Information Security Management System

1. Introduction

This document is the Information Security Management System 'ISMS' of Callwell Limited and for the purpose of this ISMS will be referred to as 'Callwell'.

The ISMS is the property of Callwell and is a controlled document.

The purpose of the ISMS is to provide an overview of Callwell, the activities it carries out and the ISMS standards of operation it conforms to.

It is not designed to act as a procedures manual, although it does carry information about where procedures information is located and the detailed information on documentation requirements for the procedures required by the respective standards.

This ISMS is designed to meet the requirements of ISO 27001 and any standard which adopts the Annex SL structure.

1.1 The Issue Status

The issue status is indicated by the version number in the footer of this document. It identifies the issue status of this ISMS.

The ISMS can be fully revised and re-issued at the discretion of the Management Team.

Please note that this ISMS is only valid on day of printing.

1.2 ISMS Policy

It is the policy of Callwell to maintain an information management system designed to meet the requirements of ISO 27001in pursuit of its primary objectives, the purpose and the context of the organisation.

It is the policy of Callwell to:

- make the details of our policy known to all other interested parties including external where appropriate and determine the need for communication and by what methods relevant to the business management system.
- comply with all legal requirements, codes of practice and all other requirements applicable to our activities; therefore, as a company, we are committed to satisfy applicable requirements related to information security and the continual improvement of the ISMS.
- provide all the resources of equipment, trained and competent staff and any other requirements to enable these objectives to be met;
- ensure that all employees are made aware of their individual obligations in respect of this information security policy;
- maintain a management system that will achieve these objectives and seek continual improvement in the effectiveness and performance of our management system based on "risk".

This information security policy provides a framework for setting, monitoring, reviewing and achieving our objectives, programmes and targets.

To ensure the company maintains its awareness for continuous improvement, the business management system is regularly reviewed by “Top Management” to ensure it remains appropriate and suitable to our business. The Business Management System is subject to both internal and external annual audits.

Scope of the Policy

The scope of this policy relates to use of the database and computer systems operated by the company in pursuit of the company’s business of providing software services. It also relates where appropriate to external risk sources including functions which are outsourced.

2. Overview of the Organisation

Callwell Limited, established in 2013, to provide software services enabling customers to be in immediate contact with their internet leads. The company primarily deals with customers from the Estate Agency Sector although the product may be sold to customers of other sectors in the future.

2.1 Scope of Registration

Provision of Information Technology and Software Services specialising in the UK estate agency sector.

3. Objectives

We aim to provide a professional and ethical service to our clients. In order to demonstrate our intentions, Our Management Team will analyse customer feedback data, internal performance data, financial performance data and business performance data to ensure that our Objectives are being met.

INFORMATION SECURITY

Our objectives are set out in our business plan and are then disseminated to each department/project for incorporation into their management roles.

Each department is responsible for delivering its objectives and this is monitored via individual, appraisals & team meetings.

Callwell's Objectives are as follows:

- Objective 1: Existing services – We will continue to deliver our services within a secure environment.
- Objective 2: Development – We will conduct risk assessments to ensure that risk to information in the care of Callwell is minimised or eliminated.
- Objective 3: Innovation – We will continue to innovate and enhance the service we provide to make our ISMS more effective.
- Objective 4: Participation – We will continue to liaise with all interested parties to improve our ISMS.
- Objective 5: Skills – We will continue to increase the level of professional skills of our staff and key sub-contractors in terms of Information Security Management.
- Objective 6: Profit – We will work to ensure our ISMS helps us to be more efficient and profitable.

Whilst the above company objectives are "high-level", we have further analysed and categorised these into our Risk & Opportunities Matrix. In some cases, this may allow for specific objectives being set across different functions. This shows how we measure and set targets in meeting the "high level" objectives.

4. Context of the organisation

4.1 Understanding the organisation and its context

The context of the organisation is demonstrated within this Business Management System and all associated processes connected with the services / products offered.
The legal legislation / regulatory compliance to the service / products offered are listed in the CROO document.
The Innovation Director reviews changes to any relevant legislation and the company retains the services of solicitors and/or specific experts (for example Patent Lawyers) to advise the company in respect of any legislation relevant to the company.

4.2 Understanding the needs and expectation of interested parties

Interested Parties	Information Requirements
Directors	Ensure that the business continues to function in a profitable manner without hindrance and bureaucracy. To ensure business information is kept confidential, available and reliable.
Employees	To protect client confidentiality To ensure employment processes are followed. To ensure Information Security Policies and Procedures are followed. To take responsibility for their own training
Clients	To ensure all related information is kept confidential Meet the requirements of the Data Protection Act 1998 To ensure integrity of the systems are maintained as appropriate To ensure adherence to relevant SLAs
Contractors	To ensure all related information is kept confidential Meet the requirements of the Data Protection Act 1998 To ensure integrity of the systems are maintained as appropriate To ensure adherence to relevant SLAs/NDAs

Suppliers	To ensure all related information is kept confidential Meet the requirements of the Data Protection Act 1998 To ensure integrity of the systems are maintained as appropriate To ensure adherence to relevant SLAs
Accountants	To ensure all related information is kept confidential Meet the requirements of the Data Protection Act 1998
Company Solicitors / Lawyers	To ensure all related information is kept confidential Meet the requirements of the Data Protection Act 1998
Governing Bodies	Provision of up to date information Provision of relevant information Provision of guidance where needed To ensure all related information is kept confidential Meet the requirements of the Data Protection Act 1998

4.3 Determining the scope of the Information Security System

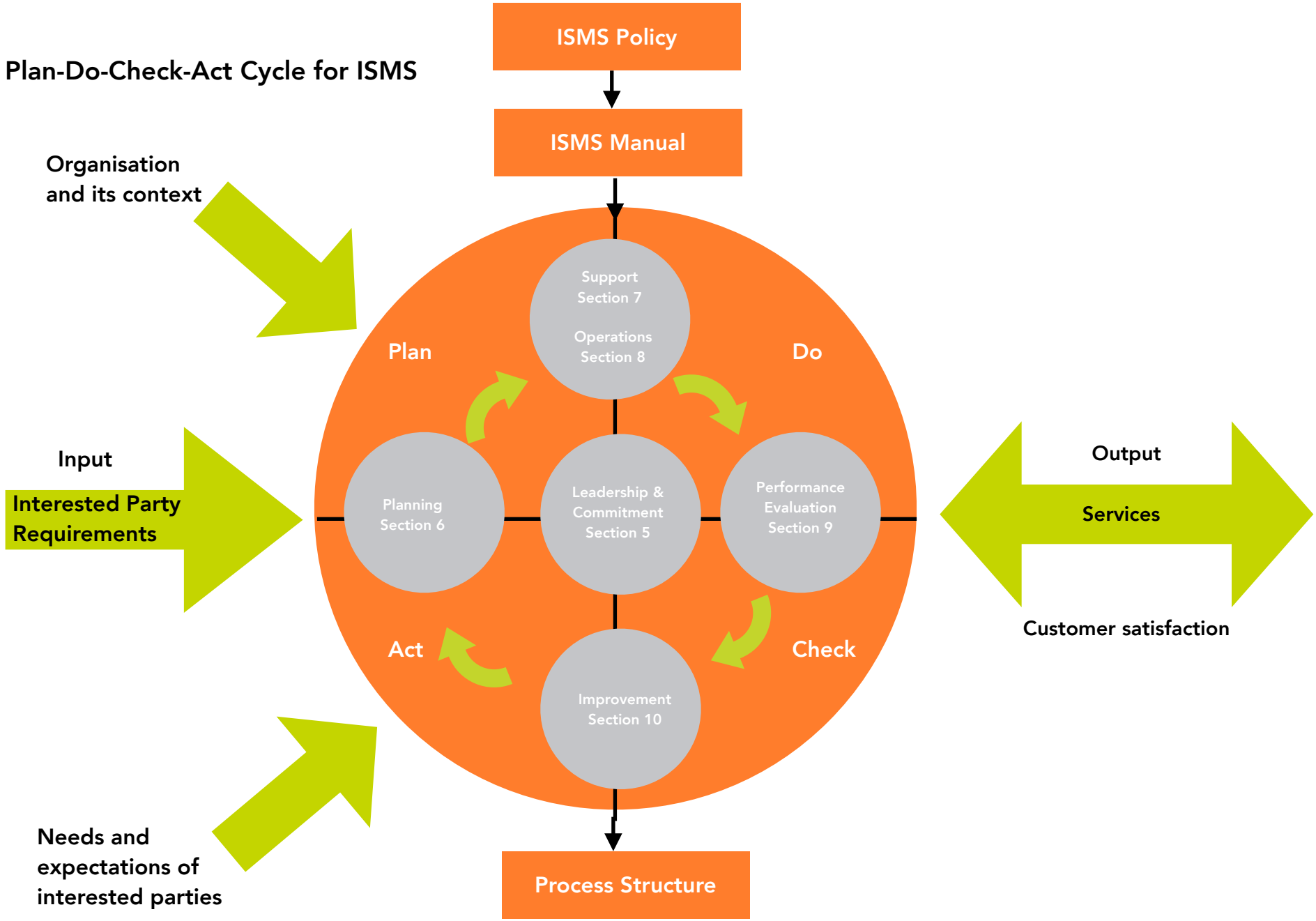
Information Security Callwell:

The scope of the system covers all the core and supporting activities of the company. The activities and arrangements of all personnel including any sub-contractors also fall within the scope of the system.

4.4 Information Security Management system

The organisation has established, implemented, maintained and will continually improve an information security management system in accordance with ISO27001. This ISMS provides information as to how we meet these requirements, with reference to key processes and policies, as appropriate.

4.4 Plan-Do-Check-Act Cycle for ISMS



5 Leadership

5.1 Leadership & Commitment

Callwell's Top Management Team are committed to the development and implementation of an ISMS Policy and the Information Security Management System which are both compatible with the strategic direction and the context of the organisation, the whole system is frequently reviewed to ensure conformance to ISO 27001. Responsibility has been assigned to ensure that the business Management System conforms to the requirements of the respective standard and the provision to report on performance to the top management team has been defined.

The designated Senior Management Representative(s) will ensure that Callwell staff are aware of the importance of meeting customer as well as statutory and regulatory requirements, and overall, to contribute to achieving Callwell's Information Security Policy and Objectives which are aligned with the organisations strategic direction

The Senior Management Team is responsible for implementing this system and ensuring the system is understood and complied with at all levels of the organisation.

In summary, the Senior Management Team will ensure that:

- The company has a designated Senior Management Representative who is responsible for the maintenance and review of the Management System.
- The ongoing activities of Callwell are reviewed regularly and that any required corrective action is adequately implemented and reviewed to establish an effective preventative process.
- Measurement of our performance against our declared Information Security Objectives is undertaken.
- Resources needed for the system are available and employees have the necessary training, skills and equipment to effectively carry out their work.
- Internal audits are conducted regularly to review progress and assist in the improvement of processes and procedures.
- Objectives are reviewed and, if necessary amended, at regular Management Review meetings and the performance communicated to all staff.
- The information security policy and objectives are established in line with the strategic direction of the organisation and that intended outcome(s) are achieved.
- The management system is integrated into the organisations business processes.
- Communication covering the importance of the effective management system and conformance to the management system requirements is in place.
- Continual improvement is promoted.

- The contribution of persons involved in the effectiveness of the management system is achieved by engaging, directing and supporting persons and other management roles within their area of responsibility.

5.2 Policy

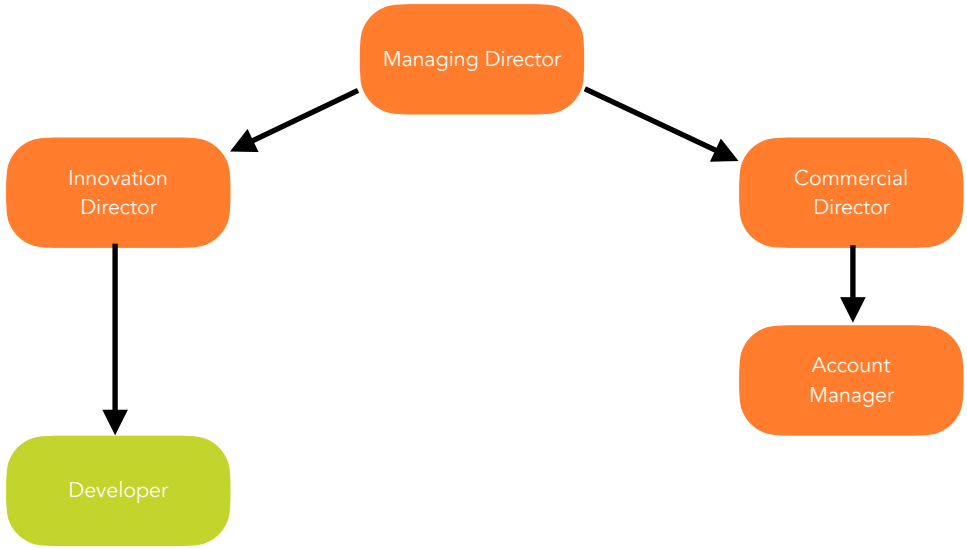
The ISMS Policy of Callwell is located within section 1.2 of this ISMS.

5.3 Organisational roles, responsibilities and authorities

Callwell has an organisation chart in place, employee contracts together with job descriptions to ensure that the appropriate personnel are in place to cover the whole context of the organisation and strategy of the business.

Our Innovation Director is responsible for randomly sampling records to ensure that all required data has been captured, and that data is accurate and complete.

5.3 Organisational Chart



Sub Contractors

Employed Staff / Directors

6 Planning

6.1 Actions to address risks and opportunities

We have identified the risks and opportunities that are relevant to our Business Management system from an operational perspective. This also links to section 4.1 and 4.2 of this ISMS and also provides information on low-level objectives. This 'Context, Risk, Opportunities and Objectives' (CROO) document is separate to this ISMS. Within each of the areas the risks are identified together with a rating as to the importance of the risk. The associated consequence & mitigation of the risk is also noted together with any new opportunities that we have identified. Where applicable, we have identified measurable objectives and these can be found within a separate tab in the 'CROO' document.

The controls identified in this document feed into our risk treatment plan (Statement of Applicability), which has been designed and implemented using the main headings within the standard (Annex A, Table A.1 – control objectives and controls) as a guide to establish that all controls required have been considered and that there are no omissions. The document identifies controls to mitigate risks following the process of identification, analysis and evaluation. The SOA document is separate to this ISMS.

6.1.2 Information Security Risk Assessment

In accordance with our 'CROO' matrix referenced in 6.1, above, we have assessed any typical / likely Information Security threats based on their potential effects on Confidentiality, Integrity and Availability (CIA) attributes.

Following this analysis, appropriate controls have been identified, which feed into our Statement of Applicability, as described in section 6.1.3, below.

6.1.3 Information Security Risk Treatment

The approach to our risk treatment plan has been designed and implemented using the main headings within the standard (Annex A, Table A.1 – Control objectives and controls) as a guide to establish that all controls required have been considered and that there are no omissions.

The document identifies controls to mitigate risks following the process of identification, analysis and evaluation described in section 7 and is directly linked to the aspects of the organisation.

The SOA document is separate to this ISMS and conforms to the requirements as defined within clause 8.3 of the ISO 27001standard.

Please see below documents as demonstration of compliance of this clause:-

- CROO Document (Context, Risk, Opportunities & Objectives)
- Statement of Applicability

6.2 Information Security Objectives and planning to achieve them

The ISMS Objectives and methods of achieving the objectives is located within section 3 of this ISMS.

7 Support

7.1 Resources

Callwell determines and provides the resources needed for the establishment, implementation, maintenance and continual improvement of the management system.

We ensure that the below elements are taken into account when completing an evaluation:

- The capabilities of, and constraints on, existing internal resources;
- What needs to be obtained from external providers

7.2 Competence

All employees have the training and skills needed to meet their job requirements. All employees are monitored on an ongoing basis to identify any training and development needs. Competences and training needs are identified / satisfied by using:

- Job descriptions which set out the competences required
- Contracts of employment which set out contractual and legal requirements
- Induction checklists to ensure / check understanding
- Development plans to set objectives
- On the job reviews to ensure / check levels of competence
- Tests of understanding
- A training / competency matrix

7.3 Awareness

We ensure that all employees are aware of all policies and their contribution to the effectiveness of the Management System through:

- Notice Boards
- Employee Intranet
- Awareness Training
- Induction
- CPD

7.4 Communication

For internal staff the peoplehr software is a source of information and is updated regularly to ensure that all information is correct. This is accessible by all staff.
Any communication which is sent external to the intranet is designated through the appropriate line manager.

For external persons, the company internet is a source of information and is updated regularly to ensure that information to up-to-date. Client mail shots are sent out regularly to provide additional services etc

7.5 Documented Information

7.5.1 General

Callwell demonstrates documented compliance to ISO 27001(or any other standard in line with Annex SL Structure) through this ISMS (which includes processes & procedures) on an electronic system which is available on the company intranet to all employees . All information is read only and only accessible via the document owner for amendment.

7.5.2 Creating and updating

The creation of documentation to support the Business Management System is primarily the responsibility of the designated "Top Management Representative".

Identification will be sought by a document number, date and author. To aid the approval and suitability of documents, the Innovation Director of Callwell authorises the release and delegates any training required to the "Top Management Team".

7.5.3 Control of documented information

All documentation is controlled by version and date and is listed on a "Master Document List".

Callwell has two backup processes in place utilising 'AmazonS3' and server replication offered by 'Digital Ocean'. These backups avoid the loss of confidentiality, improper use or loss of integrity. Key office computers are backed up daily to an encrypted hard disk and where possible files are immediately backed up using 'Dropbox' .

Control of documents can be seen on the Master Document List and encompasses the following elements:-

- Distribution, Access, Retrieval and use
- Storage and preservation, including preservation of legibility
- Control of changes (e.g. version control)
- Retention and disposition

Documents can be retrieved by authorised personnel from the storage locations specified and / or from folders held on Dropbox. Customer records are identified by customer name.

On or after the retention period stated, the relevant records will be reviewed by Top Management and will either remain in-situ, be archived or destroyed.

If records are to be destroyed, they will be disposed of in a controlled manner; sensitive hard copies will be shredded and soft copies will be deleted from the system. If records are to be archived, they will be identified and stored appropriately

8 Operation

8.1 Operational planning and control

Callwell has determined the requirements and controls implemented for all processes needed to meet Information Security requirements and has implemented the actions described in section 6.1 of this ISMS. We will also implement plans to achieve ISMS objectives, as highlighted in sections 3 and 6.2 of this ISMS. We retain documented information to the extent necessary to have confidence that the processes have been carried out as planned. We shall control any planned changes and will review the consequences of unintended changes, taking action to mitigate any adverse effects.

8.2 Information Security risk assessment

In line with the criteria established in section 6.1.2 of this ISMS, we perform ISMS risk assessments at planned intervals or when significant changes are proposed or occur. Documented information of the results of risk assessments is retained.

8.3 Information Security risk treatment

The risk treatment is incorporated within Risks & Opportunities – See Clause 6.1

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

Monitoring is based on risk and is linked to the risk & opportunities register together with the risk assessments which are carried out. This is also monitored through internal audits (section 9.2) and management review (section 9.3) to ensure the effectiveness of the management system.

9.2 Internal Audit

An internal audit schedule is prepared on an annual basis year and covers the requirements of the ISO27001 standard. Internal audits are carried out through "risk or clause based" auditing.

Appropriate personnel are allocated to complete the internal audits and must record appropriate evidence for completeness. All audits completed must be authorised by Top Management as complete once any non-conforming areas have been dealt with (without any undue delay). Internal audit documentation must be kept and filed appropriately.

9.3 Management review

Management reviews take place as a minimum on an annual basis. The attendees present are "Top Management" and any other appropriate persons of the business.

All inputs / outputs are full documented and minuted in line with the requirements of the specific ISO standard in which Callwell wish to be certified. Any actions arising from the meeting must be completed without any undue delay and appropriate evidence filed with the Management review documentation.

10 Improvement

10.1 Nonconformity and corrective action

Should a nonconformity occur, including those arising from complaints, internal audits & external 3rd part assessment Callwell designate the appropriate "Top Management" representative to ensure that corrective action including root cause analysis is completed and implemented to avoid any further occurrences. This is then analysed and should the risk to the business pose to be "high" then this is then entered onto the "CROO document" (See Clause 6.1) to assist in mitigating the risk to the business.

Should any non-conformances occur or be identified then an internal audit report / non-conformance report must be completed to ensure that a full analysis of the problem is resolved. A summary of all actions will be maintained within the Management Action Log (CAPA LOG).

The corrective action plan summary must be completed, as this then forms part of the Management Review meeting.

10.2 Continual Improvement

Continual Improvement will be ongoing through various elements of the Business Management System which is encompassed within this document. The list below is not exhaustive: -

- CROO Document – Evaluated at several stages (clause 5.1, 6.1)
- ISMS Policy / Objectives
- Competency Matrix
- Customer Satisfaction
- Internal Audits
- 3rd Party External Audits
- Management Review