ISO27001:2013 ISMS POLICY DOCUMENT

Version 6

25 May 2018

Table of Contents

1 Introduction....4
2 Issue Status 5
3 Overview of Systematics International Ltd 6
3.1 Scope of Registration....6
4 Information Security Management System....7
4.1 Documented Information....8
4.1.1 Documents 9
4.1.2 Control of Records 9
5 Management Commitment 9
5.1 Role of Senior Management....9
6 ISMS POLICY 10
6.1 Introduction....10
6.2 Scope of the Policy 10
6.3 legal and regulatory obligations....11
6.4 Roles and Responsibilities....11
6.5 Strategic Approach and Principles 12
6.6 Business Continuity Management....15
6.7 Approach to Risk Management 17
6.8 Information Security Objectives....18
6.9 Responsibility, authority and communication 19
6.10 Management Review 19
6.11 Review Input 21
6.12 Review Output....21
7 Provision of Resources....22
7.1 Human Resources General 22
7.2 Infrastructure 22
8 Risk Assessment Methodology....24
8.1 Risk Treatment Plan 23
9 Measurement, Analysis & Improvement....24
9.1 Information Security Standards 24
9.2 Internal ISMS Audits 24
9.3 Monitoring & Measurement of Processes 25
9.4 Monitoring & Measurement of Service 25
9.5 Analysis of Data 25

9.6 Continual Improvement 26
9.7 Corrective Action and Improvement 27
9.8 Compliants Policy 27
9.9 Peventative Action 27

10 Appendices 28
10.1 Appendix 1 – Organisation Chart 28
Appendix 2 – List of Controlled Documents 29

1 INTRODUCTION

This document is the ISMS Policy Document of **Systematics International Ltd ("Systematics")**. It is the property of **Systematics** and is a controlled document.

The purpose of the ISMS Policy Document is to provide an overview of the company, the activities it carries out and the quality standards of operation it conforms to. It is not designed to act as a procedure manual, although it does carry information about where procedures information is located and the detailed information on Documentation Requirements for essential procedures e.g. document control, and control of records; internal audit and corrective/preventative action (please see Procedures Log).

Throughout this ISMS Policy Document there are explanations of the requirements of the standard, paraphrased and appended in smaller grey text. This precedes a section explaining how the company implement this particular aspect of the standard.

Information security is the protection of information to ensure:

- Confidentiality: ensuring that the information is accessible only to those authorized to access it.
- Integrity: ensuring that the information is accurate and complete and that the information is not modified without authorization.
- Availability: ensuring that the information is accessible to authorized users when required.

2 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 Policy Document.

When any part of this ISMS Policy Document is amended, a record is made in the Amendment Log shown below.

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

The ISMS Policy Document will be reviewed on an Annual basis as standard.

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

Issue	Amendment	Date	Initials	Authorised
1	1st Authorised Issue	01/06/15	MB	CB
2	2nd Authorised Issue	25/02/16	MB	CB
3	3rd Authorised Issue	25/05/16	MB	CB
4	4th Authorised Issue	29/03/17	MB	CB
5	5th Authorised Issue	16/01/18	MB	CB
6	6th Authorised Issue	25/05/18	MB	CB

3 OVERVIEW OF SYSTEMATICS INTERNATIONAL LTD

Systematics International Limited, in its current format was established in 2007 and is based in Battlebridge, Essex employing ten members of staff; inclusive of the two directors.

The organization handles highly customised data requirements which allow their system to adjust to customer needs quickly, efficiently and at low cost. As an independent business with no accountability to profit-focused, non-industry shareholders or the market, Systematics is able to adapt quickly to changes both in the marketplace and customers' requirements, making simple and radical decisions very quickly and on a highly informed basis.

The organization has a passionate, committed team, with each of their data exchanges managed and delivered by dedicated key Systematics staff, all of whom have received significant internal and external training. As a result, they have considerable expertise and knowledge of their particular exchanges, enabling them to resolve issues and address queries within agreed timeframes.

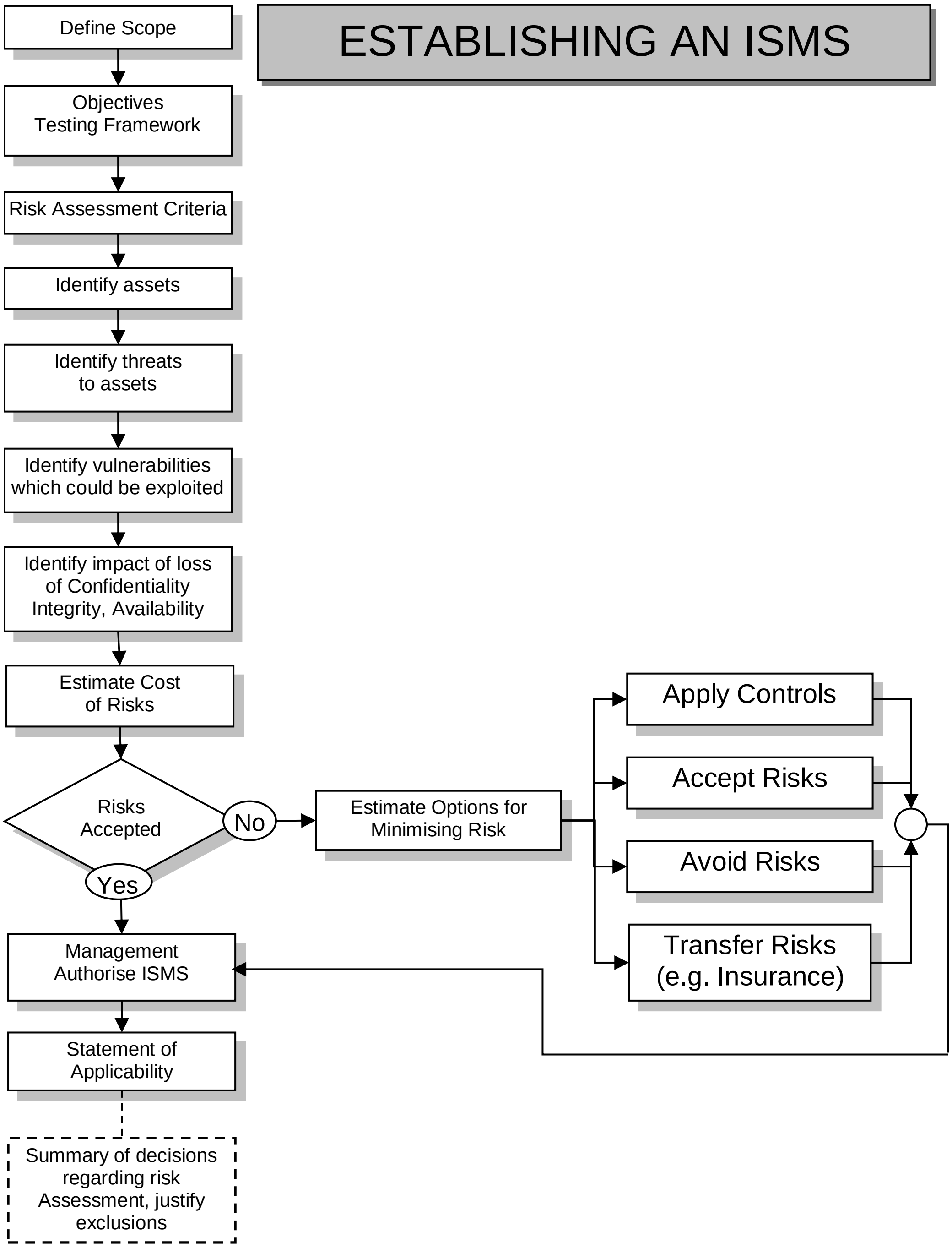
Systematics rigorously comply and adhere with all external data regulations, including the European Commission's ruling that competitive data cannot be disclosed for a period of less than twelve months in the EEA markets. In order to provide a service with no compromises, Systematics routinely carries out criterion tests on aggregate data before publishing industry reports.

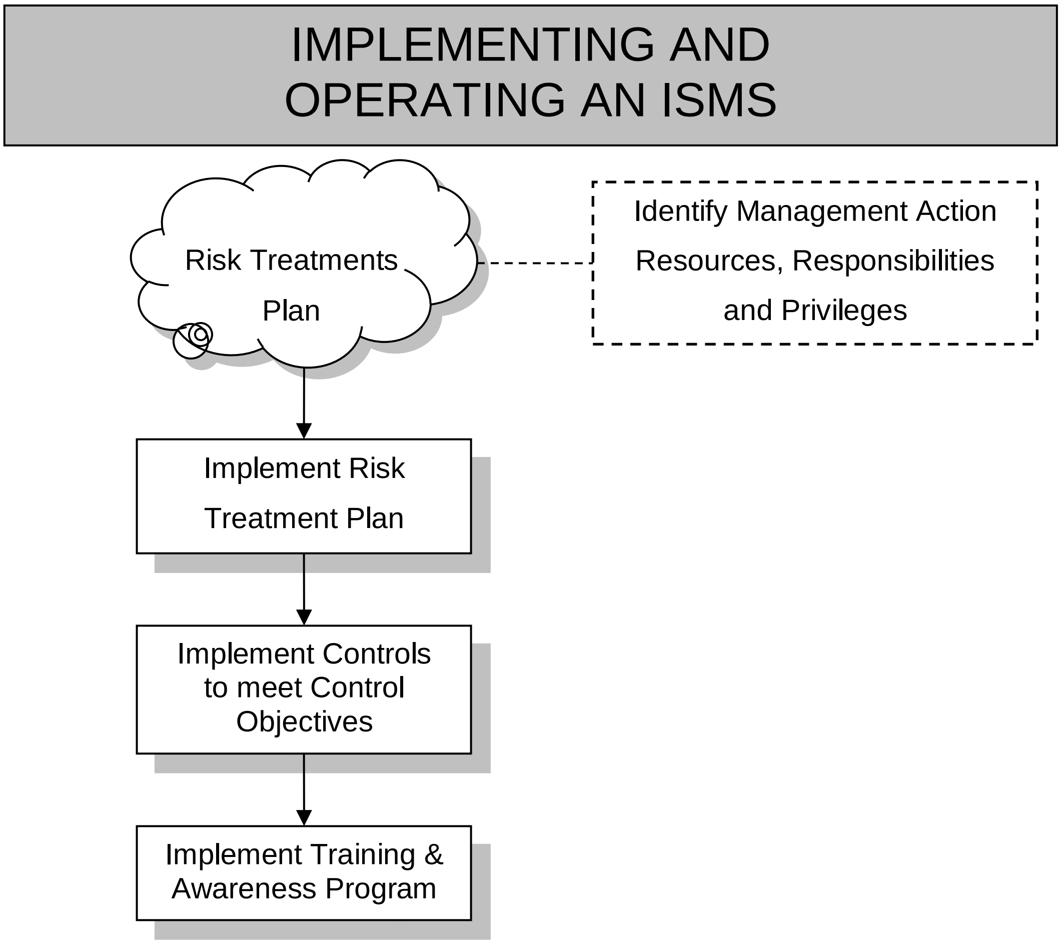
Current clients include: CNH, Claas, John Deere, SDF, Agco, JCB, Krone, Kuhn, TAFE, Nissan Forklift, Toyota, Terex and Liebherr.

3.1 Scope of Registration

Data processing, manual and automated upload and data processing of client information and security.

4 INFORMATION SECURITY MANAGEMENT SYSTEM


ESTABLISHING AN ISMS
Define Scope
Objectives Testing Framework
Risk Assessment Criteria
Identify assets
Identify threats to assets
Identify vulnerabilities which could be exploited
Identify impact of loss of Confidentiality Integrity, Availability
Estimate Cost of Risks
Risks Accepted
No
Yes
Estimate Options for Minimising Risk
Apply Controls
Accept Risks
Avoid Risks
Transfer Risks (e.g. Insurance)
Management Authorise ISMS
Statement of Applicability
Summary of decisions regarding risk Assessment, justify exclusions


IMPLEMENTING AND OPERATING AN ISMS
Risk Treatments Plan
Identify Management Action Resources, Responsibilities and Privileges
Implement Risk Treatment Plan
Implement Controls to meet Control Objectives
Implement Training & Awareness Program

Systematics has a commitment to quality and a formal information security management system (ISMS) that addresses the following areas:

- Quality
- Performance monitoring and review
- Policy and Procedures
- Managing external relationships
- Financial Management
- Strategic and business planning
- Human resource development
- Service innovation.

4.1 DOCUMENTED INFORMATION

4.1.1 Documents

All documents (statement of Intent) are maintained and controlled by the Information Security Officer. Policy and procedure documents are reviewed annually. Any documents requiring amendment are updated, authorised, and completed. All updates to documents are signed and dated by the Information Security Officer. Documents are re-issued as an electronic PDF document and a limited number of hard copies are produced. Obsolete documents will be archived and restricted by the Information Security Officer, electronic copies of all past versions are kept.
All managers hold responsibility for cascading information to staff.

4.1.2 Records

All project records (evidence of past performance) are stored in appropriate electronic folders and managed by respective departments. Hard copies of documents are restricted to a minimum and should not be produced unnecessarily. Electronic records are encouraged over hard copies due to environmental concerns, available storage space and to prevent unnecessary expenditure.

5 . LEADERSHIP

5.1 Role of Senior Management

Systematics Senior Management Team are committed to the development and implementation of an Information Security Policy, an Information Security Management System, and to frequently review this system. Responsibility has been assigned to ensure that the ISMS conforms to the requirement of the standard and the provision to report on performance to the senior management team has been defined.
The Information Security Officer will ensure that **Systematics** staff are aware of the importance of meeting customer as well as statutory and regulatory requirements, and overall, to contribute to achieving **Systematics** Information Security Objectives which are aligned with the current business plan.
The Senior Management Team is responsible for implementing the ISMS and ensuring the system is understood and complied with at all levels of the organisation.
They are responsible for ensuring that;

- The information security policy and objectives are established and in line with the strategic direction of the organisation
- Integration of the ISMS into the organisations processes.
- That resources needed for the ISMS are available
- Communication covering the importance of effective information security management and conformance to the ISMS requirements is in place.
- The ISMS achieves its intended outcome(s)
- The contribution of persons involved in the effectiveness of the ISMS by direction and support.
- Continual improvement is promoted
- Other management roles within their area of responsibility are supported.

An internal audit of procedures and policies is conducted annually in December. A review of the Information Security Objectives takes place in January. In addition achievement of the quality objectives are measured against quarterly targets set in relation to the business plan. Staff contribution towards the Information Security Objectives is measured in supervision and documented annual appraisals in March.

6 ISMS POLICY

6.1 Introduction

This document is the Information Security Policy for **Systematics**. It describes the company's corporate approach to Information Security and details how we address our responsibilities in relation to this vital area of our business. As a company we are committed to satisfy applicable requirements related to information security and the continual improvement of the ISMS.

Information Security is the responsibility of all members of staff, not just the senior management team, and as such all staff should retain an awareness of this policy and its contents and demonstrate a practical application of the key objectives where appropriate in their daily duties.

We also 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 information security management system. These include but not limited to customers and clients and their requirements are documented in contracts, purchase orders and specifications etc.

Verification of compliance with the policy will be verified by a continuous programme of internal audits.

6.2 Scope of the Policy

The scope of this policy relates to use of the database and computer systems operated by the company at its office in Battlesbridge, London, in pursuit of the company's business of providing the highest quality statistical reports to manufacturing industries worldwide. It also relates where appropriate to external risk sources including functions which are outsourced.

This policy applies to all **Systematics** staff, contractors, joint ventures and representatives of vendors and business partners, specifically anyone who:

- uses or connects to **Systematics** computer resources
- has access to personal or business confidential data held by **systematics**
- is involved in business processes that generate and receive electronic transmissions
- uses computer systems, telephone systems or devices that are linked to, part of or manage the network or electronic resources (i.e. both fixed and mobile computerised system)

6.3 Legal and regulatory obligations

Systematics is fully aware of its legal obligations to confidentiality and therefore we comply with the following regulations and obtain updates from www.gov.uk

- Data Protection Act 1998
- Employment Law Act
- EU Competition Law – 1999 DGIV Undertakings
- EU Competition Law – 2011 Guidelines
- Privacy and Electronic Communications Regulation 2003
- Computer Misuse Act 1990
- Malicious Communications Act 198
- Trade Associations guidelines (AEA, AEM, JIVA, FEM, VDMA, CEMA, etc)
- Bribery Act 2010
- Companies Act 2006
- Equality and Diversity Act 2010
- Competition and Markets Authority
- The Waste Electric and Electronic Equipment (WEEE) Regulations 2013
- GDPR (25th May 2018)

6.4 Roles and Responsibilities

Our Information Security Manager (This role is carried out by our Chief Finance and Strategic Planning Officer) is responsible for randomly sampling records to ensure that all required data has been captured, and that data is accurate and complete.

It is the responsibility of all staff to ensure that all data is treated with the utmost confidentiality, and that no data is given out without the prior authority of any person affected.

6.5 Strategic Approach and Principles

6.5.1 Information Classification & Labelling

All staff have access to the Statistical database which is structured to have different access levels. Data retrieved from the preformatted forms completed on the web site are automatically attached to the correct fields. However a visual check of all new records must be performed to verify that data was entered into the correct fields at the point of origin i.e. when a client enters their details into the web based form.

Classifications and associated protective controls for information should take account of business needs for sharing or restricting information, as well as legal requirements. Classification provides people who deal with information with a concise indication of how to handle and protect it. Creating groups of information with similar protection needs and specifying information security procedures that apply to all the information in each group facilitates this.

Systematics has adopted the following information confidentiality classification scheme:

a) Disclosure causes no harm – Information publically available;
b) Private & Confidential - disclosure causes minor embarrassment or minor operational inconvenience;
c) Private & Confidential - disclosure has a significant short term impact on operations or tactical objectives;
d) Private & Confidential - disclosure has a serious impact on long term strategic objectives or puts the survival of the organization at risk.

Labelling

The labelling of the information and its related assets in physical and electronic formats should reflect the classification scheme established above and it should be easily recognizable. Labels will be placed either at the top of the output report or below, depending on the type of report required.

Cases where publishing of non confidential information is omitted, this is purely to reduce the workloads.

6.5.2 Access Control

All user accounts (clients and staff) are provided based on their requirements of the accessing the system. Clients will have access **only** to their data. **Systematics** staff will have access to all industry data for obvious reasons as checks will need to take place to ensure that the data is correct, clean and meaningful.

Passwords MUST NOT be written down either on paper or retained electronically.

Passwords should be no less than 8 characters in length and consist of both numbers and letters.

User Identification, Authentication and Use of Electronic Information Assets

- Users must be uniquely identified and authenticated when accessing electronic information asset. Individual identity must be positively verified
- Users must maintain the confidentiality of system access methods
- Users are accountable and responsible for protecting electronic information asset accessed through or set up on their assigned computer systems
- Users must use reasonable precautions to physically protect equipment and **Systematics** electronic information
- Users must comply with use and disclosure processes as if electronic information were paper, and be accountable for executing appropriate agreements and/or obtaining required authorisations
- Requests to connect to non-Systematics owned devices to the Systematics Network must be approved by the Information Security manager and or Senior Developer, prior to establishing network connectivity
- Mobile computing technology allows user access to electronic information assets from within or out of the facility, with an increased risk of unauthorised disclosure: a) user must acknowledge risks and cooperate with security measures, b) Users using mobile devices must implement enhanced safeguards when working at off facility premises (e.g. home offices, airports, hotels and conferences)
- Individuals using personal devices (e.g. non Systematics PCs) containing Systematics information must take appropriate protective measures, i.e. (1) Use removable media which are securely stored when not is use, (2) No permanent storage of Systematics information on an individual's personal device, (3) Deletion of all Systematics information when the device is replaced or taken out of service, (4) Use approved remote secure access technologies if possible and appropriate, (5) Systematics has the right to access files and messages, including on non Systematics owned equipment that is connected to Systematics systems.

6.5.3 Incident Management

Any and all incidents must be reported immediately in the first instance to the Quality Manager who also fulfils the role of Information Security Manager.

- Information security incidents must be managed in an appropriate manner. User access and network connections may be suspended to maintain the integrity of **Systematics** systems.

- **Systematics** responses to information security incidents must cover:

  (1) Identification and reporting of information security incidents
  (2) Responding to suspected or known information security incidents
  (3) Mitigating harmful effects of known information security incidents
  (4) Documentation of information security incidents and outcomes

- Users must report information security incidents within 24 hours of discovery:
  (1) Direct to Information Security Manager and/or to the Senior IT Developer.
  (2) Record the incident using the agreed system.

6.5.4 Physical Security

Access to the office via three separate locks on the main door.

Access to the office is located on a privately owned site is through a main gate which unlocks at 07:00 and is locked at 18:00 every day. It was evidenced that on entering the site there are three CCTV cameras directed at various vantage points; one of which is Systematics' main entrance

Entry to Systematics site is fully alarmed with motion sensors throughout. Access is gained via three doors. The first is the main door into the reception area. The door was evidenced to have three locks fitted and addition bolts at the top and bottom. The second door provided access into the main administration office. This door was noted to have two main locks and again bolts. This door is usually closed. The two doors are both double glazed. The last entrance is at the rear of the premises through an emergency door. This entrance was noted to be fitted with three locks and, as with the others, bolts. Whilst the window in the back door is not double glazed it was evidenced that it was fitted with security glass. All windows at the site were noted to be locked and, as with the main doors are double glazed throughout.

All data is held on remote servers located within an outsourced data centre – Rackspace - which has amongst several certifications including ISO27001 and ISO9001 level security in place.

6.5.5 Third-party Access

Access to the data is available to only those authorised to view the individual company records. Competitors data are disclosed in conformity with the EU Competition Law.

6.6 Business Continuity Management

Systematics' entire external facing infrastructure is provided by an external Service Provider (Rackspace-http://www.rackspace.co.uk/managed-hosting/hosting-solutions/managed-hosting/data-centre-facilities/)

By using an external provider, we are able to provide a resilient, fast, 24/7 guaranteed service. The external hosted servers are also covered by managed backup solutions in addition to our own internal backup procedures. All software licenses on our remotely hosted and managed servers are held by Rackspace on behalf of **Systematics.**

- Microsoft Windows Server 2012 R2.
- Microsoft SQL Server 2014 R2
- Microsoft Internet Information Services version 11
- Continual website URL Monitoring informs us immediately if there is any interruption to our Internet services.
- Managed Backup provides daily backup to secure tape vaults.
- Cisco Firewall provides security to incoming connections.

Managed Microsoft Exchange Server (hosted by Rackspace.com) provides external email services for **Systematics** incoming and outgoing emails

<u>Data Security</u>

In House Data Security

Our local data security policy ensures that in the case of hardware loss or failure, data from the close of business on the previous working day can be restored to our systems. Data held at our local offices is backed up using the following methods:-

- Daily backups of files to removable disk cartridges, securely stored offsite in fireproof locked containers to which only Systematics employees have access. The daily backups are commenced first thing in the morning to cover the previous day's work, and are taken offsite at the end of the working day. This ensures that a backup is available to restore the system to the status from the previous working day in the event of data loss.
- Daily backups of SQL Server databases are taken to disk; these daily backups are included in the daily backup procedure. Disk backups of SQL Server databases are taken at 3am, and this ensures that the previous business day's data is contained on the offsite backup which is removed from the premises later that working day.
- Overnight replication of working files and SQL data is maintained to separate machines within the Systematics premises, in order to cover the event of single point of failure or partial hardware/software loss of data.
- A 2 hourly automated backup of SQL Server log tables is maintained, which can be restored in the event of software or hardware failure during the working day.

- Ad-Hoc backups are taken onto removable hard disks as required, for example when major updates have been undertaken.

Archive full data backups are also taken for all of our systems at the close of each period. These are held on the file system, and are incorporated into disk backup routines. The full data backups for each period close are held indefinitely for audit purposes.

External Data Security

Security of our externally hosted data is covered by the Service Provider Service Level Agreement in the case of data backup. We also maintain additional backups of external data to enable us to cover situations beyond those catered for in the standard SLA.

- All servers and equipment are housed in a SAS 70 Type II certified Data Centre in the UK, providing full network uptime and redundant Internet connectivity, with a guaranteed 24/7 network uptime.
- Full Cisco Firewall protection to all incoming connections.
- Daily managed backups of system and data files to tape. Restore of files within 4 hours is guaranteed.
- SQL Server archive backups taken at every period end for each system. These are transferred to our local premises and included in our file system and tape archives.
- Systematics online systems immediately store data batch files separately on the file system and in the database. This ensures that in the case of data loss, the data can be restored by one of a variety of methods.
- All data files are stored on a Storage Area Network, providing a separate data store with 100% uptime

Data can be restored up to the close of the previous working day guaranteed, and apart from in the case of full hardware failure, can be restored up to the latest point of data entry by using the file system based backups of the data which were created by the Systematics software.

Full disaster recovery and business continuity processes

Full disaster recovery and business continuity processes is in place and have been routinely demonstrated.

Systematics have procedures in place in the event of Disaster Recovery. These procedures are designed to provide the maximum salvage of data entered into the systems in the event of partial or full, software or hardware failure.

In House data disaster recovery procedure

Failure of hardware and software in the local **Systematics** offices would not cause any interruption to our internet facing services. Disaster recovery procedures for our local hardware are based on the following conditions:-

Our Dell File Servers are covered by 4 hour response from Dell in the event of full hardware loss. Once repaired/replaced, hardware and software will be returned to working order via tape backup from the previous working day.

In the event of data loss, restore data from removable disk backups from the previous working day.

Data restore from other external backups and archives as appropriate.

External data disaster recovery procedure

External fileserver hardware is guaranteed by Service Provider's Service Level Agreement to be replaced within 4 hours in the event of hardware failure.

In the event of hardware failure, once the hardware has been replaced, **Systematics** will then reconfigure settings remotely in order to restore full services within 1 business day. The reconfigured server will connect to the Storage Area Network for all data files at the state when the hardware failure occurred. **Systematics** will also endeavour to restore data from all possible backup sources to ensure that any loss of data which was entered after the last backup will be minimal.

6.7 Approach to Risk Management

We have carried out a full risk assessment of the potential for a breach of security as documented within our separate Risk Assessment Document.

We aim to reduce all opportunities for data to be compromised. This includes the possibility of theft of data.

6.7.1 Action in the event of a policy breach.

Access to the system is centrally controlled and removal of access to the system is a very simple procedure, which is controlled by the Information Security Manager and the Senior IT Developer within **Systematics.**

Similarly access to the premises is also controlled by the Information Security Manager who has allocated keys to the main staff.

Immediately a policy breach has been detected access is removed or reset depending upon the most appropriate action in the circumstances. A formal disciplinary process will also take place.

6.8 Information Security Objectives

Our objectives are set out in our business plan 2017-2020 and are then disseminated to the staff for incorporation into their roles. Each staff is responsible for delivering its objectives and this is monitored via individual appraisals & team meetings. **Systematics**'s Quality Objectives are as follows:

Objective 1: Existing services - **Systematics** will continue to deliver its services within a secure environment

Objective 2: Development - **Systematics** will conduct annual risk assessments to ensure that risk to information in the care of **Systematics** is minimised or eliminated.

Objective 3: Continued maintenance and adherence to the Statement of Applicability

Objective 4: To ensure availability of critical hardware and software applications twenty-four hours a day.

Objective 5: To continually strengthen and improve the overall capabilities of the information security management system

Objective 6: To ensure that information-related business operations continue to be carried out in line with the ISO 27001 standard and to establish a sustainable operation plan for business that is cost effective

Objective 7: To establish quantified information security goals annually through management and review meetings

Protection of company assets is vital to the success of our business. To this end, we have established an information security management system that operates all the processes required to identify the information we need to protect and how we must protect it.

Because the needs of our business change, we recognize that our management system must be continually changed and improved to meet our needs. To this effect, we are continually setting new objectives and regularly reviewing our processes.

ISMS Objectives
It is the policy of our company to ensure:

- Information is only accessible to authorized persons from within or outside the company.

- Confidentiality of information is maintained.

- Integrity of information is maintained throughout the process.

- Business continuity plans are established, maintained, and tested.

- All personnel are trained on information security and are informed that compliance with the policy is mandatory.

• All breaches of information security and suspected weaknesses are reported and investigated. A formal disciplinary process will also take place.

• Procedures exist to support the policy, including virus control measures, passwords, and continuity plans.

• Business requirements for availability of information and systems will be met.

• The Information Security Manager is responsible for maintaining the policy and providing support and advice during its implementation.

• All staff are directly responsible for implementing the policy and ensuring compliance across the company.

6.9 Responsibility, authority and communication

The management structure of **Systematics** is shown as an organisation chart (see **Appendix 1**) the chart shows functional relationships and responsibilities.

6.9.1 Management Representative

The Information Security Officer is responsible for the maintenance, measurement and review of our Information Security Management System. The Information Security Officer will ensure that the processes needed for the Information Security Management System are established, implemented and maintained within Systematics.

6.9.2 Internal Communications

Senior management communications framework to disseminate information about the effectiveness of the Information Security Management System is via its Team meetings.

6.9.3 Implementation

Following the annual audit, results will be collated and disseminated through **Systematics** internal communications framework:

6.10 Management Review

6.10.1 General

Senior Management ensures:

- That the ongoing activities of **Systematics** are reviewed regularly and that any required corrective action is adequately implemented and reviewed to establish an effective preventative process
- Measurement of **Systematics** performance is against our declared Information Security Objectives
- That internal audits are conducted regularly to review progress and assist in the improvement of processes & procedures. The reviews will be discussed as part of **Systematics** Board meetings
- That employees have the necessary training, support, specifications and equipment to effectively carry out the work.

The Systematics team hold planning and review meetings twice a year – 6 monthly intervals. Minutes of these are taken and the agenda normally includes an update and discussion around the current work of all departments and services.

6.11 Review Input

The annual Senior Management Team meetings review the following information:

- Risk management and the status of risk assessments and treatment plan
- Monitoring and measuring of results including internal audits
- Fulfilment of information security objectives
- Serious untoward incidents
- Status of preventive, non-conformances and corrective actions
- Follow up actions from previous management reviews
- Changes in external and internal issues that are relevant to the ISMS
- Recommendations / opportunities for continual improvements.
- Feedback from interested parties

6.11.1 Implementation

- Meetings are scheduled
- A suggested agenda is prepared by the chair
- Members invited to add items to the agenda
- Agenda is circulated to members
- Meeting take place
- Actions defined
- Meetings are minuted by a designated staff member
- Minutes are approved by Chair
- Minutes are circulated amongst members
- Completion of actions is reviewed at the next meeting.

6.12 Review Output

The Senior Management Team reviews produce the following outputs:

- Policies and procedures are updated to make operations more efficient
- Operations and services are improved through measurement against targets and actions to improve or rectify specific areas.
- Where resources are lacking, actions are put in place to rectify this.

6.12.1 Implementation

- Corrective actions are identified
- Targets created
- Improvements actioned
- Situation re-evaluated at a specified later date.

7 PROVISION OF RESOURCES

Systematics will provide all the resources needed to implement and maintain the Information Security Management System and improve effectiveness of the system. **Systematics** will also ensure that the resources needed to enhance the satisfaction and requirements of service users, service commissioners and staff are identified and in place through audit and continual review.

7.1 Human Resources General

7.1.1 Competence, Awareness & Training

Within our individual staff records, we maintain any certification obtained by the staff member demonstrating who has received what training and when.

Systematics provides training and awareness to continually advise **Systematics** staff about the Information Security Policy:

- Information security policies, standards and toolkits
- Training for employees appropriate to carry out their job-related duties
- Initial training within a reasonable period of time after an individual joins the workforce, preferably during induction period
- Documentation that training has been provided

7.2 Infrastructure

Systematics buildings, workspace, and associated utilities are managed by the Chief Executive Officer and the Chief Finance & Strategic Planning Officer. The procurement and management of hardware, software is managed by the Senior IT Developer and supporting services such as communication and information systems are also coordinated by the above directors.

We maintain an asset register, description and location or person to whom assigned.

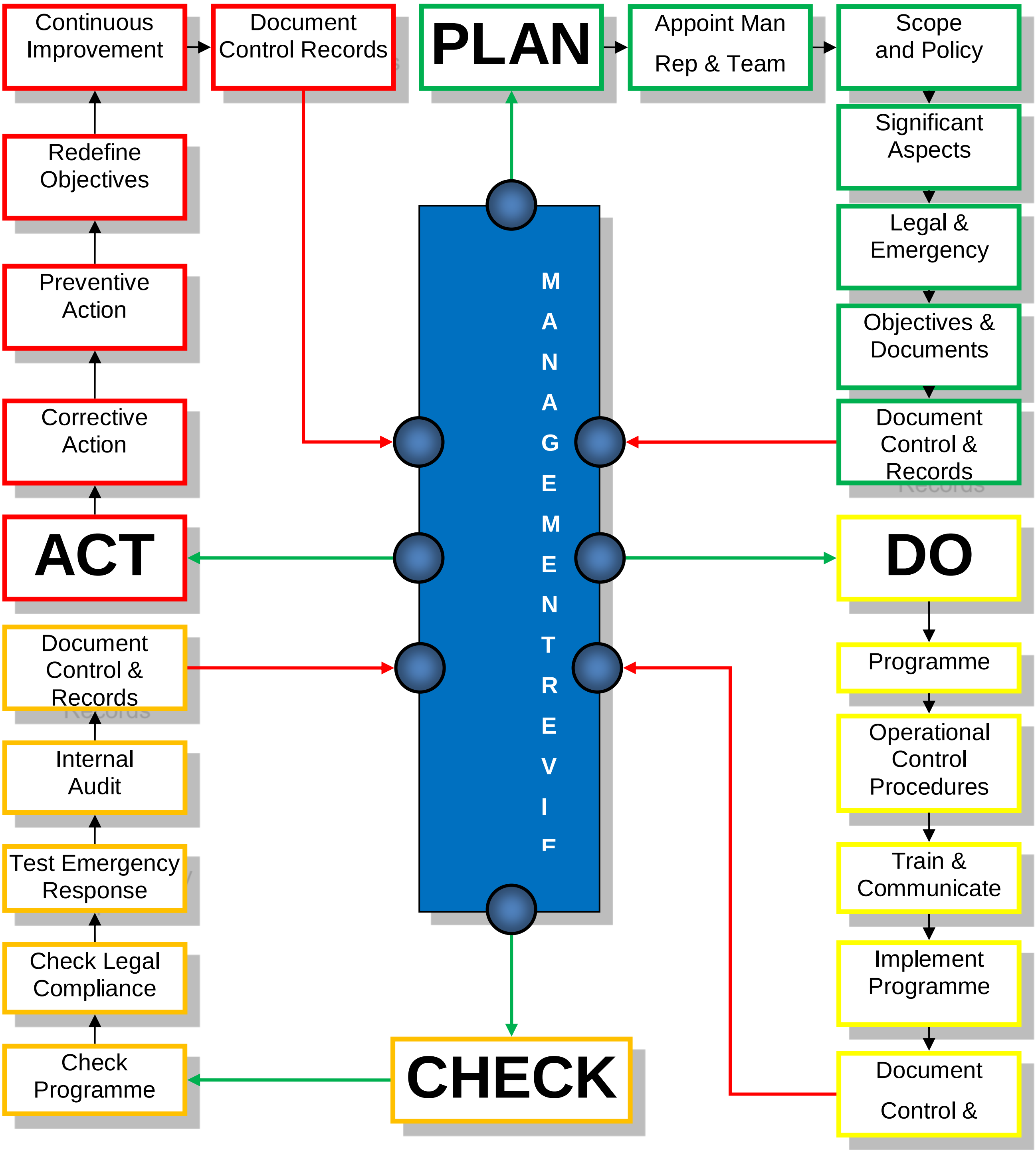
7.2.1 Implementation

Buildings, workspace and associated utilities requirements are regularly reviewed to ensure we make efficient use of office space. Both hardware and software is reviewed on an ongoing basis to ensure that staff are equipped with fit for purpose IT equipment and software.

IT systems are maintained and serviced internally by the Senior IT Developer.

7.3 Device and Media Controls

Procedures to for this area must govern the control of electronic media containing confidential information including: a) Disposition of the hardware / electronic media on which confidential data is stored, b) removal of confidential information from electronic media before it is re-used, c) Documentation of hardware / electronic media movement and any persons responsible for such movement e.g. to offsite backups transfers, d) Backup of confidential information before changes to host hardware, e.g. move.


Continuous Improvement
Document Control Records
PLAN
Appoint Man Rep & Team
Scope and Policy
Significant Aspects
Legal & Emergency
Objectives & Documents
Document Control & Records
Redefine Objectives
Preventive Action
Corrective Action
MANAGEMENT REVIE
ACT
DO
Document Control & Records
Programme
Internal Audit
Operational Control Procedures
Test Emergency Response
Train & Communicate
Check Legal Compliance
Implement Programme
Check Programme
CHECK
Document Control &

8 RISK ASSESSMENT METHODOLOGY

We have identified the following process as a means of conducting regular risk assessments relating to Information Security Issues.

Within each of these areas the risks (if any) are identified together with a rating as to the importance of the risk. The associated consequence or severity of the risk is also rated together with the probable likelihood of the risk occurring.

We use an Excel spreadsheet to collect and analyse the risks identified in the following assets / asset groups :

- Buildings, offices, secure rooms security
- Hardware – desktops. Laptops, removable media
- Software applications
- Infrastructure / servers
- Client information and data
- Paper records
- People and reputation
- Key contacts
- Critical third party suppliers
- Utilities

All typical / likely threats have been assessed based on their potential effects on Confidentiality, Integrity and Availability (CIA attributes) using a ratings scale of;

- Very Low - 1, Low – 2, Medium – 3, High 4 and Very high – 5 and expressed across key areas of Vulnerability, Probability and Impact

Following this analysis evaluations are drawn as to what the most appropriate action is. Key evaluation criteria use is 1 – Accept risk, 2 - Apply controls, 3 - Avoid risk, 4 – Transfer the risk.

8 .1 Risk Plan – Statement of Applicability

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.

This document is kept in our shared drive.

9 MEASUREMENT, ANALYSIS & IMPROVEMENT

9.1 Information Security Standards

In all **Systematics** services there are a specific set of quality measurements developed to be used to audit each service to enable a purchaser to be assured of the quality of delivery.

Service Level Agreements (SLA) are used to identify the areas of a contract that will be measured and monitored.

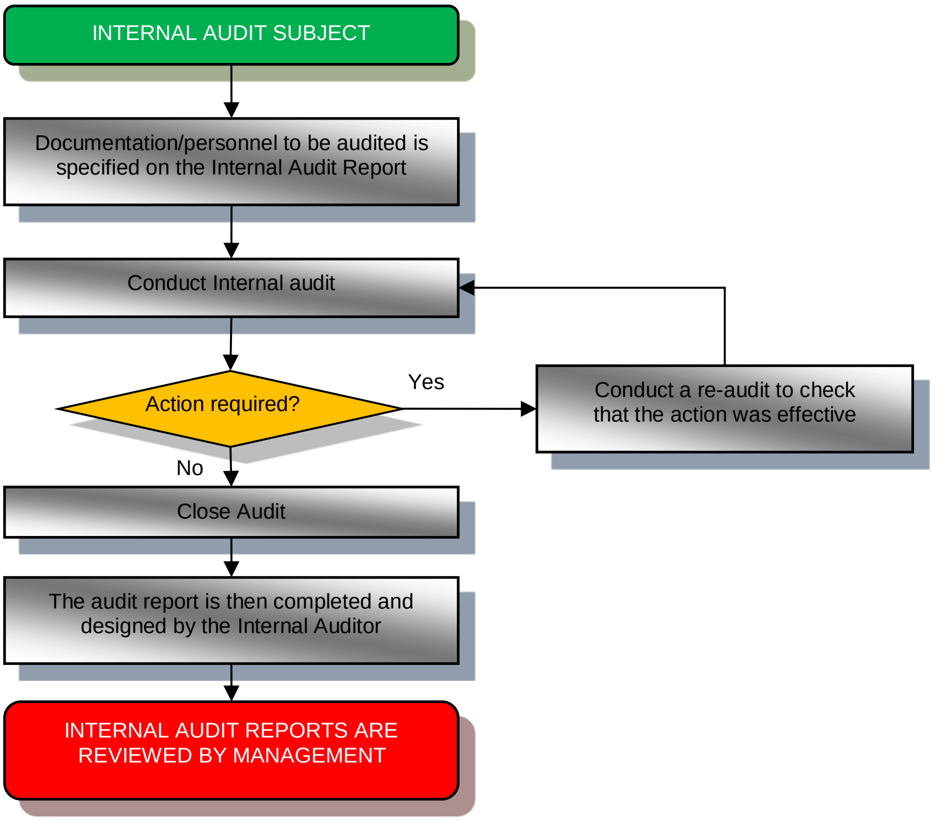
9.1.1 Implementation

We review our performance as part of a continuous review of Management Information. These reports help us to assess whether we are meeting our performance targets and provide us with month on month business performance benchmarking information. **Systematics** conducts annual audits on Information Security.

9.2 Internal ISMS Audits

The internal audit process is as follows:

9.2.1 Internal Audit Process Flowchart


INTERNAL AUDIT SUBJECT
Documentation/personnel to be audited is specified on the Internal Audit Report
Conduct Internal audit
Action required?
Yes
Conduct a re-audit to check that the action was effective
No
Close Audit
The audit report is then completed and designed by the Internal Auditor
INTERNAL AUDIT REPORTS ARE REVIEWED BY MANAGEMENT

9.3 Monitoring & Measurement of Processes

9.3.1 Implementation

Where the agreed requirements are not met, an action plan clearly detailing compliance will then be agreed with **Systematics** Chief Executive Officer with a timescale for compliance set at 6 months with the service commissioner or client.

9.4 Monitoring & Measurement of Service

Our approach determines what needs to be measured inclusive of security processes and controls, the methods by which we ensure valid results, the periods and persons involved in conducting this activity and the reporting frequency and the responsibility for analysing and evaluating the results.

We retain all documents and records involved in this process.

Systematics establishes at the outset of a new service contract the reporting demands within the Service Level Agreement. This process will be supported with the data reports compiled and will enable the review to monitor performance, effectiveness of delivery, contract compliance and potential service developments.

9.5 Analysis of Data

Incident logs are used to record any Information Security incidents or breaches giving cause for concern, and these are regularly assessed during the Management Review process to identify areas for improvement.

9.5.1 Implementation

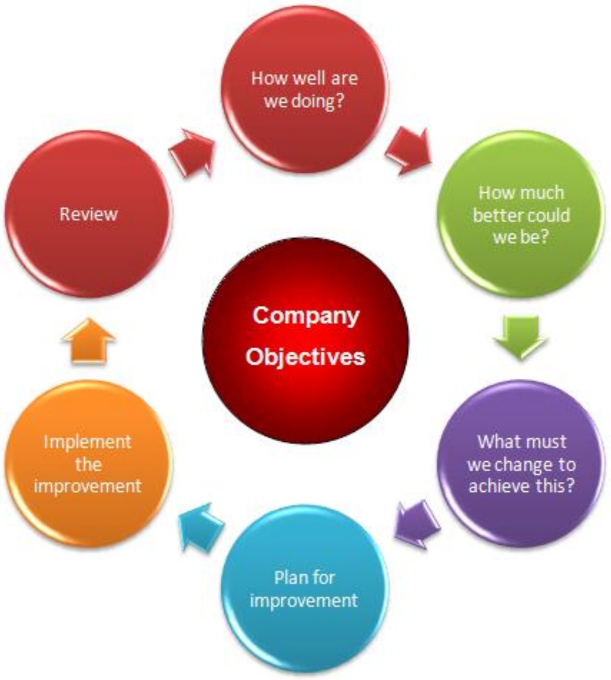
The data is collected by staff and submitted to the Information Security Manager for review.

9.6 Continual Improvement

The organisation will continually improve the effectiveness of the Information Security Management System through the use of the quality policy, quality objectives, audit results, analysis of data, corrective and preventive actions and management review.

9.6.1 Implementation

We review our performance as part of a continuous review of Management Information, service-user/customer feedback and comments. In particular we review our progress against our company information security objectives (business plan aims), with a view to seeing what we can improve and where. The chart below illustrates this process:


Company Objectives
How well are we doing?
How much better could we be?
What must we change to achieve this?
Plan for improvement
Implement the improvement
Review

9.7 Corrective Action and Improvement

Both these areas are reviewed within the agenda for the Management Review meetings and typically cover the action taken to control and correct any non-conformances noting any consequences of the action taken and themes which may be evident.

In terms of continual improvement, we also review the suitability, adequacy and effectiveness of our ISMS.

9.8 Complaints Policy

Systematics is committed to giving its clients the best possible service, involving them in the planning of their requirements, and giving them opportunities to air any complaints that they may have on the service we provide. To this end we have a complaints policy in place.

9.9 Preventative Action

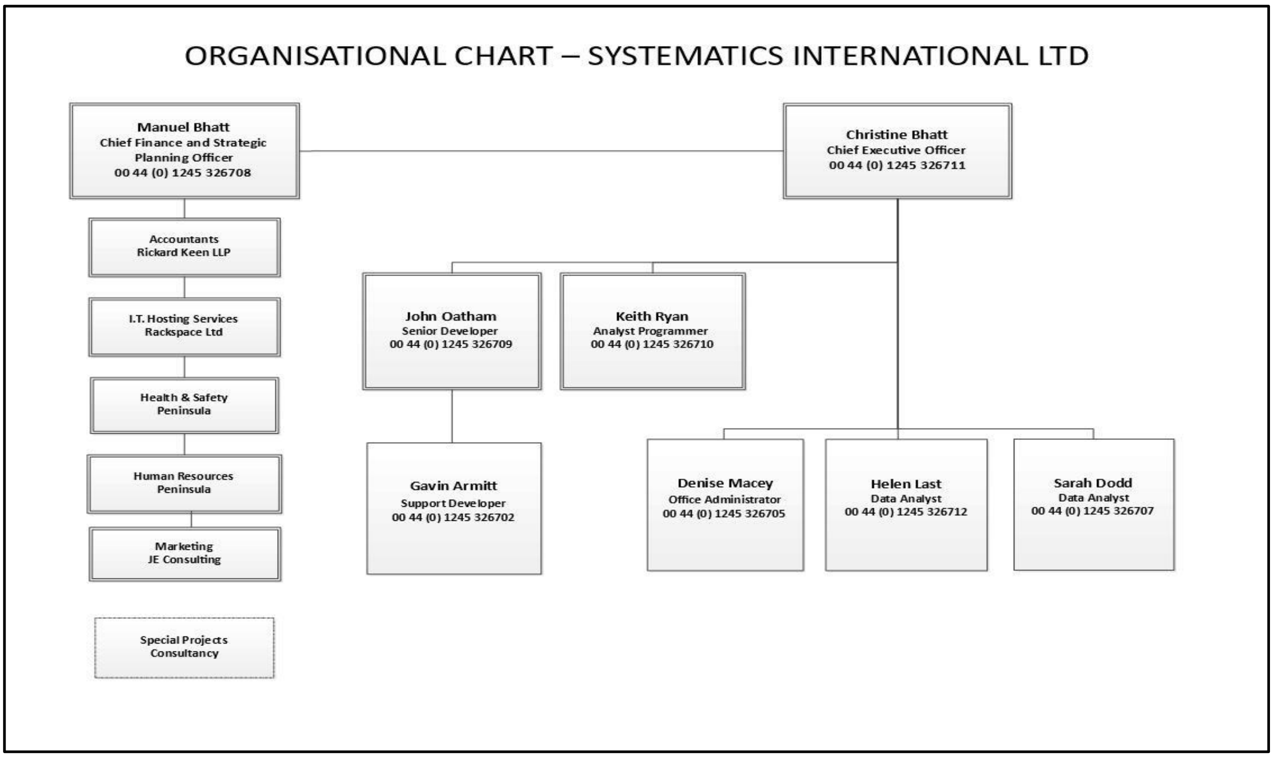
Systematics has various processes and procedures in place to ensure that preventative action against nonconformities can be introduced, documented and seen through till completion to address the initial problem.

The complex requirements nature of the clients we work with, demands that we have flexible but effective processes and procedures in place.

However, **Systematics** also uses internal risk assessments to continuously improve its service delivery, financial, HR and operational functions.

10 APPENDICES

10.1Appendix 1 – Organisation Chart



Appendix 2 – List of Controlled Documents

Ref No	Name	Version	Date	Associated Documents
F:\Statistics Team\Policies\ISO - Information Security	ISO 27001 International Standards	Second Edition 2013-10-01	01 Jun 2015	
F:\Statistics Team\Policies\ISO - Information Security	ISO – IEC 27002-2013 Code of Practice	Second Edition 2013-10-01	01 Jun 2015	
F:\Statistics Team\Policies\ISO - Information Security	ISO 27001-2013 Systematics ISMS Policy Document V4	V4	29 Mar 2017	
F:\Statistics Team\Policies\ISO - Information Security	ISO 27001-2013 Systematics_Risk Assessment V4	V4	29 Mar 2017	
F:\Statistics Team\Policies\ISO - Information Security	ISO 27001-2013 Systematics Statement of Applicability V4	V4	29 Mar 2017	
F:\Statistics Team\Policies\ISO - Information Security/Audit Forms	Internal Audit Annual Schedule 2016/17	V2	01 Jul 2016	
F:\Statistics Team\Policies\ISO - Information Security	Monthly Internal Audit Report	V1	01 Jun 2015	
F:\Statistics Team\Policies\ISO - Information Security	Management Review Notes	V2	28 Mar 2017	
F:\Statistics Team\Policies\ISO - Information Security	Interested Parties	V2	28 Mar 2017	
F:\Statistics Team\Policies\ISO - Information Security	Code of Conduct	V1	24 Jun 2013	
F:\Statistics Team\Policies\ISO - Information Security	Customer Care Policy	V1	7 Jul 2014	
F:\Statistics Team\Policies\ISO	Guide to Legislation relevant to Information Security	V1	01 Jun 2014	

- Information Security				
F:\Statistics Team\Policies\ISO - Information Security	Disaster Recovery test results 2016		17 Oct 2017	
F:\Statistics Team\Policies\ISO - Information Security	27001 Corrective and Preventative Action Log	V1	28 Mar 2017	
F:\Statistics Team\Policies\ISO - Information Security	Possible Internal and External Issues	V1	28 Mar 2017	
F:\Statistics Team\Policies\ISO - Information Security	Training Matrix – Systematics V1	V1	28 Mar 2017	
F:\Statistics Team\Policies\ISO - Information Security	Customer Complaint Form V1	V1	28 Mar 2017	
F:\Statistics Team\Policies\ISO - Information Security	Customer Complaint Summary V1	V1	28 Mar 2017	
F:\Statistics Team\Policies\ISO - Information Security	Systematics International Client Survey 2016 – 2017		10 Feb 2017	
F:\Statistics Team\Policies\ISO - Information Security	Survey Analysis 2016-2017		10 Feb 2017	
F:\Statistics Team\Policies\ISO - Information Security	Disaster Recovery test results 2017		17 Oct 2017	
F:\Statistics Team\Policies\ISO - Information Security	ISO 27001 BMS V1.0		16 Jan 2018	
F:\Statistics Team\Policies\ISO - Information Security	Interested Parties and Legal Compliance V1.0		16 Jan 2018	
F:\Statistics Team\Policies\ISO - Information Security	Possible Internal and External Issues V2		16 Jan 2018	

F:\Statistics Team\Policies\ISO - Information Security	Clear Desk & Screen Policy	V1	14 Jun 2018	