<Full Name>

Information Security Manual

Conforms to ISO 27001:2013

Revision history

Revision	Date	Record of Changes	Approved By
0.0	[Date of Issue]	Initial Issue	

Control of hardcopy versions

The digital version of this document is the most recent version. It is the responsibility of the individual to ensure that any printed version is the most recent version. The printed version of this manual is uncontrolled, and cannot be relied upon, except when formally issued by the <Document Controller> and provided with a document reference number and revision in the fields below:

Document Ref.		Rev.		Uncontrolled Copy	X	Controlled Copy	

Contents

1 Introduction

<Short Name> has developed and implemented an Information Security Management System (ISMS) which enables us to:

- assess and treat information security risks in accordance with our particular needs
- demonstrate commitment and compliance to global best practice
- demonstrate to customers, suppliers and stakeholders that security is paramount to the way we operate
- better secure all financial and confidential data, so minimising the likelihood of it being accessed illegally or without permission

This manual describes our ISMS and sets out the authorities and responsibilities of those operating within it, as well as referencing those procedures and activities that fall within its scope.

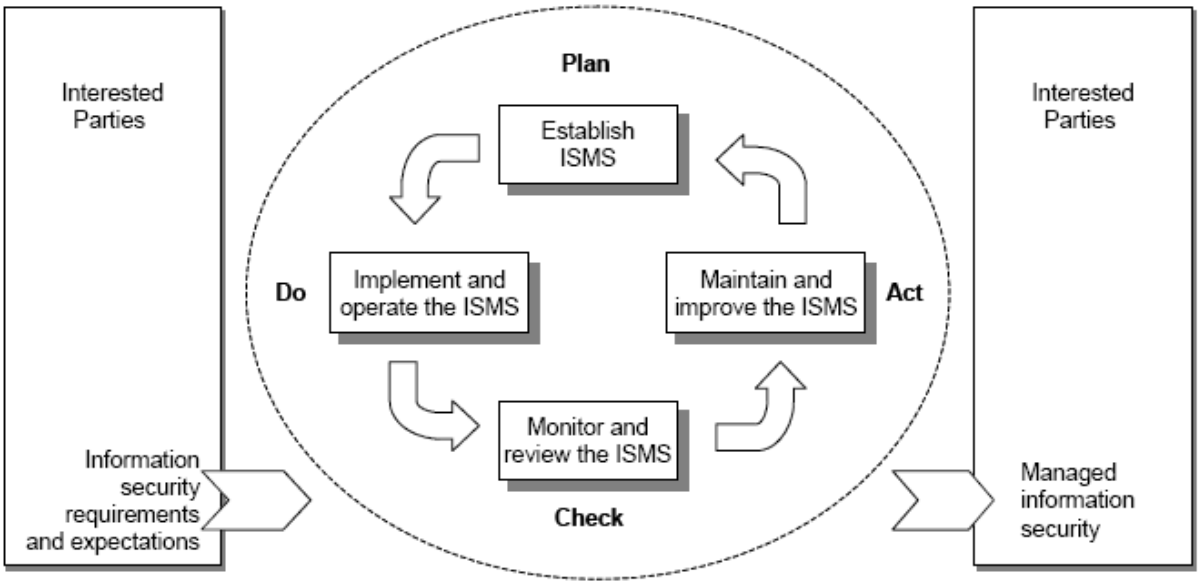
1.1 ISO 27001:2013

Our Information Security Management System (ISMS) has been developed in compliance with the ISO 27001:2013 standard which sets out a process based approach for establishing, implementing, maintaining and continually improving an information security management system within the context of our organisation.

Understanding and managing our interrelated processes as a system enables us to control the interrelationships and interdependencies so that our overall performance is enhanced.

Management of the processes and the system as a whole is achieved using the Plan-Do-Check-Act (PDCA) cycle with an overall focus on using risk based thinking to take advantage of opportunities and prevent undesirable results.

1.2 Plan-Do-Check-Act (PDCA) cycle



2 References

Standard	Title	Description
ISO 27000:2014	information security management Systems	Overview and vocabulary
ISO 27001:2013	information security management Systems	Requirements
ISO 27002:2013	Information technology - security techniques	Code of practice for information security controls
ISO 19011:2011	Auditing Management Systems	Guidelines for auditing

3 Terms and Definitions

The terminology used in this ISMS reflects both that used in ISO 27001:2013 and:

- standard business/quality terminology
- terms and vocabulary typically used within our scope of activity
- terms typically used in standards and regulations as they relate to our scope of activity

“we” and “our” refer to <Short Name>.

“Top Management” as referred to in ISO 27001:2013 is represented in <Short Name> by the <Senior Management Team>.

4 Business Context

4.1 Understanding our organisation and its context

4.2 Understanding the needs and expectations of interested parties

To fully understand our business we identify all key internal and external issues that are relevant to our operations and which affect our ability to achieve the intended outcomes of this information security management system.

This involves:

- understanding our core products/services/processes
- understanding the scope of our information security management system
- identifying those interested parties (“stakeholders”) who are relevant to our information security management system
- identifying and understanding the requirements of those internal and external interested parties relevant to information security

Many such issues are identified through an analysis of risks facing either ourselves or our stakeholders.

Our stakeholders and relevant internal and external issues are identified and are monitored as part of information security management reviews and updated as necessary.

The methodology we employ in achieving this understanding is set out in the ISMS Identification of Information Security Context Procedure.

We operate and maintain our ISMS Compliance With Legal and Contractual Requirements Procedure to ensure conformance with:

- legal, statutory, regulatory or contractual obligations related to information security
- any security requirements

4.3 Scope of the information security management system

4.3.1 Scope

Our information management security system satisfies the requirements of ISO 27001:2013 and, based on our understanding of our business and the needs and expectations of our stakeholders, addresses and supports our processes at our head office in Boston for management, administration and the design, development, manufacturing, installation and servicing of our products, including software development and maintenance.

Insert your scope statement above. This should summarise your activities/products/services that are subject to this information security management system in a single sentence. If you intend to subject your system to independent third party certification in due course, this summary will be shown your ISO 27001:2013 certificate.

Top management must define the scope of your ISMS implementation to match the scope of the information that the ISMS is aiming to protect. Getting the scope right for your purposes can be tricky, so we will go into a little detail.

It doesn't matter how or where this information is stored, you are setting out to protect this information no matter where, how, and by whom this information is accessed.

So, for example, if you have mobile devices, then even if they contain no sensitive information, they would fall within the scope if they can remotely access secure information stored on your network.

If you go for certification, the auditor will check if all the elements of the ISMS work well within your scope, he won't check the departments or systems that are not included in your scope.

Basically, ISO 27001 says you have to do the following when defining the scope:

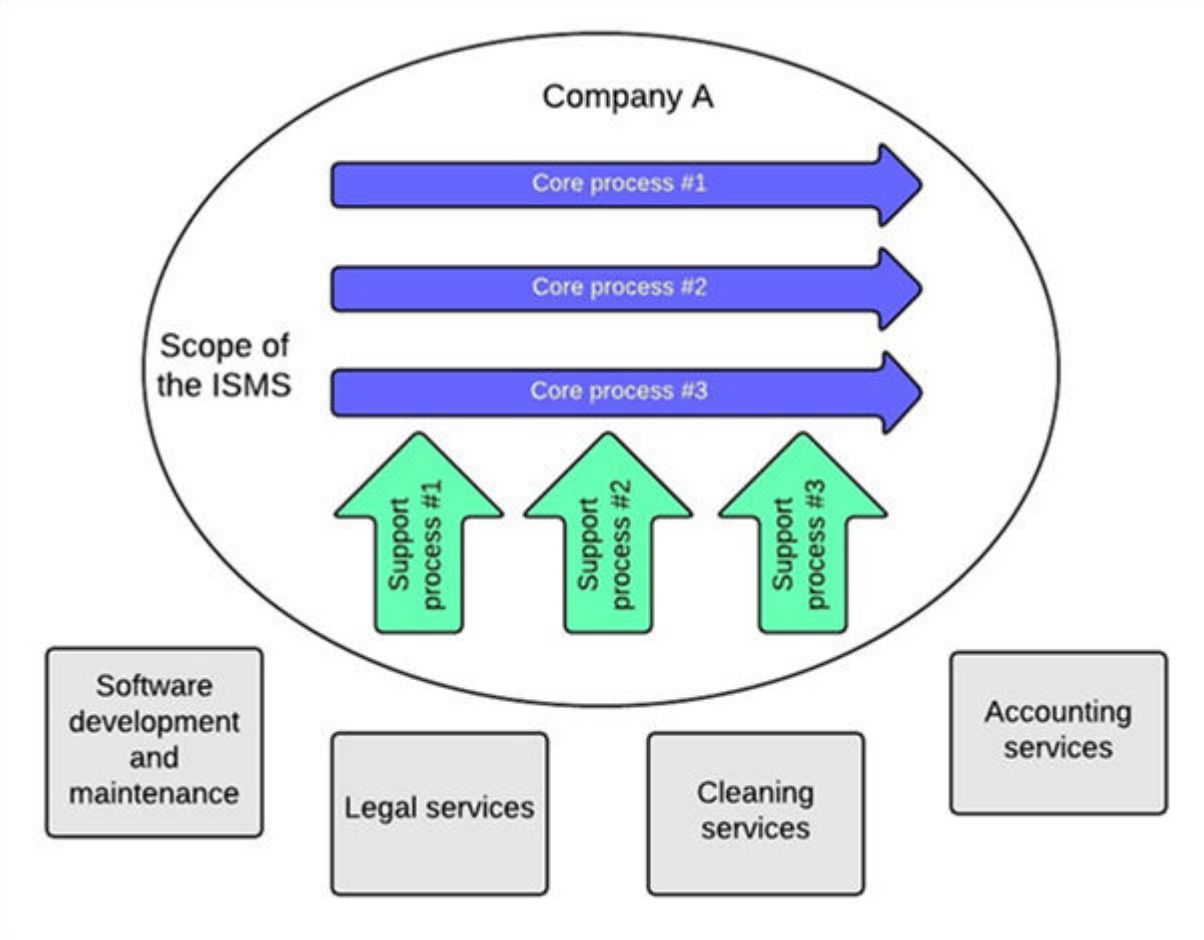
- *take into account internal and external issues defined in clause 4.1*
- *take into account all the requirements defined in clause 4.2*
- *consider interfaces and dependencies between what is happening within the ISMS scope and the outside world*

Although it is not required by the standard, it is often helpful to include a short description of your location (you could use floor plans to describe the perimeter) and organisational units (e.g., org charts) in your documented scope.

Dependencies

To best visualise this, draw your processes (all business processes, not just security or IT processes) that are included in your ISMS scope, and then outside of this circle draw the processes that are provided from outside of your scope.

If you have already implemented ISO 9001, you probably have a similar process chart like this:



*Once you know the dependencies, you have to identify the **interfaces**. Once you have identified the interfaces and their inputs/outputs you can include them in the scope if they impact on information security.*

27001 Example Scopes

The Information Security Management System (ISMS) applies to the control of our entire business, premises and resources within the UK. Premises and resources outside of the UK are excluded from the ISMS scope.

The ISMS is scoped to include all business processes conducted by the IT department at XYS motors. All other business units are excluded from scope.

The ISMS will protect the confidentiality, integrity and availability of XYS motors customer data at all times while in UK offices. This includes IT department, call centres and XYS office locations.

When determining this scope, we have considered:

- our organisation and its context (both internal and external issues)
- the needs and expectations of interested parties
- the interfaces and dependencies between activities performed by ourselves, and those that are performed by other organisations

4.3.2 Exclusions

The following are excluded from this information security management system, as they are not applicable to our business.

Exclusions	Reason for Exclusion
Example : Teleworking (A.6.2)	We have not implemented teleworking at present. All employees need to attend the company premises and work from there.

Insert any exclusions in the above table or state specifically that there are no exclusions.

4.3.3 Business locations within the scope

This information security management system applies to our business activities at:

Address Line 1

Address Line 2

Address Line 3

Address Line 4

Insert the address of your organisation above. If you have multiple sites which are covered by this ISMS, then you need to list each site to clarify the scope of the application of the ISMS.

4.4 Information security management system

To achieve our Information Security Objectives, we have established, implemented, maintained and continually improve our information security management system, including the processes needed and their interactions.

Our information security management system takes into consideration the needs and expectations of interested parties.

5 Leadership

5.1 Leadership and commitment

The <Senior Management Team> demonstrates leadership and commitment to achieving the objectives of our information security management system by taking accountability for the effectiveness of our information security management system and ensuring that:

- an Information Security Policy and Information Security Objectives are established for the management system and that they are compatible with our strategic direction and context
- our information security management system requirements are integrated into our business processes as appropriate
- our information security management system is suitably resourced
- there is clear communication on the importance of effective information security management and of conforming to the management system requirements
- our information security management system achieves its intended results

- all personnel are encouraged to contribute to the effectiveness of the management system
- continual improvement is actively promoted
- our information security policies, objectives and targets are, where appropriate, reflected in individual responsibilities and performance objectives

5.2 Information Security policy

The <Senior Management Team> has developed our Information Security Policy, which is to:

"Establish, monitor and continually improve our safeguards for the confidentiality, integrity and availability of all physical and electronic information assets to ensure that regulatory, operational and contractual requirements are fulfilled."

This is a simple example. You could adopt something similar or include some or all of the Information Security Objectives you establish below. It is up to you, but it must:

- *be appropriate to the purpose of your organisation*
- *include Information Security Objectives (see 6.2), or provide the framework for setting Information Security Objectives*
- *include a commitment to satisfy applicable requirements related to information security*
- *Include a commitment to continual improvement*

For more examples just Google "example information security policies"!

This policy governs our day-to-day operations to ensure the security of information and is communicated and implemented throughout our organisation. Our Information Security Policy is made available as a stand-alone document and widely distributed, including during induction.

Our Information Security Policy is typically reviewed annually, as part of our information security management review program, or as required to recognise the changing needs and expectations of relevant interested parties or the risks and opportunities identified by the risk management process.

5.3 Organisational roles, responsibilities & authorities

The <Senior Management Team> has assigned responsibilities and authorities for all roles relevant to the full and proper implementation, operation and maintenance of this management system, including the following:

Responsibility	Principal Responsible Persons
Determination of organisational context, establishment of overall direction, framing of policies for information security management, and conduct of management review	<Senior Management Team>
Ensuring the promotion of a focus on information security matters throughout the organisation	<Senior Management team>, <ISMS Manager>, <IT Manager>

Framing of ISMS objectives, targets, and plans	<Senior Management team>, <ISMS Manager>, <IT Manager>
Control of ISMS documents	<Document Controller>
Control of ISMS records	<Document Controller>
Information security training, awareness and competence	<HR Manager> and <ISMS Manager>
Management of internal ISMS audits	<Audit Manager>
Corrective and/or preventive actions	<ISMS Manager>
Assessment and treatment of information security risks	<ISMS Manager> and Risk Owners
Ensuring that our information security management system conforms to applicable standards	<ISMS Manager>
Implementation, operation, monitoring, review, maintenance, and Improvement of the ISMS	<ISMS Manager>
Ensuring that the integrity of our information security management system is maintained when changes are planned and implemented	<ISMS Manager.
Organising of independent review of information security management practices of the company	<ISMS Manager> and <Audit Manager>
Achieving and maintaining appropriate protection of organisational assets, and ensuring that information receives an appropriate level of protection	<ISMS Manager>
Human resources security (prior to employment, during employment, and, on termination or change of employment)	<HR Manager> and <ISMS Manager>
Physical and environmental security	<Facilities Manager> and <ISMS Manager>
Communications and operations management	<ISMS Manager>
Media handling and information exchange	<ISMS Manager>
Network security management and access control	<ISMS Manager>
Acquisition, development, and maintenance of information systems	<IT Manager>, <Purchasing Manager>, <ISMS Manager>
Information security incident management	<ISMS Manager>
Business continuity management	<ISMS Manager>
Complying with legal and regulatory requirements regarding information security	<ISMS Manager>
Complying with contractual obligations regarding information security	<Sales Manager> and <ISMS Manager>

These responsibilities and authorities are communicated through the combination of our Organisation Chart and internal Job Titles.

All managers are expected to demonstrate their commitment to the development and improvement of our information security management system through:

- the provision of necessary resources
- their involvement in the internal audit process
- their proactive involvement in continual improvement activities
- focusing on the improvement of key system processes

All managers are responsible for the implementation of the policies, processes and systems described in this manual and for planning (jointly with the <ISMS Manager>), controlling and resourcing our information security management system processes within their area of responsibility.

All personnel are responsible for the implementation of the policies and procedures applicable to processes they perform and are encouraged to identify and report any known or potential problems and to recommend related solutions.

6 Planning

6.1 Addressing risks and opportunities

In creating this information security management system, we have identified the risks and opportunities that need to be addressed, based particularly on: *4.1 Understanding our business*, and *4.2 Understanding the needs and expectations of our stakeholders* but also including all other aspects of our information security management system. Those risks and opportunities have been addressed to:

- ensure that our information security management system can achieve its intended outcomes
- enhance desirable effects
- prevent, or reduce, undesirable effects
- achieve continual improvement

When managing risks and opportunities we have defined and apply an information security risk assessment process that establishes and maintains information security risk criteria, including both the risk acceptance criteria, and criteria for performing information security risk assessments.

- we consider risks and opportunities when taking actions within our information security management system, as well as when implementing or improving our information security management system
- formal risk management may not be utilised in all circumstances and the level of risk assessment, analysis, actions and recording will be to a level appropriate to each circumstance

- the actions we take to address risks and opportunities are proportionate to the potential impact on information security

We operate and maintain arrangements to identify, assess, evaluate and treat our information security risks and opportunities as set out in our ISMS Control of Risks and Opportunities Procedure.

6.2 Establishing and achieving Information Security Objectives

6.2.1 General

The <Senior Management Team> have developed our Information Security Objectives, which are to:

- ensure that we can continue operations with minimal disruptions
- ensure absolute integrity for all information that we disburse or produce
- manage all information with appropriate confidentiality
- include information security training in our induction process
- minimise information security incidents to less than four per year

An example "simple" set of Information Security Objectives is given above. State your own Information Security Objectives here.

These objectives take into account our information security requirements and those risks and opportunities that we have identified.

The <Senior Management Team> ensures that our Information Security Objectives are:

- consistent with our Information Security Policy
- measurable (if practicable)
- monitored
- communicated
- updated as appropriate

Progress towards achieving each target, and the targets themselves, are reviewed during information security management review meetings by the <Senior Management Team> and updated as necessary.

These objectives and, where appropriate, the results of the <Senior Management Team>'s reviews, are communicated to all employees, customers, suppliers, contractors, interested parties and the wider community.

We maintain documented information on each of our Information Security Objectives.

When a process does not meet its objective(s), or an unexpected problem is encountered with a process, our ISMS Control of Corrective and Preventive Action Reporting (CPAR) Procedure is employed to research and resolve the issue and, wherever possible, improve the process.

6.2.2 Planning actions to achieve our Information Security Objectives

When planning how to achieve our Information Security Objectives, we determine:

- what will be done
- what resources will be required
- who will be responsible
- when it will be completed
- how the results will be evaluated, including indicators for monitoring progress toward achievement of our measurable Information Security Objectives.

Wherever practicable, we seek to integrate actions to achieve our Information Security Objectives into our business processes.

Periodically, or whenever our Information Security Objectives are changed, the <ISMS Manager> prepares an ISMS Objectives Realisation Plan, which is submitted to the <Senior Management Team> for approval, implementation and monitoring.

6.3 Change management

This manual constitutes our overall plan for establishing, maintaining and improving our information security management system.

Whenever changes are to be made to processes or our information security management system, those changes are planned, implemented, and then verified for effectiveness as set out in our Control of Management System Documentation Procedure.

Our information security management review and internal audit processes ensure the continuing integrity of the ISMS when significant changes are planned.

7 Support

7.1 Resources

7.1.1 General

The <Senior Management Team> ensures that all necessary resources are available to:

- implement and maintain this information security management system
- continually improve its effectiveness

Resources and resource allocation are assessed and monitored during information security management reviews.

7.2 Competency, and

7.3 Awareness, and

7.4 Communication

We operate and maintain arrangements to ensure competency, awareness and communication as set out in our Competency Communication and Awareness Procedure.

These arrangements ensure that:

- all staff are competent to undertake their tasks
- all staff are aware of:

  - our management system(s) and their related policies and objectives
  - their roles and responsibilities
  - their contribution to the effectiveness of our management system(s)
  - the benefits of improved personal performance
  - the importance of complying with our management systems, policies and procedures
  - the consequences of any departure from our management systems, policies and procedures
  - emergency preparedness and response requirements
  - any management system changes
  - the results of the <Senior Management Team>'s annual review of management system(s) compared to their objectives
- training needs are identified
- appropriate training plans are developed and implemented (with the <HR Manager>)
- each role affecting management system outcomes is recorded in the Role Profile Register

In addition to our staff, awareness programmes are also provided for contractors, temporary workers and visitors etc. as appropriate.

7.5 Documentation and records

7.5.1 General

Our information security management system documentation includes both documents and records[1].

The <Senior Management Team> has determined the extent of documented information:

- required by the ISO 27001:2013 International Standard
- necessary for the effectiveness of our information security management system

Based on the following criteria:

- the size of our business
- the scope, complexity and interaction of our processes and products/services
- the need to demonstrate fulfilment of our compliance obligations
- the competence of our personnel

[1] While ISO 27001:2013 uses the sole term "documented information" our quality management system uses both "document" and "record" to avoid confusion. For our purposes, a "document" is a written information used to describe how an activity is done and a "record" is documented evidence of the completion of an activity.

7.5.2 Control of documents

We operate and maintain arrangements for the control of our quality management system documentation as set out in our Control of Management System Documentation Procedure.

By means of this procedure we ensure that staff have access to the latest, approved information, and that the use of obsolete information is restricted.

Once established, all documented procedures are implemented and maintained.

7.5.3 Control of records

We operate and maintain arrangements for the identification, storage, retrieval, protection, retention, and disposition of environmental records as set out in our Control of Management System Records Procedure.

This procedure also defines the methods for controlling records that are created by and/or retained by suppliers.

These controls are applicable to all those records which provide evidence of conformance to our information security management system, Information Security Objectives and regulatory and other obligations.

8 Operations

8.1 Operational planning and control

The <Senior Management Team> ensures that the processes needed to meet our information security management system requirements, to address risks and opportunities and to establish and achieve our Information Security Objectives, are properly planned and controlled.

- we identify, assess and treat our information security risks and opportunities as set out in our ISMS Control of Risks and Opportunities Procedure
- the <ISMS Manager>, periodically, or whenever Information Security Objectives are changed, prepares an ISMS Objectives Realisation Plan which is submitted to the <Senior Management Team> for approval, implementation and monitoring
- we retain, analyse and evaluate records to the extent necessary to have confidence that the processes have been carried out as planned
- we control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary
- we control/influence out-sourced processes in accordance with our ISMS Control of Outsourced Processes Procedure
- when a process does not meet its objective(s), or an unexpected problem is encountered with a process, our ISMS Control of Corrective and Preventive Action Reporting (CPAR) Procedure is employed to research and resolve the issue and, wherever possible, improve the process
- we review the suitability, adequacy and effectiveness of this management system, in accordance with our ISMS Control of Management Reviews Procedure, at planned intervals

These reviews include assessing the information security management system's continuing alignment to our strategic direction, opportunities for improvement, and the need for changes

8.2 Information security risk assessment

The <Senior Management Team> ensures that information security risk assessments are undertaken, recorded and retained, both periodically and when significant changes are proposed or occur

These risk assessments take into account both our agreed risk assessment criteria and criteria for performing information risk assessments as set out in our ISMS Control of Risks and Opportunities Procedure.

8.3 Information security risk treatment

We manage and control our risks as set out in our ISMS Control of Risks and Opportunities Procedure.

9 Performance Evaluation

9.1 Monitoring, measurement, analysis and evaluation

To evaluate the performance of our information security management system, we determine:

- what needs to be monitored and measured
- the methods of monitoring, measurement, analysis and evaluation needed to ensure valid results
- the criteria against which we evaluate our information security performance and various indicators
- when such monitoring and measurement should be undertaken
- when the results from monitoring and measurement are to be analysed and evaluated

These activities are used to evaluate:

- the performance and effectiveness of the information security management system
- the effectiveness of actions taken to address risks and opportunities
- the effectiveness of planning
- the performance of external providers
- other improvements to the management system

We operate and maintain arrangements for this monitoring, measuring, analysis and evaluation as set out in our ISMS Control of Monitoring, Measuring, Analysis and Evaluation Procedure.

9.2 Internal audit

We operate and maintain arrangements for internal auditing at planned intervals as set out in our Control of Internal Auditing Procedure.

By means of these audits, we provide information to management and determine whether our information security management system:

- conforms to our own requirements
- conforms to the requirements of the ISO 27001
- is effectively implemented and maintained
- is effective in achieving our management system's policies and objectives

9.3 Management review

We operate and maintain arrangements for the review the the suitability, adequacy and effectiveness of our information security management system, at planned intervals as set out in our ISMS Control of Management Reviews Procedure.

These reviews include assessing our information security management system's continuing alignment to our strategic direction, opportunities for improvement, and the need for changes.

10 Improvement

10.1 General

We use our information security management system, and other inputs, to continuously improve our information security outcomes.

The improvement opportunities we seek include:

- addressing evolving and future needs and expectations
- correcting, preventing and reducing undesired effects
- improving the performance and effectiveness of this information security management system

10.2 Non-conformity and corrective action

We operate and maintain arrangements to take corrective action to eliminate and further prevent the cause of any non-conformity, and preventive action so as to eliminate the causes of potential similar non-conformities, as set out in our ISMS Control of Corrective and Preventative Action Reporting (CPAR) Procedure.

10.3 Continual improvement

We seek to continually improve the suitability, adequacy and effectiveness of this information security management system.

We use the results of analysis and evaluation, and the outputs from information security management review, to identify needs and opportunities for such improvement.

The overall effectiveness of our program of continual improvement, including both corrective actions and our wider progress in achieving corporate level improvement objectives, is monitored and assessed through our information security management review process.

11 Annex A – Control Objectives and Controls

We adopt those information control objectives set out in Annex A of ISO 27001:2013 as appropriate, and add additional control objectives and controls where necessary.

We set out our approach to the objectives and controls set out in Annex A in our high level control objectives and control documents:

- A6 Organisation of Information Security
- A7 Human Resource Security
- A8 Asset Management
- A9 Access Control
- A10 Cryptography
- A11 Physical and Environmental Security
- A12 Operations Security
- A13 Communications Security
- A14 Acquisition Development and Maintenance of Information Systems
- A15 Information Security in Supplier Relationships
- A16 Information Security Incident Management
- A17 Business Continuity Management
- A18 Information Security Reviews

Add in here any further controls you adopt and remove any of the above that you deem unnecessary.

We detail those operational policies and procedures necessary to ensure the consistent application of appropriate controls across all activities and systems within the scope of our ISMS, in Management Instructions to operatives and users.

12 Appendix 1 - Organisation Chart

Add your organisation chart here to demonstrate who is responsible for what.

13 Appendix 2 - Organisational High Level Process Map

Add your high-level process map here, it should feature all of the processes you have identified above and show how those processes interact.