IMS1

Integrated Management System Manual

Pointer Ltd / PointerFire
JGE Security Systems Ltd

65 North Wallace Street
Glasgow
G4 0DT

The controlled master copy of this IMS Manual is held electronically in the Pointer Portal.
Any electronic or hard copies are uncontrolled.

Issue No :	**Version 3.2**
Issue Date :	**23rd May 2022**
Controlled By :	**Hugh Lawson**
Approved By :	**Alex Cassells (Managing Director) & Andy Torrance (H&S Champion)**
Standards :	**ISO 9001:2015, ISO 14001:2015, ISO 22301:2019, ISO 27001:2013, ISO 45001:2018**

Contents

Section 1 Integrated Management System 3
1.1 Update Log 3
1.2 Integrated Management System – Overview and Scope 4
1.3 Context, Company Profile and Scope of Operations 5
1.4 Interaction of Processes 5
1.5 Management of Documented Information and Data 7
1.6 Legal Compliance 8
Section 2 Leadership, Commitment and Planning 10
2.1 Company Policies and Objectives 10
2.2 Responsibilities 11
2.3 IMS Organisational Chart 16
2.4 Management Review 17
2.5 Risk Management 18
Section 3 Resource Management and Support 19
3.1 Management of Staff and Company Personnel 19
3.2 Management of Equipment and Premises 20
3.3 Management System Communication 21
Section 4 Operational Processes 22
4.1 Control of Enquiries & Sales 22
4.2 Control of Purchasing and Outsourced Services 23
4.3 Control of Operations 24
4.4 Management of Change, Variations and Design 24
Section 5 Monitoring, Evaluation and Improvement 26
5.1 Customer Satisfaction 26
5.2 Control of Nonconforming Outputs, Problems and Complaints 27
5.3 Management System Audits (Internal Audits) 28
5.4 Continual Improvement 29
Section 6 Environmental Management 30
6.1 Commitment to Environmental Protection 30
6.2 Environmental Assessment 31
6.3 Environmental Incident Prevention & Management 32
6.4 Environmental Procedures 33
Section 7 Health & Safety Management 34
7.1 Commitment to Health and Safety at Work 34
7.2 Health and Safety at Work – Guidance and Arrangements 35
7.3 Health and Safety Procedure 37
7.4 Accident, Incident and Near Miss Reporting 38
7.5 Hazard Identification and Risk Assessment 39
Section 8 Information Security Management 40
8.1 Commitment to Information Security Management 40
8.2 Information Security Arrangements 42
8.3 IT Equipment and Physical Security 44
8.4 Information Security Risk Management 46
8.5 Information Security Procedures and Policies 47
Section 9 Business Continuity Management 48
Appendix i Management System Registers 49
F-IMS20 - Document Register 49
F-IMS21 - Business Continuity Register 49
F-IMS22 - Interested Parties 49
F-IMS23 - Opportunities Risks Register 49
F-ENV2 - Waste Matrix 49
F-ENV4 - Environmental Aspects Register 49
ER14 - Hazard Risk Assessment Register 49
F-IMS25 - Information Assets Register 49
F-IMS26 - Statement of Applicability 49
Business Impact Analysis and Risk Assessment 49
Business Critical Function Analysis 49

SECTION 1 INTEGRATED MANAGEMENT SYSTEM

1.1 Update Log

This document issue number is as indicated on the front page and footer and any significant changes since issue are summarised below.

Section Changed	Date Changed	Description of Change
1.18	28/04/2017	Rewording for ISO 14001:2015
1.19	20/11/2017	Merging of Management Systems for Pointer and PointerFire
1.20	28/01/2018	Amendments for ISO 9001:2015 and ISO 14001:2015
1.21	23/02/2018	Added SP203-1 for PointerFire
1.22	14/03/2018	Added Fire Responsibilities for FSQS 101
1.23	27/02/2019	Review based on ISO 14001:2015 and PD6662:2017
1.24	06/05/2019	Roles & Responsibilities of H&S Advisor
1.25	19/02/2020	ISO 45001:2018 GAP Analysis and BAFE SP203-1 inclusion
1.26	04/03/2020	Life Cycle approach for ISO 14001:2015
1.27	1/02/2021	PointerFire Structure Changes
2.0	12/04/2021	Management Review Updates
3.0	08/07/2021	Whole document revised and approved by Management
3.1	29/04/2022	Review after external audits from NQA and Corrective Actions
3.2	23/06/2022	Further changes to section 1.4 and 1.6 to reflect ISO 22301 after Internal Audit
3.3	01/07/2022	Section 5.3 Internal Auditor requirements.

1.2 Integrated Management System – Overview and Scope

Overview

Integrated Management System (IMS) is made up of this IMS manual, Pointer Integrated Procedures (PIP) and other documents detailed below. The IMS also includes all controlled forms and registers as detailed on the document register. The IMS documentation is made available to all colleagues and any interested parties.

Integrated Management System (IMS)

IMS1 - IMS Manual
- **Section 1** - Integrated Management System
- **Section 2** - Leadership, Commitment and Planning
- **Section 3** - Resource Management and Support
- **Section 4** - Operational Processes
- **Section 5** - Monitoring, Evaluation and Improvement
- **Section 6** – Environmental Management
- **Section 7** – Health & Safety Management
- **Section 8** – Information Security Management
- **Section 9** – Business Continuity Management
- **Appendix i** - IMS Registers

Policies / Procedures / Registers
- Various Policies
- Policy Statements
- Register of Third Parties
- Registers of Legal Compliance
- Aspects Register
- Risk Registers
- Issues Register
- Company Handbook
- Document Register

Applicability and Scope of the Integrated Management System

This manual outlines the management system that has been designed to meet the requirements of **ISO 9001:2015 & ISO 14001:2015 & ISO 22301:2019 & ISO 27001:2013 & ISO 45001:2018 & SQS101 & FQS101 & BAFE SP203-1**

The Company has implemented this Integrated Management System (IMS) to reinforce its ability to consistently provide a service that meets customer and applicable regulatory requirements. The scope of this management system is represented by the procedures documented within this manual.

A formal Business Continuity Management System is also in place to ensure all aspects of business continuity are considered and effectively managed. BCMS is made up of this IMS Manual and the business continuity policy. This policy provides an overview of the various mechanisms in place for reviewing continuity, risk and the potential impact of disruptive incident.

Scope of ICO & Industry Registrations

Pointer Ltd (Glasgow)
- ISO 9001
- ISO 14001
- ISO 22301 (Working towards)
- ISO 27001
- ISO 45001
- NSI NACOSS and Fire Gold
- BAFE SP203-1

Pointer Ltd (England)
- ISO 9001
- ISO 14001
- ISO 22301 (Working towards)
- ISO 27001
- ISO 45001
- NSI NACOSS and Fire Gold
- BAFE SP203-1

Pointer Fire
- ISO 9001
- NSI Fire Gold
- BAFE SP203-1
- ISO 14001 (Leeds Only)
- ISO 45001 (Leeds Only)
- ISO 22301 (Working towards)

JGE Security Systems
- ISO 9001
- NSI NACOSS Gold

The scope of registration is as follows:

Design, Installation, Service, Maintenance and Monitoring of Fire and Electronic Security Systems.

Exclusions - the following requirements have been determined to not be applicable to the scope of our management system; **None.**

1.3 Context, Company Profile and Scope of Operations

Context of the organisation

Internal context (our vision, culture, strategic direction, organisational roles, operating procedures, resources) as well as external context (needs and expectations of interested parties, contractual obligations, legal, social, political factors in general as well those specific to our marketplace such as competition, technology and regulatory requirements) are relevant to the operation of this management system and achievement of company objectives.

These considerations are demonstrated by this IMS which includes a formal review and register of Third Parties and an Opportunities and Risks Register which includes **SWOT** (Strengths, Weaknesses, Opportunities and Threats) analysis and a formal review of relevant Internal and External factors (**PESTLE** - Political, Economic, Social, Technology, Legal, Environmental).

This IMS and associated records are formally reviewed at least annually during Management Review.

The organization's activities, functions, services, products, partnerships, supply chains, relationships with interested parties, and the potential impact related to a disruptive incident is documented across the IMS, listed & reviewed in our Register of Third Parties and following key BCMS documents;

- **Business Continuity Policy**
- **Business Continuity Register**
- **Business Continuity Risk Register**

Links between the business continuity policy and the organization's objectives and other policies, including its overall risk management strategy is outlined within the above three documents.

Company Details

Full Company Name: Pointer Limited	
Registration No: SC047359	
Registered Address:	65 North Wallace Street Glasgow G4 0DT
Trading Address:	As above
Website:	www.pointer.co.uk, www.pointerfire.com, www.johngrahamelectronics.co.uk
Main activities / products / services:	Design, Installation, Service, Maintenance and Monitoring of Fire and Electronic Security Systems. Access Control Systems, CCTV Systems, Fire Detection Systems, Intruder Alarm Systems, Integrated Security Systems, Perimeter Intrusion Detection Systems and Video Surveillance Systems
Mission Statement:	To build a robust, resilient, sustainable and successful business which can support our customers and colleagues through good times and bad.

Company Profile

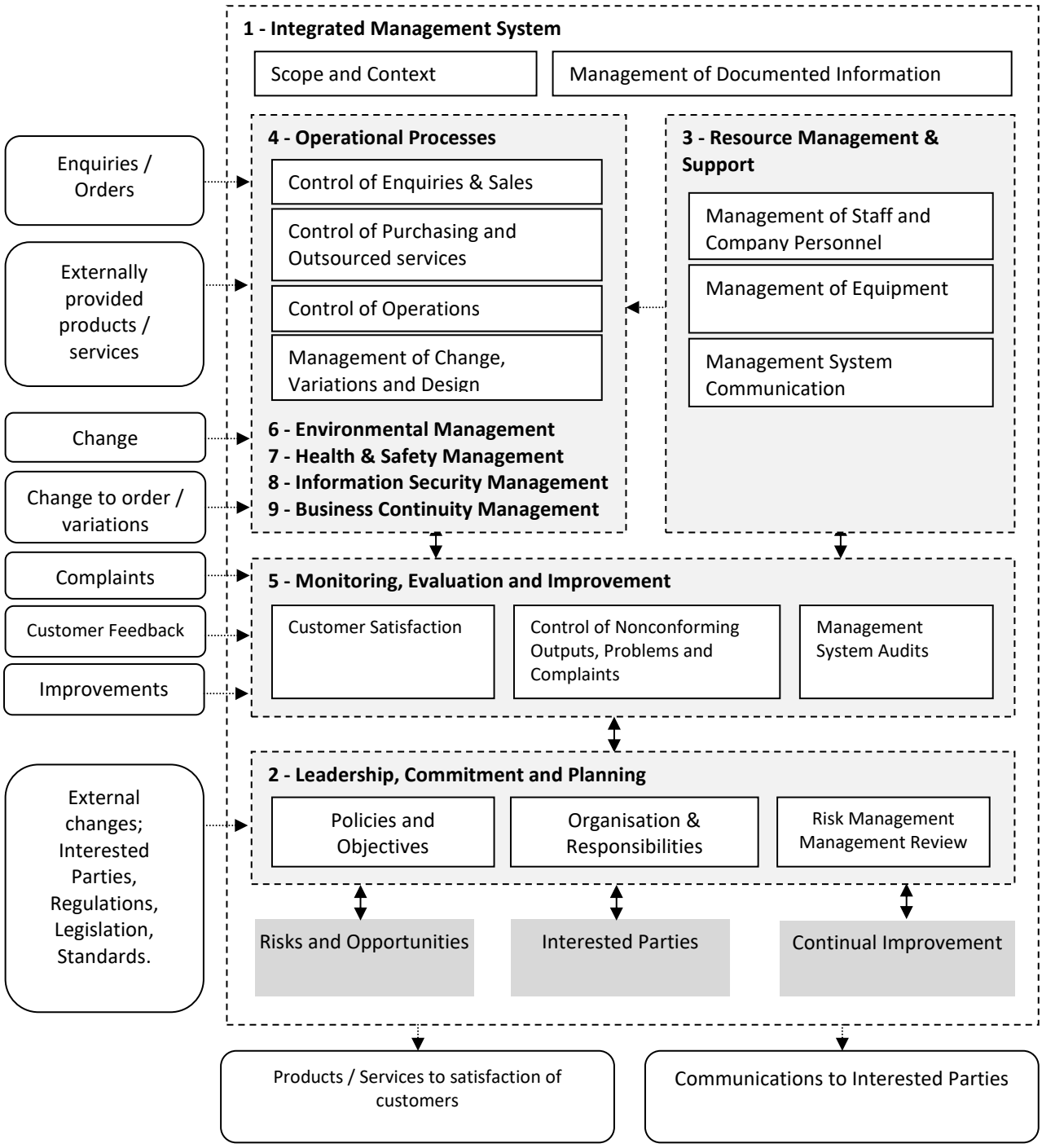
Please refer to our company websites for current profile information.

1.4 Interaction of Processes

Correlation of ISO clauses to this IMS

ISO Clause	Relevant section in this IMS
4 - Organisation and its context	**Section 1** - Integrated Management System
5 - Leadership	**Section 2** - Leadership, Commitment and Planning
6 - Planning	**Section 2** - Leadership, Commitment and Planning
7 - Support	**Section 3, 6, 7 & 8** - Resource Management and Support
8 - Operation	**Section 4, 6, 7 & 8** - Operational Processes
9 - Performance Evaluation	**Section 5** - Monitoring, Evaluation and Improvement
10 - Improvement	**Section 5** - Monitoring, Evaluation and Improvement

Overview of interaction of Key processes



1.5 Management of Documented Information and Data

Responsibility: Technical & Compliance Manager

1.5.1. Management of Integrated Management System (IMS) documentation
All key IMS documentation is controlled, and files are held electronically on the Pointer Portal and available to all colleagues. These are read only files and uncontrolled.
Master electronic copies of files are managed and updated by the person named above and key files such as this document are password protected / read-only to ensure only those authorised can update / amend.
All documentation will be legible, readable and backed-up.

1.5.2. Management of Changes and Review
Significant changes to the IMS are agreed by person in charge of the area where the change will occur (person named in ***'Responsibility'*** field). Changes to document templates are logged on the relevant document.
The IMS will be formally reviewed at least annually during the management review to ensure it accurately reflects good practice within the organisation and that all key processes and procedures are appropriately documented and continuing to meet the requirements of the standards.

IMS Document Approval, Removal and Review
Any new procedures, policies, registers or other key documents should be approved by person named above prior to use.
Old versions are archived / removed from use.

1.5.3. Management of Company Forms, Key Files and Other Documentation
Key forms will be numbered, issue controlled and saved in the forms folder with details logged on the **Document Register** to ensure all colleagues are aware of and have access to key forms through the Pointer Portal. Many forms are now electronic and are controlled by the person responsible named above.

Data Protection Classification
Where possible company-controlled documents should be labelled with data protection classification and any documents that include sensitive or confidential information will be marked '***Top Secret'*** in the document footer and stored securely.
Documents for business use will be marked ***'Secret'*** and public documents marked ***'Public'***.
Data Protection - all colleagues will be aware of data protection regulations and data protection procedures / policies.

Key Standards / Guidelines / Legislation / Registers
Key standards, legislation and guidelines are detailed in section **1.6. Legal Compliance** and our Legal Registers and other key documents will be detailed in the Document Register.

Key Company Records - key records including paperwork supplied by 3rd parties will be listed in the Document Register to ensure all colleagues are aware of what records are required to be retained, where to be stored or filed, for how long and who is responsible.
Paper records will be collated, filed, and kept in a suitable, secure environment.
Documents of external origin will be identified and controlled.
Key documents required as evidence of conformity should be protected from unintended change (e.g. PDF format).

1.5.4. Data Backup - Management of Electronic Information
Computer information will be backed-up and IT equipment and Information Security will be checked and maintained. **PIP 88 – Information Backups**
Identification and review of key information held and managed will be completed on an ongoing basis.
Information assets identified are logged on our **Information Assets Register**.

1.5.5. Data Destruction
Cross shredding facilities are provided in our offices to dispose of all personal, confidential, secret and top secret information.
Information stored on computer / server hard disks will be destroyed on site with certificates of destruction stored.

1.5.7. More Information
Data Retention times are recorded on our Document Register. A requirement of National Security Inspectorate (NSI) is that week keep customer records for the life of the contract plus 2 years. BAFE Fire System certificates are required for 12 years, with maintenance certificates required for 7 years.

1.6 Legal Compliance

Responsibility: Technical & Compliance Manager

Consideration has been given to assessing of legal requirements, guidelines, industry codes of practice and standards that are applicable and **KEY** standards, guidelines and legislation are detailed below. Detailed requirements are contained in our legal registers.
This includes industry, pertinent environmental, H&S and other legislation deemed applicable to our business.
Legal compliance will be formally evaluated during management review and internal audits through review of our Legal Registers.

Relevant Standards / Industry Codes of Practice / Guidelines

Description	Compliance
ISO 9001:2015 Quality Management	Integrated Management System
ISO 14001:2015 Environmental Management	Integrated Management System
ISO 22301:2019 Business Continuity Management	Integrated Management System
ISO 27001:2013:Information Security Management	Integrated Management System
ISO 45001:2018:Occupational Health & Safety Management	Integrated Management System

Quality / Industry Legislation

Ref.	Description	Compliance
C1	The Equality Act	**Register of Legal Compliance for Quality**
C2	Companies Act Corporation tax Act	Company name, registration number and registered address on paperwork and other arrangements in place for compliance
C3	The Employers Liability (Compulsory Insurance) Regulations)	Insurance in place
C4	Sale of goods Act Consumer rights act	Compliance with regards any sales
C5	The Working Time Regulations	Where required working time regulations opt-out form to be completed
C6	Data Protection Legislation (GDPR)	Information assets identified. **Privacy policy** and **Data Protection policy**.
C7	Privacy and Electronic Communications Regulations The Telecommunications (lawful Business Practice and Interception of Communications) Regulations Computer Misuse Act Electronic Communications Act	Various procedures / policies in place covering acceptable use of IT equipment.

Pertinent Legislation - Equipment

Ref.	Description	Compliance
EQ1	Lifting Operations and Lifting Equipment Regulations (LOLER). The Provision and Use of Work Equipment Regulations (PUWER).	Equipment Checklist & schedule of maintenance
EQ3	Electricity at work regulations	Equipment Checklist, PAT testing, Fixed wiring inspection

Pertinent Health & Safety Legislation

Ref.	Description	Compliance
HS1	Health & Safety at work act. The Management of Health and Safety at Work Regulations. The Workplace (Health, Safety and Welfare) Regulations Safety, Health and Welfare at Work (Signs) Regulations.	HSE poster on wall. Signage in place. Ongoing inspections, risk assessments & monitoring
HS2	Control of noise at work regulations Smoke-free (premises and equipment) regs	Noise monitored and no smoking permitted on the premises
HS3	The Health and Safety (Display Screen Equipment) Regulations	DSE assessments completed annually.
HS4	Lone Worker Legislation	Risk assessment if relevant
HS5	Control of Substances Hazardous to Health Regulations (COSHH)	COSHH Register / COSHH Folder / Pointer Portal
HS6	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR) First Aid (Emergency Situations) Health and Safety (First Aid) Regulations	Accident reporting procedure, accident book. First Aid & Welfare Arrangements checked monthly as part of walk around checklist Colleagues with First Aid Training recorded on training matrix and each vehicle has a First Aid kit

Ref.	Description	Compliance
HS7	Manual Handling Operations Regulations	If relevant - Manual Handling Training for all colleagues & logged on training matrix
HS8	Personal Protective Equipment (PPE) at Work Regulations	PPE available to all colleagues as per any control measures identified during Risk Assessments. PPE issue recorded.
HS9	The Work at Height Regulations	Risk assessment if relevant
HS10	Fire Safety Regulations Regulatory reform (Fire Safety) order (Scotland and England)	Fire risk assessments completed and reviewed annually.

Pertinent Environmental Legislation

Ref.	Description	Compliance
E1	Environmental Protection Act Environmental Protection (Duty of Care) Regulations The Landfill (Scotland) Regs	Spillage and Environmental Protection Procedure
E2	Waste Electrical & Electronic Equipment (WEEE) Regs	All waste electrical and electronic equipment is disposed of using licensed contractors
E3	Waste (England and Wales) Regs Waste (Scotland) Regs	Waste Procedure Requirement to segregate waste streams and put waste in correct bins when provided
E4	The Controlled Waste Regulations The Hazardous Waste Directive Special Waste (Scotland) Regs	Waste Procedure Special waste cannot be disposed of in general waste
E5	Environmental Permitting (England and Wales) Regs The Environmental Protection (Duty of Care) (Scotland) Regs	Waste Procedure Duty of Care for waste even after it leaves site. Waste Transfer Notes are required for all waste transfers
E6	The Batteries and Accumulators (Placing on the Market) (Amendment) Regs	Disposal of security system standby batteries and UPS batteries.
E7	The Waste Batteries and Accumulators (Amendment) Regs	Waste Procedure - Batteries deemed as hazardous waste and cannot be disposed of in general waste
E8	Packaging (Essential Requirements) Regs Producer Responsibility Obligations (Packaging waste) Regs	Review requirements to establish if obligated under these regulations
E9	Control of Pollution (Oil Storage) Regs	Storage of oils and chemicals procedure
E10	Fluorinated Greenhouse Gas Regs Ozone Depleting Substances Regs	Equipment Checklist & schedule of maintenance

Pertinent Information Security Legislation

Ref.	Description	Compliance
IT1	The Telecommunications (lawful Business Practice and Interception of Communications) Regulations	Allows businesses to intercept communication on their own telecommunications network without consent, for certain specified purposes - any interception of communication will be documented and reviewed.
IT2	Computer Misuse Act	No one within the company is permitted to attempt to hack into any other computer systems
IT3	Copyright, Designs and Patents Act (CDPA)	Checks to ensure we do not use any copyrighted materials without permission and software installation controlled.
IT4	Companies Act (contains a number of provisions concerning records and communications)	Various implications on retention of records & availability for inspection, duties to take precautions against falsification, company communications provisions etc...
IT5	Forgery and Counterfeiting Act Fraud Act Anti-terrorism Crime and Security Act Proceeds of Crime Act	Currently no online transactions and checks on any cash transactions.
IT6	Privacy and Electronic Communications Regulations (PECR)	Marketing by electronic means and web site in compliance - no spamming and privacy and cookies policy in place.

SECTION 2 LEADERSHIP, COMMITMENT AND PLANNING

2.1 Company Policies and Objectives

Responsibility: Managing Director

Policies

Various Policies have been prepared as separate documents so that they can be more readily shared and issued to interested parties and policies which can be openly shared out with the organisation are labelled [**Public**]. Any other policies can only be shared with approval from the Technical & Compliance Manager.

Policies are signed / approved by top management and located in the Pointer Portal to ensure they are available to all colleagues.

The following Policies are also on company noticeboards -

- Integrated Management System Policy Statements
- Summary of Insurance Information

Policies are applicable to all colleagues, unless specific applicability stated within the relevant policy, and must be followed. Training and induction will be completed to ensure all colleagues are aware of and understand all relevant company policies. Awareness of policies should be logged using training records, toolbox talk attendance or training attendance forms.

It is the responsibility of all colleagues to follow and comply with company policies and failure to do so may lead to disciplinary action.

Company Objectives

Objectives are set and reviewed at least annually during Management Review. These objectives are measurable and based around enhancement and improvement of company operations and the provision of services.

A full summary of objectives including what is to be done, resources required, responsibility, timescales for review are detailed in the Management Review or on our Directors Strategy / Policy Statement for each Management System.

Consultation and Participation of Workers

We have appointed Health & Safety Champions to assist us in the Participation and Consultation of the workforce. This role is new and is continuing to develop. Roles for the champion can be found in Section 2.2 of this Integrated Management System.

PIP 28 - Communication and Consultation Procedure details other ways we consult with employees and encourage participation in our management systems.
These include:

- Business Roadshows conducted by the Managing Director
- Online Surveys (Satisfaction and selection of resources)
- Company Wide Focus such as wellness, cyber security
- Asking for volunteers to complete training and roles (such as Mental Health 1st Aid)
- Intent Based Leadership principles on the involvement of all staff to get better.

2.2 Responsibilities

Responsibility: Managing Director

The Managing Director has overall responsibility and is committed to the development and continual improvement of the management systems. Responsibility for key functions is delegated as detailed below and on the following Organisational Chart (**2.3 Organisational Chart**).

Integrated Management System (IMS) Responsibilities
The IMS Lead (Technical & Compliance Manager) is responsible for ensuring that the IMS is consistently implemented. On an annual basis the system should be reviewed during Management Review. The review will be based upon the reports of the internal audits and any other pertinent information relating to operational activities, to ensure that it reflects the current requirements of clients, the company and other interested parties.

The **IMS Lead** shall be responsible for:

- Ensuring the IMS documentation is maintained, effective and correct;
- Reporting on the performance of the IMS and determining where improvements are needed – these will be reported to top management;
- Promoting a customer focussed approach throughout the organisation;
- Ensuring operational processes are being carried out as planned and meeting required outputs;
- Providing guidance on the management system to colleagues;
- Ensuring any changes to the management system are carried out in a planned and responsible way while retaining the integrity of the IMS;
- Monitoring and ensuring that meeting the requirements of the ISO standards and other requirements.

Management System **Internal Auditor** shall be responsible for;

- Completion of audits as per audit schedule
- Reporting of any issues

An **Impartiality Auditor** will audit the works that the **Internal Auditor** is responsible for.

The **Data Protection Officer / Representative** (HR Manager) shall be responsible for:

- Responsibility for compliance with data protection legislation
- Ongoing monitoring of use, accuracy and retention of personal data
- Point of contact internally for any concerns relating to management of personal data or questions
- Provision of guidance / training on management of personal data to other colleagues
- Point of contact externally for any data requests
- Reporting minor data breaches internally or significant breaches to ICO / Data subjects

The **Business Continuity Lead** (Technical & Compliance Manager) shall be responsible for:

- Ensuring Business Continuity Plans and Policy are kept up to date.
- Ensuring Business Continuity objectives are set and communicated.
- Ensuring continuity arrangements are effective and tested.
- Subscribing to relevant threat advisory systems as required.
- Monitoring and reviewing any issues, risks, legislation or other changes with outsourced services or interested parties that could impact on business continuity.
- Monitoring the effectiveness of the business continuity management system, ensuring it meets the requirements of the ISO 22301 standard, and reporting on the performance to top management.

Director (Responsible for Health & Safety)

The Director has overall responsibility for all activities at Pointer Ltd. Included in the management of the business are the duties associated with the establishment and maintenance of the Integrated Management System. These include:

- Appoint competent personnel to undertake manage all management systems;
- Commit to review of training needs and undertaking activities that give colleagues the necessary attitude, knowledge and skills to carry out their tasks conscientiously and safely.
- Ensuring that this Management System confirms to the requirements of the various ISOs;
- determining the criteria for customer satisfaction measurement
- overall responsibility for security screening of employees;

- the identification and acquisition of equipment, fixtures, production resources and skills that may be needed to achieve the quality policy and business objectives.
- Ensuring that worker consultation and participation is included in this management system;
- Legally responsible for Occupational Health & Safety for staff and contractors working for Pointer.
- Provide a commitment to the continual improvement of environmental performance and to pollution prevention by reducing fuel consumed, reduction in waste by reusing, reducing and recycling materials and reducing carbon footprint.

Managing Director

The MD is responsible for implementing relevant Integrated Management Procedures which include:

- Participate in the establishment of management systems and their smooth running.
- Appoint competent personnel to co-ordinate the smooth running of all management systems and assist as required.
- Defining roles, allocating responsibilities and accountabilities and delegating authorities to facilitate effective management.
- Ensuring the availability of resources essential to establish, implement, maintain and improve the Integrated Management System;.
- System in place to measure staff competence and provision of adequate training and awareness to staff.
- Considering and acting upon (where appropriate) data generated from the measurement of processes with the view of effecting continual improvement of this Management System.
- Participate and lead Management Review Meetings, ensuring minutes recorded and actions are completed in a timely manner.
- Act upon non-conformances, employee suggestions, audit results and management reviews to continually improve our management systems.
- Consider Risks and Opportunities which affect the management systems along with the needs of colleagues and interested parties.
- Commitment to get better at what we do.
- Ensuring that this Management System confirms to the requirements of various ISOs;
- Measurement and monitoring of customer satisfaction;
- Effective monitoring of procedures including planned maintenance, corrective maintenance, and False Alarm Management;
- Appointment of a False Alarm Systems Performance Executive;
- Effective liaison with the emergency services and their policies;
- Identification and acquisition of equipment, fixtures, production resources and skills that may be needed to achieve the quality policy and business objectives.
- Engage with employees and contractors to ensure safe working practises for their health and safety;
- Participate in the programmes to reduce work related accidents and injury to staff and contractors;
- Provide PPE and plant to staff identified through Risk Assessment of activities.
- Ensure the safety and integrity of plant and equipment used by staff ensuring correct level of inspections and audits are carried out.
- Provide a commitment to the continual improvement of environmental performance and to pollution prevention by reducing fuel consumed, reduction in waste by reusing, reducing and recycling materials.
- Lead the Business Continuity Team to ensure minimum disruption to clients and services.

Competent Health & Safety Advice

Additional advice can be given by a Project Manager who has completed a Masters in Science in Risk and Safety Management (Grad IOSH). Duties and capabilities include:

- ensure continued membership of Grad IOSH and ensure all CPD is completed in order to refresh their H&S competence.
- Provide assistance when required by Technical and Compliance Manager, Managing Director, Directors. This may involve assisting with any investigations into incidents or accidents, liaising with third parties, involvement in the creation of Risk Assessments or Safe Systems of Work where required.
- Identify any actions as a result of new legislation, regulations, audit findings, codes of practice to improve our systems and performance of objectives.

Competent Environmental Advice

Our internal expertise includes –

- Technical & Compliance Manager –(NEBOSH General, H&S & Environmental Internal Auditor Training, Over 10 years of working withing ISO 14001).
- Grad ISOH - Our internal project manager with Masters in Science

- We also have an external consultancy we use for training / internal verification who is BSC in H&S Management, Chartered IOSH and a member of International Institute of Risk and Safety Management.
- We have subscription to Environmental Legislation Newsletters which includes UK Environmental Legislation Updates.
- We can also use SEPA and EA websites for legislation updates.

Security Governance Team (Business Continuity Management Team)

The Information Security team oversee the Information Security Management function and business continuity arrangements, providing line management, leadership and strategic direction for the function and liaising closely with other managers. The purpose of the Information Security Management function, in turn, is to bring the organization's information security risks under explicit management control through the Information Security Management System.
Key responsibilities

- Routine line management and leadership of staff within the Information Security Management function
- Liaison with and offers strategic direction to related governance functions (such as Physical Security/Facilities, Risk Management, IT, HR, Legal and Compliance) plus senior and middle managers throughout the Organisation as necessary, on information security matters such as routine security activities plus emerging security risks and control technologies
- Leads the design, implementation, operation and maintenance of the Information Security Management System
- Forms a "centre of excellence" for information security management, for example offering internal management consultancy advice and practical assistance on information security risk and control matters throughout the organization and promoting the commercial advantages of managing information security risks more efficiently and effectively
- Leads the design and operation of related compliance monitoring and improvement activities to ensure compliance both with internal security policies etc. and applicable laws and regulations
- Leads or commissions suitable information security awareness, training and educational activities
- Leads or commissions information security risk assessments and controls selection activities
- Leads or commissions activities relating to contingency planning, business continuity management and IT disaster recovery in conjunction with relevant functions and third parties

Health & Safety Champions

We ask for volunteers from the workforce to become Health & Safety Champions to represent the workforce in the development and improvement of the Management System and the Health & Safety of the Workforce. Champions should not be in a management roll; however, members of management are welcome to contribute in the same way if requested.

1. H&S Champions work closely with the Compliance Manager and can have time allocated to complete any duties required during their normal working hours.
2. H&S Champions will meet at least once a year to discuss findings / feedback and recommendations. This could be through conference call, video conferencing.
3. H&S Champion(s) can attend Management Review Meetings and provide input into the meeting. A set of minutes is also sent to the H&S Champion.
4. H&S Champion name for that office location to be included on the H&S Poster for staff to see.
5. The role of the H&S Champions will continue to develop as we review our systems and get feedback from the Champions.

Examples of Functions that H&S Champions can get involved with

- Reviewing / Improving our Risk Assessments and Method Statements.
- Reviewing / Improving our Processes and Procedures.
- Reviewing / Improving our key documents.
- Assist with consultation and communication of our systems throughout the company.
- Be a point of contact for colleagues relating to H&S matters.
- Provide suggestions on how we get better from experience and interactions with colleagues.
- Participate in our Management Review Meetings.
- Participate in carrying out premises / on site safety inspections.
- Incident Investigations
- Suggest ways we can communicate our systems / performance more effectively.
- Help us develop the role of H&S Champion.

A champion may not do all of the above but can get involved in areas where they identify. If requested, additional training can be arranged to help provide competence in new areas.

Nominated Designers

The Technical & Compliance Manager / General Managers and the Operations Director shall be deemed to fulfil the role of Nominated Designer under the NSI scheme. Duties and capabilities include:-

- To be the resource for when questions or queries arise from Designers.
- To be conversant with and update company activities in respect of new technologies, regulatory standards, EU
- Directives etc. that are relevant to the design process.
- To be conversant with the installation requirements such that system design specifications are professionally compiled and finalised in a manner which gives clear and unambiguous information to the engineering department.
- Controlling and monitoring all calibrated test equipment including plant and vehicles.

Surveyors/Designers/Account Managers

Some of the duties of Nominated Designer will be carried out by Designers. Where new technologies, requirements, standards require consultation or approval, the Nominated Designer will be required.

- To be the focal point for the matters of the design of installation.
- To ensure the content of quotations and system specifications are compatible with the requirements of the appropriate Technical Standards and NSI Codes of Practice.
- To sign off designs on behalf of the company.
- To be a Process Owner of the business process for converting enquiries into sales.
- To be conversant with and update company activities in respect of new technologies, regulatory standards, EU Directives etc that are relevant to the design process.
- To be conversant with the installation requirements such that system design specifications are professionally compiled and finalised in a manner which gives clear and unambiguous information to the installing engineer.

System Performance Executive (SPE)

The General Manager's / Branch Managers acting as SPE shall be responsible for all matters dealing with False Alarms, having the authority to achieve the following objectives: -

- Liaising with all staff to ensure effective monitoring of surveying and installations so that:-
    - Specifications meet the security requirements of company policies
    - Specifications do not call for systems which are likely to generate abnormally high false alarm rates.
    - Standards and Codes of Practice are being maintained during installation.
    - Customer documentation standards are being maintained during installations.
- Training standards for customers are being maintained.
    - The effective monitoring of preventive maintenance procedures.
    - The effective monitoring of demands for corrective maintenance.
    - The effective monitoring of faulty equipment records returned from installations.
    - The effective monitoring of the company's False Alarm Policy: -
        - Collection, reporting and analysis of false alarm statistics and their cause and resolution.
        - Identification and treatment of rogue systems.
        - Identification of troublesome equipment and practice.
- Effective liaison with the Police Forces / Fire Brigade and their policies.
- The effective monitoring of evaluation trials on new equipment with reference to false alarms.
- Adherence to the BS 5839, BS 8243 and BS 8473 for the Management of False Alarms.

All Colleagues (One Standard)

All applicants must adhere to the following if successfully employed by Pointer Limited: -

Health & Safety

- Look after yourself whilst at work.
- Carrying out your work so that it does not present a risk to others.
- Use all work items provided by Pointer Ltd / PointerFire / JGE Security correctly and in accordance with the training and information you have been given.
- Follow Pointer Ltd / PointerFire / JGE Security health and safety rules, risk assessments and emergency procedures etc. put in place.
- Use personal protective equipment provided and report and defects immediately for replacement.
- Report back to your supervisor / manager anything you consider a risk to your health and safety, or that of other people, so that remedial action can be taken.
- Not intentionally damage or misuse anything Pointer Ltd / PointerFire / JGE Security has provided for the health and safety of colleagues, contractors, and other people, such as visitors or members of the public.

Environmental

- Work with Pointer Ltd / PointerFire / JGE Security to reduce the amount of pollution, particularly CO2 emissions, caused by inefficient energy consumption.
- Work with materials and equipment responsibly to reduce the amount of waste of materials.
- Dispose of waste in the correct manner determined by our policies and legislation.

Quality

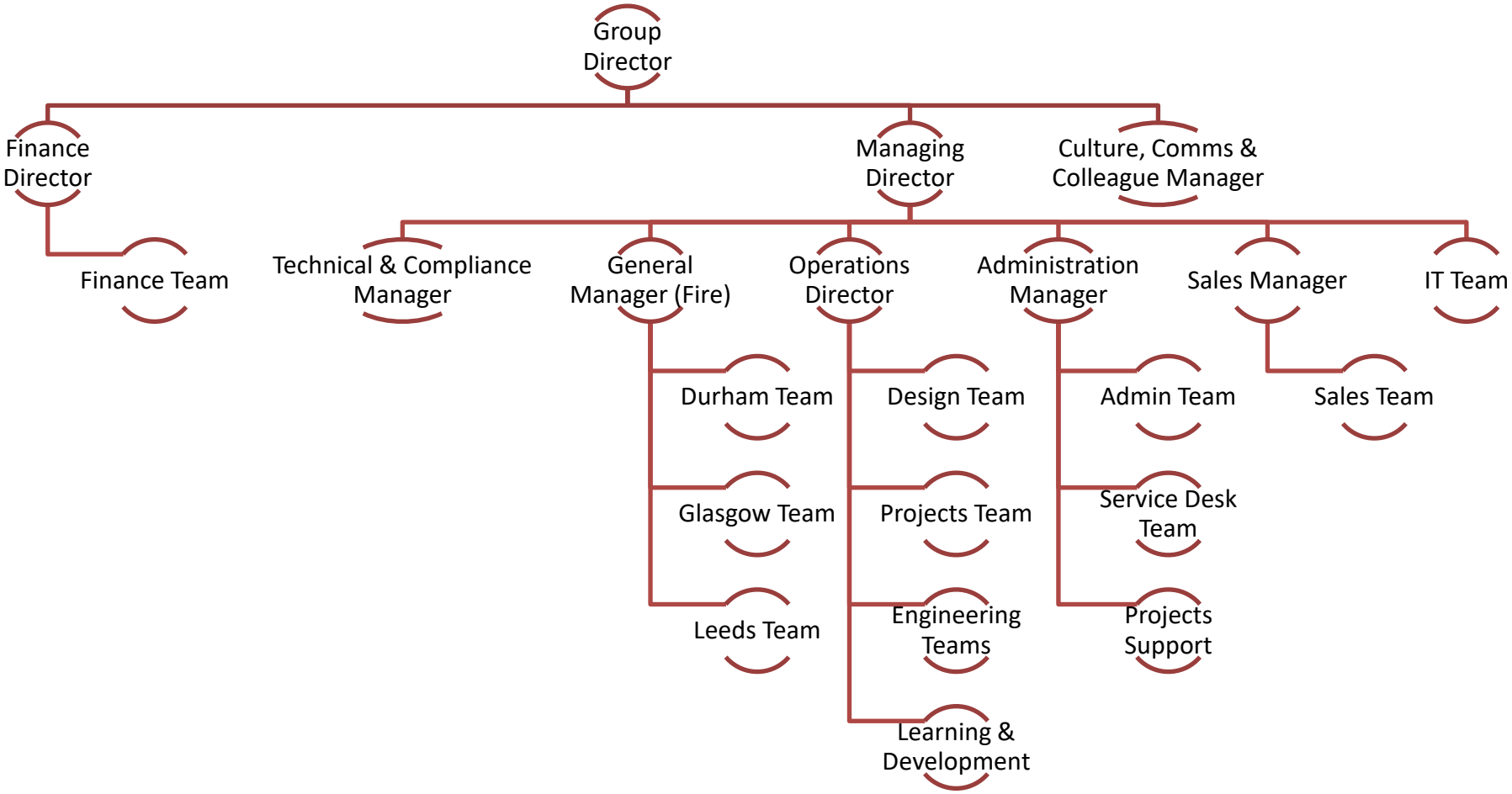
- Deliver excellent Customer Service at all times
- Present a professional image through high standards of personal appearance including upkeep of work wear and equipment provided
- Report back to supervisor / manager any improvements that can be made to our Quality systems and customer service.

Information Security

- All colleagues have a duty to safeguard assets, including locations, hardware, software, systems or information, in their care and to report any suspected breach in security without delay
- Colleagues attending customer locations must ensure the security of the Organisation's data and access their systems by taking particular care of laptops and/or similar computers they have in their possession, together with any information on paper or other media.
- Follow company policies such as acceptable use, Email and Internet, Information Technology Assets.

2.3 IMS Organisational Chart

Responsibility: Technical & Compliance Manager



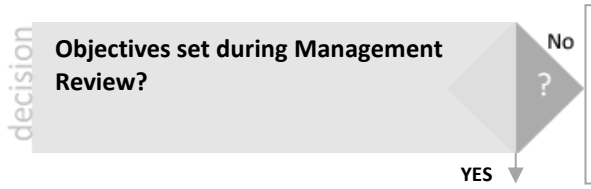
2.4 Management Review

Responsibility: Managing Director

2.4.1. Schedule Management Review
Management Review to be completed and documented at least annually or at planned intervals to review the management system and ensure its continuing suitability, adequacy, effectiveness and alignment with the strategic direction of the organisation. Date for next management review can be set during management review.

2.4.2. Complete Management Review
Management review should cover all items on the Management Review Agenda with input from relevant management systems.

Company Objectives
Any previously set objectives should be reviewed and current objectives documented.
Objectives should be relevant to operations and consistent with company policies, the management system and overall objectives of the organisation. The objectives should be measurable and details of how they are to be measured and success evaluated documented.



Complete **Company objectives** form to ensure measurable objectives have been set and clear strategy for monitoring achievement of objectives as well as for communicating objectives.

2.4.3. Document Agreed Actions
Action points and discussions documented within **Management Review Minutes.**
Actions will be dealt with as per **4.4 Management of Change** with relevant details added to the **Issues Register** (detail person responsible for action close out).
Any additional strategy or actions required for achieving and monitoring of objectives should also be prepared.

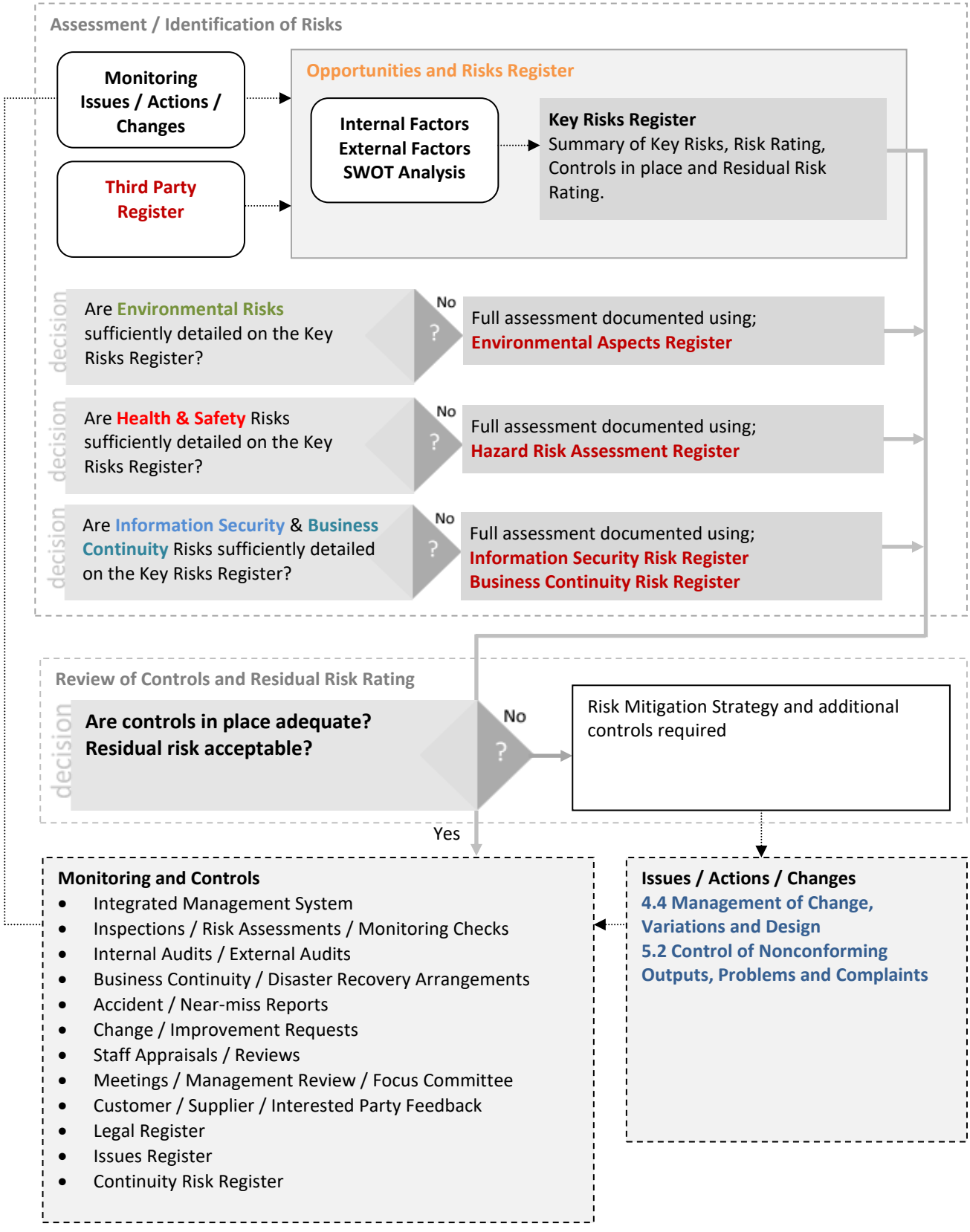
2.4.4. Communicate Management Review
Approved Management Review Minutes should be filed in IMS folder to ensure all interested parties have access and / or copy of the completed review / objectives shared on the Pointer Portal or the company newsletter – Pointer Patter.

Summary of key points or copy of management review distributed / meeting arranged to ensure colleagues are aware of key elements (particularly objectives).
Any other interested parties who require update to be contacted.

2.5 Risk Management

Responsibility: Managing Director

Overview of Risk Management, Controls and Monitoring.



SECTION 3 RESOURCE MANAGEMENT AND SUPPORT

3.1 Management of Staff and Company Personnel

Responsibility: HR Manager

3.1.1 Recruitment / Pre-Employment Checks

Job description prepared and approved and advertising approach agreed. Applications reviewed / Interviews arranged. Application form / pre-employment screening forms sent as required. Once job offer accepted written offer and contract of employment sent out. Pre-employment checks completed including references and employment checks as required. Competence of potential new employees is considered during recruitment.
All colleagues are security screened to BS 7858:2019. Our screening process is documented in **PIP 29 – Security Screening.**

3.1.2 New Employee on-boarding Procedure

Colleague Induction is documented using an Induction Checklist - Ensuring that all essential checks completed;

- Staff Files completed and filed correctly to comply with Data Protection Legislation.
- New employee made aware of the IMS / Policies / Procedures.
- Photographic ID / Other employability checks completed.
- Colleague Identification Card with Physical access rights to authorised areas issued.

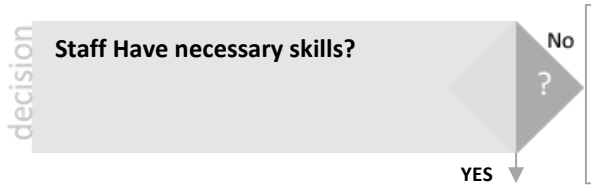
Where required job descriptions / contracts prepared and employee personnel folder setup (locked). Training folder setup if required. Equipment issued including keys or logins to software logged.

3.1.3 Management of Employee Personal Data

Employee Personal Details checked on ongoing basis and formally checked during annual review to ensure all personal data held is accurate.

3.1.4 Training / Management of Competence

Competency requirements for job or specific processes / activities documented.
Training programmes are designed to assist the workforce in achieving competency for their operational activities.
Awareness - All persons doing work under our control will be made aware of relevant policies, procedures, objectives, the management system and achievement of objectives.
Training Delivery - Training completed in-house or by 3rd party and records updated. Effectiveness of training will be reviewed.
Toolbox talks - when completed attendees should sign attendance form.



Update Training Programme to ensure all colleagues have skills necessary for their role.

3.1.5 Staff Training Records

Training record setup to record details of training where required. Copies of training certificates / licenses should be filed and retained as required with key details including renewal / expiry dates logged on a team Competency Matrix.
Training records should include details for labour-only sub-contractors.

Training Review - Where possible an annual review is completed with all colleagues to review training records, competencies and awareness and to give colleagues a formal opportunity to provide suggestions, feedback and identify any training requirements.
Overall review of competencies and training needs within the organisation completed during Management Review.

3.1.6 Staff Leaving Procedure

Arrange exit interview / meeting prior to departure if possible and complete Termination Checklist.
Security - Ensure any logins, keys to secure areas and IT equipment with access to company data is returned or appropriate action taken to disable.

3.1.7 More Information

Our **PIP 04 – Competence, Awareness and Training Procedure** has more information.

3.2 Management of Equipment and Premises

Responsibility: Operations Director

All equipment that requires inspection, maintenance, calibration will be managed and checked with summary of arrangements for management of equipment and premises detailed below.

Description	How Managed	Responsibility
Computer / Office Equipment	Office equipment is visually checked on a weekly basis. Faulty equipment is segregated and taken out of service. Computer and Office Equipment will be maintained on a reactive basis. PAT Testing to be completed every 2 years.	User/ Manager/ IT Department
Electrical Equipment	To ensure electrical equipment is safe for use regular checks should be completed and where required Portable Appliance Testing (PAT) completed and checked items marked accordingly. PAT Testing to be completed every 2 years unless it is high risk which it will be completed annually.	User/ Manager/ Operational Director
Premises, Buildings and Infrastructure	Buildings and Infrastructure will be checked on an ongoing basis and checks documented on a monthly basis using the Premises Inspection Form on Pointer Portal. Electrical Checks (Fixed Wiring Inspection), Emergency equipment checks completed every 5 years, Heating / Ventilation and any other scheduled checks of equipment within the premises will be detailed on **PIP 05 – Equipment Maintenance**.	Manager/ Compliance Manager Compliance Manager
Vehicles	Vehicles will be inspected / serviced / MOT as per the vehicle list / monthly checklist	Owner/ Manager/ HR Manager
Work Equipment	All equipment is maintained and repaired as required and inspected prior to use. Where documented pre-use checks are required, this will be logged and records maintained. Faulty equipment will be marked as 'not for use' or quarantined. Where required a schedule of maintenance is prepared for any items of equipment that require regular checks and maintenance. Details are logged the asset list and records of checks retained.	User/ Manager
CDM Principal Contractor Role	Where we are the designated principal contractor then the following equipment is to be provided, adequate and inspected. First Aid Kit & Signs, H&SAW Poster, Induction, Induction Records, Sign In Book, Induction Register, Competency check, Details of Welfare. Emergency arrangements.	Senior Project Engineer
Telecommunications	Mobile Phones and Tablets with SIM Cards will require the user to sign an agreement of use.	User/ Manager/ IT Department

3.3 Management System Communication

Responsibility: Technical & Compliance Manager

The following internal and external communications have been identified as relevant to this management system.

Item	Communication Frequency	Interested Parties Communicated to	Communication Form	Responsibility
IMS related; Audit findings, issues & actions, objectives, changes & improvements, company policies (public policies)	Available at all times. Colleagues / interested parties notified of any significant changes. When findings are reported.	Top management. Relevant parties. All colleagues.	**Pointer Portal** Training / Toolbox talks, Appraisals. Focus Committee. **H&S Alerts**; emails, meetings, risk assessments / method statements	IMS Lead. Relevant Manager.
Environmental; Environmental Incidents. Environmental aspects and impacts.				IMS Lead. Relevant Manager.
Health & Safety; H& S updates H&S Incidents / near misses				IMS Lead. Relevant Manager.
Emergency Arrangements; Business Continuity / Disaster Recovery	As required by authorised persons only.	All relevant parties. Top management.	**Pointer Portal** Continuity Plans / Register.	IMS Lead Authorised persons only.
Data Protection; Data subject access requests. Data Breaches.	When requested. As required.	Data subjects.* Management. ICO.*	**Pointer Portal** Secure communication for external communications.	IMS Lead. DPO.
Authorities; Significant 3rd party enquiries / communications	When requested.	Regulators or other significant 3rd parties.	As appropriate based on enquiry or communication received.**	IMS Lead. Authorised persons only.
Customers; Product / Service Information. Feedback from Customers.	As required.	Top management. Any interested parties upon request.	Promotional literature, quotes, marketing material & specifications. Feedback forms.	Relevant Manager. IMS Lead.
External Providers; Product / Service requirements.	As required.	Top management. External providers.	**Pointer Portal** Supplier appraisal forms.	Relevant Manager. IMS Lead.

*** Data protection** - Security checks completed to confirm identity of data subject before any personal data is shared using appropriate secure communication. Minor data Breaches are reported internally, significant breaches are reported to relevant authorities i.e. ICO (Information Commissioner's Office) and the Data Subject(s) concerned.

**** Communication Log -** All significant communications with external interested parties should be logged on the **Issues Register** / communications log and relevant communications filed and retained as required.

External Communications
Key policies (marked public) can be distributed & made available to all Interested parties upon request (e.g. customers). All other documents are controlled and should not be distributed without approval.

Communication Guidance - All colleagues should be aware of and follow the **P 17 - Communications Policy**. Consideration of diversity aspects (language, culture, literacy, disabilities) will be made when planning all communications.

More information can be found on **our PIP 28 – Consultation and Communication** Procedure.

SECTION 4 OPERATIONAL PROCESSES

4.1 Control of Enquiries & Sales

Responsibility: Administration Manager

4.1.1. Receive Enquiry
Enquiry from prospective or existing customer.

decision
Process Enquiry?
Technical Review outcome - proceed?
Can we provide product / service requested?
No ?
YES

Details discarded if no action has been taken.
If useful, document.
If customer or other requirements cannot be met do not proceed.

4.1.2. Process Enquiry
Register Enquiry onto system by completing (Pointer, PointerFire – **Survey Information Form**. JGE – Sales Enquiry)
Check that all customer (and organisational) requirements can be met.
Prepare Quote / Design Proposal where appropriate. All quotes are reviewed by nominated designers before issued to customers. If the solution is a larger project then the design approval stage process is required. The response to the client may be through a tender submission which would be the clients own documentation and requirements.

decision
Quote accepted?
No ?
YES

Review and if appropriate request feedback on why unsuccessful
Any issues / shortcomings identified logged on the **Issues Register.**

4.1.3. Enquiry Successful
The status of the enquiry is changed to Work Accepted.
For long term jobs, contracts are drawn up specifying time span, staged payments, payment terms and variation allowances. A project kick off meeting is required to be completed.
If a customer does not provide any documentation of their order requirements, this should be confirmed before accepting the order. Where required a Purchase Order with full order details should be requested.
Any change or additional requirements should be documented and if required agreed with the customer.

4.1.4. Process Customer Details
If a new customer, then payment details requested (where applicable) using **Credit Account Request** Form and details added to accounts system.
Payment terms agreed or no credit offered. Any staged payment schedule / payment terms agreed passed to Finance for invoicing.

decision
Credit check outcome - proceed?
PO supplied?
Payment terms agreed?
No ?
YES

Order put on hold until resolved.
A director can approve the credit check if still to progress.

4.1.5. Contract Review
The engineering department will review all the documentation before accepting the works. This involved reviewing all the information on the survey information form and system design proposals along with any drawings.
The supervisor / project manager will change the status of the Survey Information Form to Contract Reviewed and sign once approved. Installation Planning can then go ahead.
Larger projects will have a project plan agreed by the client or principal contractor. If Principal Contractor, then a Construction Phase Plan is required.

4.3 Control of Operations

4.2 Control of Purchasing and Outsourced Services

Responsibility: Finance Director

4.2.1. Supplier / Contractor Appraisal
Approved Suppliers are listed on approved suppliers list and entered in our Accounts Software. Any new suppliers will be appraised against supplier requirements before details are added to the approved suppliers list.
Quality, Environmental, Information Security, Corporate Social Responsibility and Health and Safety consideration is given when appraising suppliers.

Key Suppliers / Sub-Contractors
Key suppliers or sub-contractors (where product / service supplied could impact on the quality of our own product / service provision) is fully appraised and details added to the key suppliers / sub-contractors register. Where required the key suppliers appraisal form should be completed and copies of relevant insurances, licences, certifications or qualifications obtained.
Other suppliers who are required to hold a valid licence(s), registration or insurance(s) should also be added to the Key **Approved Suppliers list on SharePoint**

decision
Does the Approved Supplier List contain a suitable supplier?
No
YES

Research new suppliers and complete appraisal before adding to approved suppliers list.
If Key supplier / Contractor full appraisal required and details should be added to the **Approved Suppliers List.**

4.2.2. Continue with Order
Raise purchase order (PO) with adequate specification where required.
Copy of PO held in office / copy supplied to incoming goods

4.2.3. Check of incoming Goods / Materials / Paperwork / Supply of Services
Check incoming goods against delivery note ensuring everything is in a satisfactory condition, quantity and specification as per delivery note and relevant paperwork supplied as required. Where required incoming goods marked with PO number, stock product code or relevant job number if allocated. Stock updated and materials stored in an appropriate manner.
Incoming paperwork - check against issued PO and process / schedule payment if correct.
Review any service provided was as agreed and work completed to an acceptable level.

decision
Supplied goods / services all correct?
No
YES

Materials / Products
Wrong / Missing Paperwork / Damaged - Note & Quarantine
Short / Late – Note and Use
All significant issues to be raised as per **5.2 Control of Nonconforming Outputs** or logged on the **Issues Register.**

4.2.4. Review of Supplier Performance
Existing suppliers are appraised on an ongoing basis and the approved list should be updated to reflect current performance rating / approved status. Approved suppliers will be reviewed during management review.
Significant supplier issues raised as per **5.2 Control of Nonconforming Outputs.**

4.2.5. Information Security in Supplier Relationships
Suppliers who can access, store, communicate or provide IT infrastructure components for company information will have information security requirements agreed and documented. Documented agreement will identify and address any information security risks identified. Ongoing services will be monitored to ensure effective management of change and reappraisal of risks.

4.2.6. Performance of Suppliers
Supplier performance will be discussed at part of our Management Review Meetings.

4.2.7. More Information
More information can be found in our **PIP 06 – Control of Suppliers and Contractors** Process.

4.3 Control of Operations

Responsibility: Operations Director

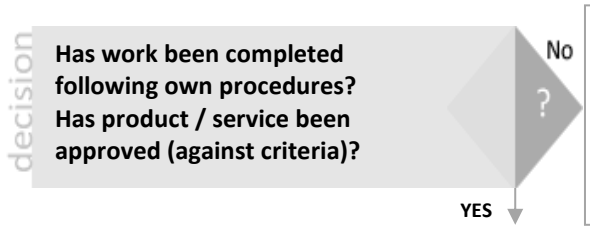
4.3.1. Planning
Staff Competency - Work will be carried out by competent persons Ref. **3.1 Management of Staff…**
Work Equipment - Work equipment will be maintained and calibrated Ref. **3.2 Management of Equipment…**
Safety Arrangements / Pre-start Checks - Hazard / Risk Assessments completed prior to commencement of work as required. Any Personal Protective Equipment (PPE) or other safety equipment or controls should be in place and functional prior to starting work. Any pre-use checks of equipment or vehicles must be completed & any defects reported.
Pre-Start Check of Customer Requirements - Colleagues will have access to customer requirements and any other specifications before commencing work. Manager contacted if any issues. Customer informed if agreed arrangements cannot be met and alternative arrangements made.

4.3.2. Operational Process
Work completed as per supplied job sheets / work instructions / operational procedures.
If any changes are required this must be approved and the customer informed where required. Any significant changes should also be controlled and reviewed (with documentation on review results retained).

Operations should be completed as per the following Operations Procedures;

Operational Activity	Operational Procedure
First and Second Fixes	**Section 4.4**
Commissioning and Handover	**PIP 22 – Commissioning and Handover**
Inspection and Test Plan	**Inspect and Test Register**

4.3.3. In-process / Final Inspection and Process Review
Ongoing Inspection / monitoring and final inspection of operations will be completed to ensure conformity and documented with details of each input / process as required. Labelling will be used to indicate inspection status as required. There are no in-progress inspection records unless the client requests additional checks or if work is being handed over to another team. Final inspection records are provided to the client upon final commissioning and handover of the system.
Any issues or improvements should be reported to management.



Document problems as per **5.2 Control of Nonconforming Outputs** and if necessary, quarantine non-conforming products / implement corrective action.

4.3.4. Documentation Requirements
Measurement Readings, Handover Checklist, Completion Certificates and Handover paperwork will be collated and filed Ref. **1.5 Management of Documented Information and Data.**
Documentation is retained with the evidence product / service meets requirements, any identification or traceability evidence including details of labour, materials, components or equipment used and any other details as required. Final inspection records including the name of the person who inspected or authorised the product / service release is also be retained as required.
Document retention times can be found in our **PIP 01 Documented Information and Records Procedure.**
On completion, an NSI Certificate of Compliance / BAFE Certificate is issued to the client within 28 days on completion.

4.3.5. Accounts / Invoicing
Details of completed work including any agreed variations or additional work passed to Administration for invoicing.
Ongoing review of payment status and ongoing work to manage risk associated with any non-payment.

4.4 Management of Change, Variations and Design

Responsibility: Technical & Compliance Manager

4.4.1. Management of Change

Changes may be required in response to a significant problem, a planned improvement or in response to some other internal or external requirement. Changes must be planned and reviewed with consideration of any impact the change could have on identified risks or any new risks that might result from the change. Ref. **2.5 Risk Management.**

The change review process (as detailed on **Management of Change Form** should be followed for all changes and for significant changes for company systems and processes, these should be documented using the **Management of Change Form.**

Where there is any significant impact on hazards / risks a full risk assessment process will be completed.

All changes must be authorised by the person(s) named above and / or person(s) responsible for process / area being changed. Simple changes are managed by logging actions on **the Issues Register**.

Changes to documentation - managed as per **1.5.2. Management of Changes and Review**

4.4.2. Variations

Changes to customer requirements will be logged and managed effectively. Where a customer requests a change that may lead to additional cost this must be agreed formally and documented. An additional Purchase Order, written instruction or completed job variation form may be required.

4.4.3. Design - Initial Design Assessment

Initial design reviewed to establish if suitable for further consideration and allocation of resources.

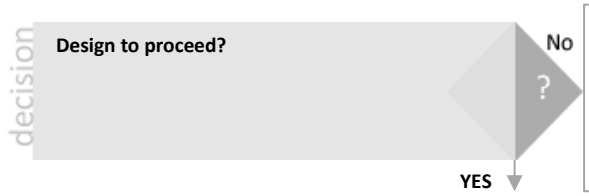
Consideration given to nature & duration of design activities required, complexity and process stages, likely internal and external resource requirements, who would need to be involved in the design process and how this would be managed.

Other factors such as regulatory requirements, overall cost / benefit and documentation requirements should also be considered.

4.4.4. Design Review

Design reviewed using F-Q1 Design Review and Planning form.

Decision taken to establish if to proceed after design inputs considered.



Update F-Q1 Design review and planning form detailing why design was rejected and not to proceed.

4.4.5. Design - Project Assessment, Completion and Review

Drawings prepared (if required) and summary of requirements in terms of functionality, safety and regulatory requirements. Project phases, key roles and project lead identified and recorded on F-Q1 / Gantt chart.

Technical File with all design stages, testing, reviews and other documentation including any drawings, paperwork or certificates relating to any parts, materials and components used and other relevant details setup.

Pre-start and ongoing meetings held as required to review and minutes / key points noted in minutes or on F-Q1.

Design verification completed to ensure outputs meet input requirements and validation completed to ensure meeting requirements for intended use.

4.4.6. Design Changes

Design changes required to existing products or services should be reviewed to ensure there is no adverse impact on conformity to requirements. Details of design changes reviewed and details logged on F-Q13-Design Change Request Form

SECTION 5 MONITORING, EVALUATION AND IMPROVEMENT

5.1 Customer Satisfaction

Responsibility: Technical & Compliance Manager

5.1.1. Customer Requirements Determined

Management shall ensure that customer requirements are determined and are met with the aim of enhancing customer satisfaction.

5.1.2. Employees Awareness on Customer Satisfaction

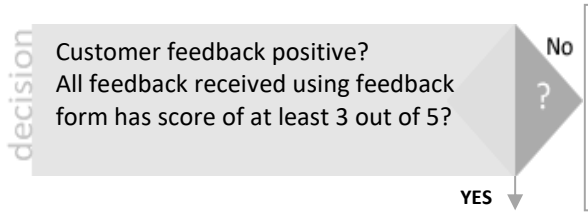
Colleagues will be made aware of the importance of achieving, and where possible, improving customer satisfaction, and will be trained on the importance of customer satisfaction and how to respond to customer feedback.

5.1.3. Collecting Feedback from Customers

Customer satisfaction will be checked by ongoing reviews with customers using the most appropriate approach for collecting feedback such as meetings, emails or telephone conversations.

Customer feedback gathered should be retained and filed in Feedback folder for review and analysis.

Where appropriate formal feedback can be requested by providing an **online customer feedback questionnaire** to customers.



Negative feedback or any feedback forms returned with a score of 2 or less should be investigated as a problem and documented as required.

Ref. **5.2 Control of Nonconforming Outputs...**

5.1.4. Review Customer Feedback

Customer feedback should be reviewed and any trends or significant findings noted.

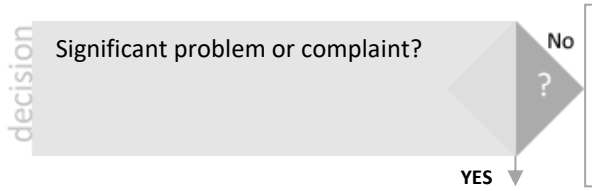
All feedback received using the customer questionnaire can be added to the **Customer Focus Register (Sharepoint)** which is used to analyse trends in customer satisfaction.

Feedback is reviewed on an ongoing basis, with significant trends reviewed during Management Review.

5.2 Control of Nonconforming Outputs, Problems and Complaints

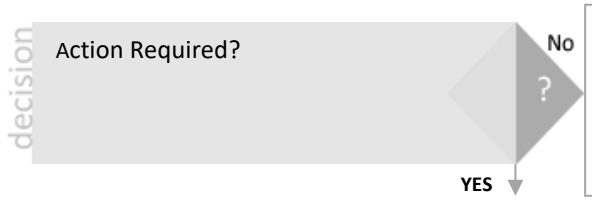
Responsibility: Technical & Compliance Manager / Appropriate Managers

5.2.1. Training on Dealing with Problems and incidents
Colleagues given training to ensure they are aware of how to deal with problems, incidents & complaints, how to raise improvement suggestions, report information security weaknesses and how to identify and control nonconforming outputs.



Rectify and if helpful add details to the **Issues Register**.

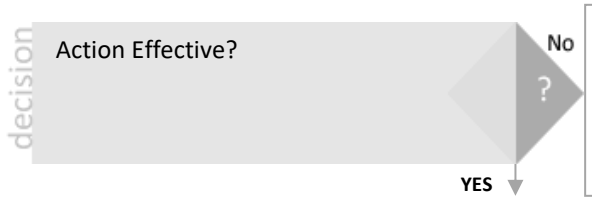
5.2.2. Problem / Complaint / Information Security Incident / Nonconforming Output Identified
Deal with problem / complaint / incident/ nonconforming output, investigate and if useful document key points using Significant Problem Incident Complaint Form (F-Q10) and / or record on the **Issues Register**.
All significant information security weaknesses or events are to be logged on the **Issues Register**. If the event or incident is serious, Senior management must be immediately informed and all work on systems affected by the issue will be suspended or controlled to ensure no further issues.
Root Cause Analysis - when reviewing the issue consideration should be given to the root cause of the problem so that action can be taken to ensure similar problems do not occur again.



If no further action is required the issue is closed and this should be documented on the **Issues Register**.

5.2.3. Containment and Corrective Action
Containment action should be taken as required to ensure. Plan and implement corrective action to further deal with and prevent re-occurrence of problem. Ref. **4.4 Management of Change...**
If nonconforming output identified, either segregate / return, inform customer, rectify problem or receive approval of output as it is. Update **Issues Register** with details of corrective action.
Any communications with external authorities or other interested parties necessary as a result of the issue should be managed by designated responsible person. Ref. **3.3 Management System Communication.**

5.2.4. Review Corrective Action - Verification
Review and confirm that the corrective action taken has been effective.



Re-investigate and take alternative / additional corrective action and update the **Issues Register** accordingly and then check again if action has been effective.

5.2.5. Review of Controls / Opportunities for Improvement
Decide whether training / further controls are required or if changes to IMS are necessary.
Review significant problems at Management Review.
Review **Risk and Opportunities Register** and update if required. Ref. **2.5 Risk Management.**

5.2.6. More Information
More information can be found in our **PIP 26 – Corrective and Preventative Actions Procedure**

5.3 Management System Audits (Internal Audits)

Responsibility: Technical & Compliance Manager

5.3.1. Internal Audit Planning - Audit Schedule

Internal Audit Schedule will be prepared detailing area / department / process to be audited, assigned auditor and audit frequency.

The audit schedule must take into account importance of area audited, findings from previous audits, risks, importance of area being audited and any other relevant problems / issues that may have been raised and adjust schedule accordingly.

Any special requirements needed for an audit will be taken into consideration. Further details can be found on **PIP 20 – Internal Audits and Inspections** procedure.

5.3.2. Internal Audits - Audit Completion

Internal audits should be completed by competent persons who are, wherever possible, independent of the area they are auditing. Audits will be completed using observations, interviews, and reviewing documentation / records

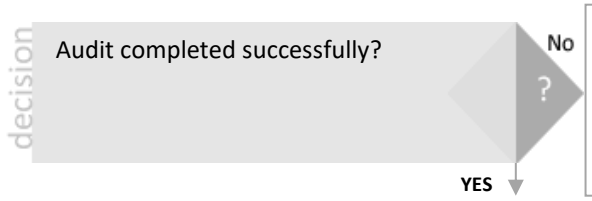
The nominated Lead Auditor is required to have completed Internal Auditor Training of Management Systems and qualifications or relevant experience in the different types of Management Systems. Where the Lead Auditor is responsible for a process in the Management System then the Impartiality Auditor will audit these functions, conducted by interview and sampling documents/records. The Impartiality Audit must have auditing qualifications and experience, the Lead Auditor will provide the Impartiality Auditor with all information required to complete the audit process.

The purpose of the audit is to;

1. Check whether the company is meeting the requirements of the ISO Standard(s)
2. Check whether the IMS is reflecting current practice and that documented procedures are being followed
3. Ensure operations / processes are being completed correctly and that paperwork is in order and all regulatory / statutory requirements are being met
4. Identify any possible improvements

Audits can be completed using a pre-prepared Audit Checklist or by simply asking pertinent questions and noting down what was asked and evidence viewed.

An impartiality Auditor will review the work of the Internal Auditor that they are responsible for.



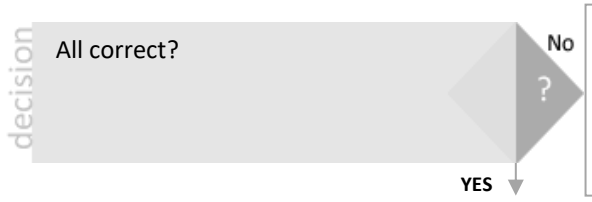
Arrange additional training for internal auditors.
Adjust Internal Audit Schedule reschedule audit as required.
Prepare new Audit Checklist.

5.3.3. Internal Audit Findings - Audit Report

Evidence viewed should be recorded on the internal Audit Checklist. This can also be used to report minor findings or recommendations for improvements back to auditees and management.

Significant findings (identified non-conformities) should be dealt with as per **5.2 Control of Nonconforming Outputs** to ensure finding is documented using Problems form / Issue Tracker with detail of who is responsible for investigation and follow-up to ensure any proposed corrective action is carried out.

Where significant findings are raised the Internal Audit Schedule should be reviewed and updated with additional audits as required and relevant management informed.



Further audits completed until no issues and any new procedures / processes implemented are found to be working effectively.

5.3.4. Internal Audits - Review

Findings from Internal audits are reviewed at Management Review where forward audit schedule should also be reviewed and approved.

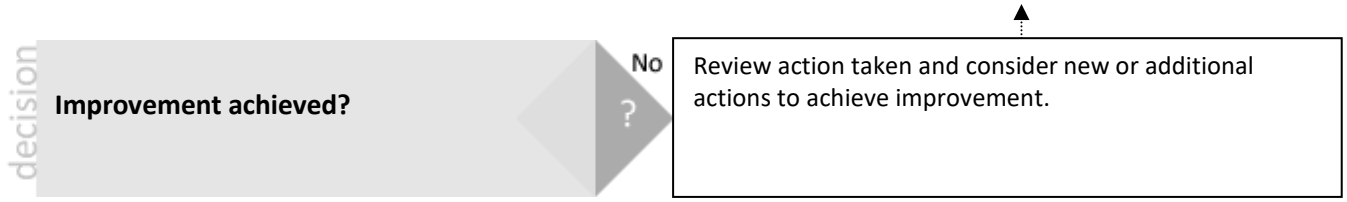
5.3.5. More Information

More information can be found in our **PIP 20 – Internal Audits and Inspections Procedure.**

5.4 Continual Improvement

Responsibility: Technical & Compliance Manager

5.4.1. Actions to Achieve Continual Improvement
Action taken to improve IMS or any other aspect of operations.



5.4.2 Mechanisms for Achieving Continual Improvement

Various mechanisms are in place to assist with achievement of continual improvement including the various processes and procedures outlined within this IMS1 document as summarised below;

Section of IMS1	Mechanisms to achieve continual improvement
1 Integrated Management System	- **IMS / Forms / Documents** - processes to manage and improve documentation - **Information Assets** - process to ensure information is effectively managed - **Legal Compliance** - Improvements required to comply with existing or new legislation
2 Leadership Commitment and Planning	- **Company Policies -** Certain policies include commitment to continual improvement - **Company Objectives -** Overall strategy to achieve improvement - **Risk Management -** Improvements to reduce / avoid risk
3 Resource Management and Support	- **Management of Staff** - Worker engagement; meetings, reviews and training with staff to get feedback and participation with / initiation of improvements - **Management of Equipment & Premises** - Ongoing checks and monitoring to identify any improvements required
4 Operational Processes	- **Enquiries -** Ongoing review of requirements and enquiry conversion to identify opportunities for improvement - **Suppliers** - Ongoing review to improve supplier performance / select better suppliers - **Operational Review** - process for review and improvement of service provision - **Management of Change, Variations and Design** - formal process for managing change, including any improvements
5 Monitoring, Evaluation and Improvement	- **Customers** - Feedback reviewed to identify improvement opportunities - **Problems / Complaints -** Ongoing review of issues to identify improvement opportunities - **Management System Audits -** Improvement opportunities identified during audits
6 Environmental	- **Environmental Monitoring -** Improvements to Environmental Management
7 Health & Safety	- **OH&S Monitoring -** Improvements to OH&S Management
8 Information Security	- **Information Security Management -** Improvements to Information Security
9 Business Continuity	- **Business Continuity Management System** – Improvements from incidents and rehearsals

SECTION 6 ENVIRONMENTAL MANAGEMENT

6.1 Commitment to Environmental Protection

Responsibility: Technical & Compliance Manager

6.1.1. Environmental Commitment
The Environmental Representative, Ref. **2.2 Responsibilities**, is responsible for ensuring the company is committed to protecting the environment (as outlined within the Environmental Policy). This Management System has been developed to the requirements of **ISO 14001:2015** and this ensures we monitor and strive to continually improve our Environmental performance.

6.1.2. Environmental Legal Compliance and Updates
The Environmental Representative shall be responsible for maintaining current information on environmental legislation and supplementary information as documented in **1.6 Legal Compliance**. Environmental legal compliance will also be assessed during internal audits **Ref. 5.3 Management System Audits**.
The Environmental Representative has access to appropriate environmental updates. **Ref. 2.2 Responsibilities**

6.1.3. Environmental Impacts and Aspects Assessment
Consideration has been given to identify the environmental aspects of the business which have a significant impact on the environment and which can be controlled and influenced by identifying priorities, setting objectives and implementing procedures. **6.2 Environmental Assessment** outlines our procedure for managing this.

6.1.4. Life Cycle Perspective
The purpose of a life cycle perspective is to consider how environmental performance could be improved by considering if there are improvements that could be made beyond those directly relating to our operational activities such as improvements that could be made by other interested parties such as suppliers or customers and whether these interested parties could be influenced to achieve improvement. The life cycle perspective involves consideration from the very start (upstream) such as how raw materials required are extracted or energy generated right through to (downstream) final end of life disposal. Life cycle perspective analysis can be found on the **Environmental Life Cycle Perspective Review Register**

6.1.5. Environmental Awareness / Environmental Training
Environmental awareness training is provided to all colleagues on an ongoing basis and during induction of new colleagues. The training will cover significant environmental aspects and their associated impacts, and planned emergency responses.
As well as training, all colleagues can also be issued with / have access to **Environmental Staff Handbook**.
Ref. 3.1 Management of Staff and Company Personnel.

6.1.6. Environmental Communication
Any communication regarding environmental matters will be recorded. For cases where environmental complaints are received, these will be documented and investigates as per **5.2 Control of Nonconforming Outputs...**
Significant problems or environmental incidents will be discussed during the Management Review.
3.3 Management System Communication further details how environmental communication will be handled.

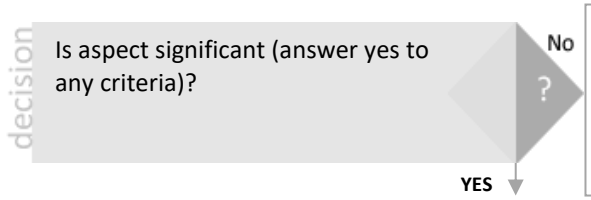
6.2 Environmental Assessment

Responsibility: Technical & Compliance Manager

Aspects and Impacts Significance Procedure

6.2.1. Determine Environmental Aspects
Check activities / business areas that may have environmental aspects, e.g. fluorescent lights, energy, toners, computers, mobile phones, paper waste, chemicals, vehicles. Abnormal business conditions will also be considered in determining environmental aspects. Once environmental aspects are established, consider their environmental impacts.

6.2.2. Determine Level of Environmental Impact and Aspect Significance
Our **Environmental Aspects and Impacts Register** describes each aspect and its environmental impact with significance determines by scoring against a criterion of **potential for emergency situation, impact on the environment**, and **if legislation covers the aspect**.



No further action required – review existing controls and improve is possible.
Retain completed form for record of aspect assessment.

6.2.3. Determine Controls
Environmental Aspects and Impacts Register completed to detail controls in place. Controls are actions you are taking to manage the significant aspect, and can include actions that should be taken if an environmental incident occurs (emergency response). You must also determine if the aspect can be controlled or influenced (stated in description of controls).

6.2.4. Record Significant Environmental Aspects
Significant aspects and their controls are documented on **Environmental Aspects and Impacts Register**

6.2.5. Life Cycle Perspective
Life cycle perspective consideration is given to all aspects identified and further review of upstream and downstream activities to establish if any control or influence could be used to achieve improvement in environmental performance at any stage of the product / service life cycle. This is documented in the **Environmental Life Cycle Perspective Review Register.**

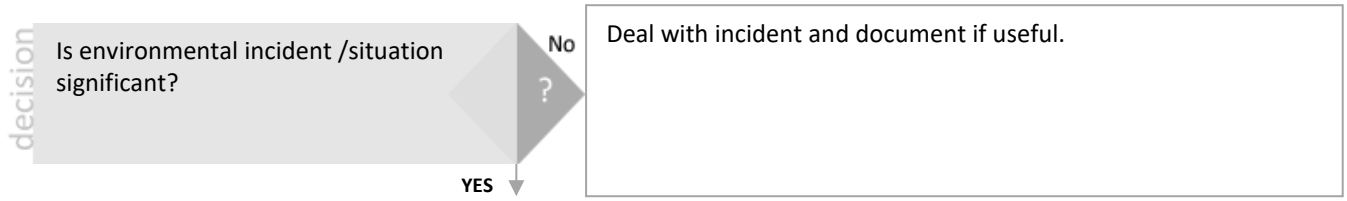
6.3 Environmental Incident Prevention & Management

Responsibility: Technical & Compliance Manager

6.3.1. Staff Training
Colleagues given training to ensure they know how to respond to environmental incidents.

6.3.2. Oil and Chemical Storage
Oils and chemicals will be stored in a responsible way to reduce any potential environmental incidents and emergency situations and comply with relevant legislation.
Ref. **6.4 Environmental Procedures**

6.3.3. Environmental Incident
Any environmental incidents (e.g. oil or chemical spill, or fire) will be reported to the person responsible named above..



6.3.4. Deal with Environmental Incident
Contact emergency services and other environmental contacts if required (listed in table below).
Ref. **6.4 Environmental Procedures**

6.3.5. Review and Test Emergency Response
Document the incident/emergency as per **5.2 Control of Nonconforming Outputs...**
Following the occurrence of an emergency, the effectiveness of the arrangements and response will be reviewed.
Incidents will also be formally reviewed during Management Review.
Emergency response actions (e.g. fire drill, oil spill) will be tested during the Environmental internal audit, ongoing site inspections and as part of the premises monthly inspection **(F-Q26 Premises Checklist).**

Environmental Contact Help lines / List of Contacts / Specialist Contractors
See Site Safety Emergency Details for each office location.

6.4 Environmental Procedures

Responsibility: Technical & Compliance Manager

We have Environmental Policy-Procedures in place to provide additional guidance and procedures relating to how we manage all aspects and activities which can impact on the environment.

All workers are given training in environmental management and all the Policy-Procedures listed below.

Environmental Policy-Procedures

Procedure	Policy-Procedure File Name - Any files referenced within the Policy-Procedure
Environmental Waste Management	**PIP 64 – Production and Disposal of Waste** **F-ENV2 Waste Matrix**
Environmental Oils Chemicals COSHH	**PIP 42 – Control of Substances Hazardous to Health** **COSHH Register (Pointer Portal)** **COSHH Assessments (Pointer Portal)**
Environmental Emergency Response	**PIP 27 – Emergency Planning and Response**
Environmental Spills	**Emergency FAQ's (Pointer Portal)**

SECTION 7 HEALTH & SAFETY MANAGEMENT

7.1 Commitment to Health and Safety at Work

Responsibility: Managing Director

We, as an organisation, recognise and accept our responsibility to provide a safe and healthy working environment for all employees, contractors and clients in order to prevent injury and ill health, in accordance with the Health and Safety at Work Act and other pertinent Health & Safety regulations as detailed in **1.6 Legal Compliance**.

This Management System has been developed to the requirements of **ISO 45001:2018** and this ensures we monitor and strive to continually improve our Health and Safety performance. The benefits of improved Occupational Health and Safety (OH&S) are numerous;

- Safer, happier and healthier workers and workplace
- Increased productivity - less work time lost due to injury
- Enhanced reputation - meeting customer expectations and other OH&S scheme requirements
- Demonstration of social responsibility - less chance of litigation.

The health and safety of all interested parties, colleagues, customers, visitors and general public, will be of paramount importance. Specifically we will ensure that all colleagues, visitors, contractors and consultants have sufficient information to carry out their duties with minimum of risk. Safety will always be the first consideration in all matters relating to our activities.

In addition to this IMS we have prepared a **Health and Safety Policy Statement** which is available to all colleagues and other interested parties and also the following Health & Safety documents are made available as required;

- **Safe Operating Procedures**
- **Risk Assessments / Method Statements**
- **Health and Safety Handbook**
- **HSE Guidance Documents**

Health and Safety Statement of Intent:

- We will provide and maintain safe and healthy working conditions for all our employees, providing appropriate tools, equipment, operational processes and safe systems of work covering all our activities.
- Our management accepts the responsibility for applying the above and for providing information, instruction and training at all times and for the duration necessary to achieve this purpose.
- Other parties that may be affected by our activities i.e. visitors, neighbours, contractors etc. should also be considered and it is our responsibility to provide appropriate levels of safety for them as well.
- We will provide suitable facilities and / or make the necessary arrangements for the welfare of all our employees at work.
- Where risks to safety or health need to be assessed we will ensure that an appropriate assessment is carried out and that all actions shown to be necessary will be implemented.
- Should any of our activities endanger the health of any employee, such activities will be monitored and where necessary, arrangements for health surveillance and risk mitigating controls will be made.
- We will provide suitable information regarding the safety or safe use of our services and / or products.
- We plan to minimise the risks created by work activities, products and services.
- We are committed to developing a positive health and safety culture with participation and communication of OH&S issues and improvements at all levels and throughout the organisation.

Additionally we will ensure:

- That adequate resources for ensuring Health & Safety are provided;
- That training needs are identified and met;
- That plant and equipment, owned or hired, is of safe design and properly maintained;
- That we maintain a robust system of self-regulation which involves inspections, audits and continuous monitoring.

7.2 Health and Safety at Work – Guidance and Arrangements

Responsibility: Technical & Compliance Manager

The greatest importance is placed on Health and Safety matters and we undertake to conduct operations in such a way as to ensure the health and safety of all personnel, visitors and the general public.

You are required to take all reasonable steps to safeguard your health and safety, and that of any other person who may be affected by your actions, and to observe at all times safety rules and procedures.

You must report incidents and near misses no matter how small. **Ref.** **7.4 Accident, Incident and Near Miss Reporting**
It is important to avoid accidents and injury and to ensure this all colleagues should be familiar with and follow company OH&S procedures and requirements. Any personnel who do not conform to OH&S requirements will be subject to disciplinary action.

Medical Assessments

1. Prospective Employees may be required to complete a pre-employment medical questionnaire. Employment will be conditional upon the satisfactory outcome of this Medical Questionnaire.
2. Employees who are absent due to a personal illness may be required at any time to have Medical Assessment by an Occupational Health Advisor or a Doctor nominated by the company to determine their fitness for employment.
3. Employees must be prepared to be medically assessed by an Occupational Health Advisor or a Doctor nominated by the company where it is believed that the Employee may be endangering his / her health and safety or another Employee's health and safety.

Display Screen Equipment (DSE) Regulations
On commencement of employment all colleagues using DSE should complete an individual workspace assessment. Any additional equipment required will be arranged and supplied by the Company. Where required DSE assessments are then completed at least annually or if there is a change to workstation.

Health and Safety at Work Act
Our high standards of Health and Safety are in accordance with the Health and Safety at Work Act which places legal duties on colleagues and management as follows:

- *To take reasonable care for the health and safety of themselves and of other persons who may be affected by their acts or omissions at work.*
- *To co-operate with Management to enable the employer to carry out his legal duties or any requirements as may be imposed.*
- *No person shall intentionally or recklessly interfere with or misuse any item provided in the interests of Health, Safety and Welfare.*
- *Every employee must use machines, equipment, dangerous substances, transport equipment, means of production or safety device provided by the employer, in accordance with the training and instructions received (whether this be written or verbal).*
- *Every employee must inform the employer or any other employee with specific health and safety responsibilities for fellow employee;*
  - *Of any work situation where it is considered that the training and instruction received by themselves or a fellow employee, could represent a serious and imminent danger to their health and safety, and*
  - *Of any matter where it is considered that the training and instruction received by themselves or a fellow employee, could present a failure in the employers' protection arrangements for their health and safety, even where no immediate danger exists.*

Responsible Persons
Responsibilities for Health & Safety are detailed in **2.2 Responsibilities.**

Reporting Concerns and the Right to Refuse Work
If you become aware of any potential hazards or unsafe working conditions you should have no hesitation raising them with H&S Lead / Line manager. As detailed in the **Whistleblowing Policy** there will be no negative consequences for anyone who reports any incidents or concerns.
Under the Employment Rights Act employees have the right to refuse to work in or to leave their place of work if they reasonably believe that there is a serious and imminent risk of danger to themselves or to others**. Ref. Right to Refuse Work Policy**

Emergency Arrangements
Emergency arrangements are in place and tested on an ongoing basis. Emergency arrangements are detailed on Business Continuity Management Plan and site specific details on **Site Safety Emergency Details Form**. Other emergency information / signage will also be in place within the premises.
Premises are checked on an ongoing basis to ensure all emergency equipment, first aid facilities, signage etc.. is in place as required. Monthly checks are documented on Premises Checklist (**F-Q26**).
Ref. 7.5 Hazard Identification and Risk Assessment

Consultation and Participation
It is important that everyone in the organisation not only takes responsibility for their own safety but also feel they are able to contribute to and participate with the overall Health and Safety arrangements. Effective participation requires clear communication channels to facilitate open dialogue between the company and relevant personnel. To assist with this the Focus Committee is made up of representatives from all different areas of the organisation and is tasked with reviewing current H&S arrangements, highlighting any issues or concerns and making improvement suggestions. Focus committee notes – documented on **F-Q22 Health and Safety Champions** -are reviewed by management and any actions required are added to the **Issue Register**.

Workplace Stress
As a company we recognise that workplace stress is a health and safety issue and acknowledge the importance of identifying workplace stressors. The company takes a proactive approach to recognising, acknowledging and preventing potential stress risks both work related and externally. A Stress audit form (**F-HS7**) is available to all workers.

Change and Improvement
Any changes that could impact on the identified Hazards and Risks must be planned and reviewed with consideration of any impact on identified risks or any new risks. Unplanned changes must be reviewed and Risks Assessments completed as required. Ref. **4.4 Management of Change, Variations and Design**

H&S Updates and Communication
The H&S Lead has access to appropriate H&S and legislative updates though subscription to the Health & Safety Executive (HSE) update service and also through other industry associations / web sites. Competent H&S advice is also available from our internal H&S expert (Grad ISOH.

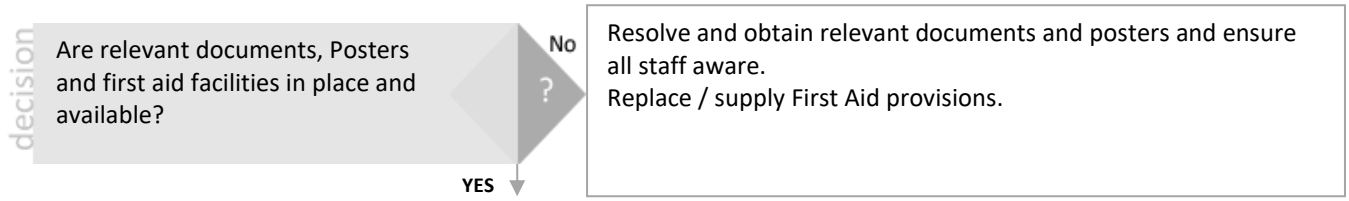
The primary method of communicating health and safety information will be through this Manual, the Health and Safety Policy, the Objectives and Targets, and Risk Assessments and through ongoing training programmes.
The responsible person named above will further communicate health and safety information by issuing Health and Safety alerts as required.
Ref. 3.3 Management System Communication

H&S Performance Evaluation
Quantitative review of performance will be completed with reference to number of accidents and incidents with targets for improvements as part of OH&S objectives. Incidents, ill health, near-misses and accidents will be monitored and reviewed and will help in the formulation for new targets and adjustments / improvements to the H&S system i.e. risk assessments / method statements / Sickness Absence Management
Ref. **2.1 Company Policies and Objectives**

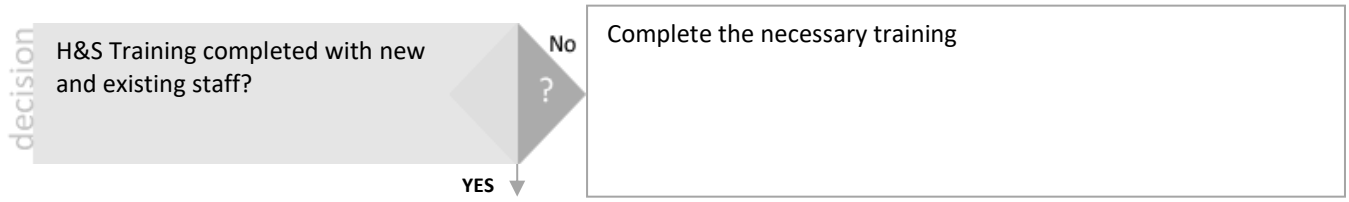
7.3 Health and Safety Procedure

Responsibility: Technical & Compliance Manager

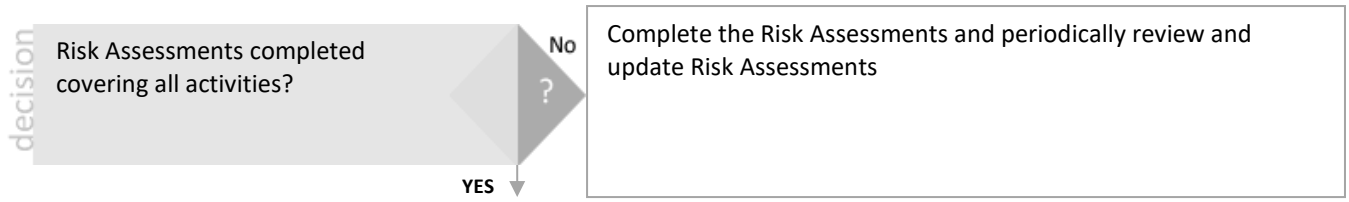
7.3.1. Key Guidance Documents, Forms, Posters, Signage & First Aid provisions
Key forms and posters will be available to workers i.e. Accident book, H&S poster, Relevant HSE Guidance, Risk Assessments, Method Statements etc...
First aid facilities will be made available and checked / maintained on an ongoing basis.



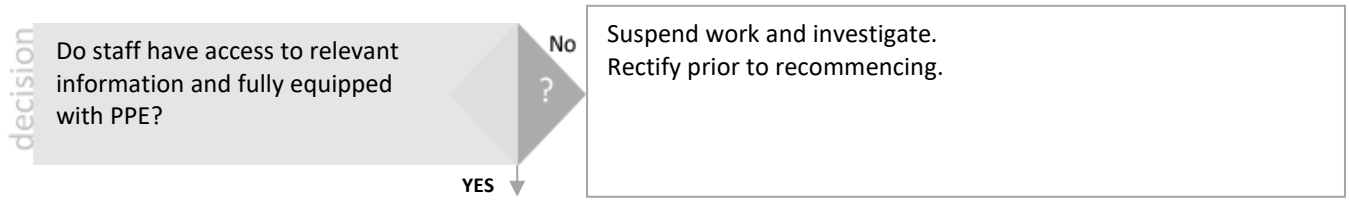
7.3.2. Health & Safety Training
All workers have are given relevant task specific training as well as general H&S training and Training records updated accordingly Ref. **3.1 Management of Staff and Company Personnel.**
Where required Toolbox talks provided to workers and attendance logged.



7.3.3. Hazard Identification / Risk Assessments
Risk assessments will be carried out for work operations & equipment and will indicate level of risk & any action or equipment required to reduce risk & will be an integral part of all work being carried out.
Ref. **7.5 Hazard Identification and Risk Assessment.**



7.3.4. Communication of H&S Requirements to Workers / PPE Provisions
Workers will have access to the appropriate Risk Assessments / Safe Operating Procedures / Method Statements and any Personal Protective Equipment prior to carrying out work. PPE issued logged on PPE Issue Register.



7.3.5. Health & Safety Review
Internal audits will review the performance of the H&S system for adequacy
Health and Safety problems / incidents are reviewed during Management review
Site safety inspections and ongoing walk round inspections completed as required.

7.4 Accident, Incident and Near Miss Reporting

Responsibility: Technical & Compliance Manager

7.4.1. In the event of an Accident / Incident

In the event of an accident or incident immediate action should be taken to ensure that containment and elimination of any further risk or potential for further incident. This action should include consideration of whether all work / site should be closed. Only once appropriate action taken to ensure there is no further risk should any investigation be completed.

7.4.2. Accident / Incident Reporting

In the event of an accident or incident (including near misses) that is not reportable to RIDDOR the H&S Lead, or delegated person, will carry out an investigation immediately and gather all associated evidence.
If appropriate Accident / Incident / Near Miss should be documented using appropriate form / register **(F-HS6 / F-HS13 / F-Q10 / ER1)** and will be reviewed by H&S Lead and any corrective action or additional controls implemented. Any actions required will be logged on issues register **(ER1)** and outcome of any investigation or any updated procedures will be communicated to all relevant workers.
Employees must report all accidents, near misses, diseases or dangerous occurrences that occur as a result of their work activities, even although no injury may have been received.

In the event of a serious accident or dangerous occurrence reportable to RIDDOR, the H&S Lead will carry out a comprehensive accident investigation immediately using the accident report form **(F-HS13)**. The results of the investigation will be used to help identify any underlying deficiencies, possible contributing factors and necessary corrective action.
Reportable accidents and dangerous occurrences which are identified in the RIDDOR Regulations must be reported at : **http://www.hse.gov.uk/riddor/**

7.4.3. Accident / Incident Investigation and Review

Wherever possible all near-misses, incidents or accidents should be reviewed to try and establish any causation factors and root cause with the aim of preventing such issues happening again in the future. The investigation should involve all relevant personnel and interested parties whose input should be sought.

In the event of an incident (or near miss) of any degree, minor or major, all associated Risk Assessments and methods of work will be examined. Improvements made to these documents will be recorded and approved by the H&S Advisor. Any changes will be reviewed and managed as per **2.5 Risk Management** and communicated to all relevant workers.

The results of all accident /incident (and near miss) investigations will be considered during Management Review. The subsequent information provided will be used to determine any underlying deficiencies or contributing factors, and help identify any possible preventative and / or corrective action, along with the opportunities for continual improvement.

All accident / incident (and near miss) investigation information will be kept for a minimum period of seven years. All information will be collated and summarised to provide relevant data for the next Management Review.

7.5 Hazard Identification and Risk Assessment

Responsibility: Technical & Compliance Manager

Description of Hazard Identification and Risk Management Process
The company use various means of Hazard Identification at the Company premises and on work sites.
Site Safety Inspections and Risk Assessments are completed and reviewed periodically to ensure that any new hazards introduced through changes to the organisational systems, new plant and machinery and products are assessed. The Risk Assessment process should include consultation with workers or other individuals involved with the area being assessed.
Generic risk assessments shall be available for most of the standard work activities and where appropriate site or task specific risk assessments will also be completed. No work should commence on site or tasks without suitable risk assessments being in place.
All Risk Assessments and significant findings from Risk Assessments are made available to all relevant interested parties who are also asked to contribute and participate with the Risk Assessment process.

Management of Change / Response to Unintended Change
Where any change, temporary or permanent, could impact on OH&S performance risk assessments will be completed prior to change, or as soon as is practicable in the event of unintended change, to mitigate any adverse effects as required. **Ref. 2.5 Risk Management**

Hazard Identification and Risk Assessment
Prior to completing work on a new site, location or new activity a Hazard prompt list risk assessment and / or task based risk assessment should be completed to identify and score significance of risks **(F-HS3 / F-HS14)**.
The following sources of information may also be utilised to identify hazards:

- Direct report from / consultation with workers, health and safety representatives or any other relevant persons;
- Industry and legislative requirements / guidance;
- Incident reports;
- Hazard inspection reports / Workplace hazard inspections;
- Observation of work tasks and activities;

When a potential hazard has been identified a Risk Assessment will be completed to assess the risk and identify the rating of the risk and any controls already in place or additional controls required to mitigate the risk.

Hazard & Risk Assessment Register
All identified hazards should be logged on Hazard Register **(ER14)**
Completed Risk Assessments should be logged on Risk Assessment Register **(ER14 / F-HS12)** detailing when last completed and any scheduled review date.

Plant Assessments
Hazard identification and risk assessments shall be completed for existing plant, the modification of plant or new plant or processes. A programme for maintenance and inspection of all plant used in the workplace will be established and maintained including a maintenance schedule. **Ref. 3.2 Management of Equipment and Premises.**

Safe Operating Procedures / Method Statements
Where required a Safe Operating Procedure / Method Statement detailing controls, safety equipment and safe method of work should be prepared.

Safety Inspections / Workplace Checking Procedure
Employers are required to assess the risks of the workplace and ensure appropriate First aid provisions. Workplace checks will be completed on a daily / weekly / monthly basis and documented as required **(F-HS8 / F-HS9)**.
The checklist will be analysed and will be included in the performance measurement. In addition any significant issues identified during checks should be reported **Ref. 5.2 Control of Nonconforming Outputs, Problems and Complaints.**
Safety Inspections are also completed periodically to identify potential workplace hazards.

SECTION 8 INFORMATION SECURITY MANAGEMENT

8.1 Commitment to Information Security Management

Responsibility: Managing Director

This information security management system (ISMS) is concerned with safeguarding information, no matter how or in what form the information is held, processed or shared. In addition to our own information we must also protect any information from external service providers, business partners, customers and many others. There are legal, commercial and business reasons for ensuring information security. Senior Management within the company recognise that information is a valuable asset and that it has to be protected, together with the systems, equipment and processes that support its use.

This ISMS includes all of the policies, procedures, plans, processes and practices detailed as well as the framework for identification and management and control of information security risks. In addition this ISMS also includes the registers listed in **Appendix i** and our **Statement-of-Applicability** which details the various controls in place including all the **ISO 27001:2013 Annex A** controls.

This ISMS has been implemented to ensure all important information is identified, that **Confidential** information is protected from unauthorised access, that the **Integrity** of all information is protected and that information is **Available** when required to ensure business continuity.

It is the responsibility of the responsible person listed above to ensure that this section of the management system and Information Security specific policies are followed. All managers and supervisors are responsible for their business areas, and all workers have a personal responsibility to ensure that they, and others, who may be responsible to them, are aware of and comply with the ISMS.

ISMS terms and definitions;

Term / Abbreviation	Definition
Access control	**Access control** includes both access authorisation and access restriction. It refers to all the steps that are taken to selectively authorise and restrict entry, contact, or use of assets.
Asset	In information security an **Asset** is anything that has value to the organization. This includes computers, databases, and software but the term can also include things like services, information, and people, and characteristics like reputation, company image or skills and knowledge.
Attack	An **attack** is any unauthorised attempt to access, use, alter, expose, steal, disable, or destroy an asset.
Availability	**Availability** is a characteristic that applies to **assets**. An asset is available if it is accessible and usable when needed by an authorised entity.
Business continuity	**Business continuity** is a corporate capability defined by ability to deliver products and services as normal after disruptive incidents occur.
Confidentiality	**Confidentiality** is a characteristic that applies to information. To protect and preserve the confidentiality of information means to ensure that it is not made available or disclosed to unauthorised entities.
Context	In ISMS an organisation's **context** includes all of the internal and external issues that are relevant to its purpose and the influence these issues could have on its ability to achieve the objectives and outcomes that its ISMS intends to achieve.
Control	A **control** is any administrative, management, technical, or legal method that is used to manage risk. Controls are safeguards or countermeasures. Controls include things like policies, procedures, rules, technologies and organisational structures.
Information processing facilities	An information processing facility is any system, service, or infrastructure, or any physical location that houses these things. A facility can be either an activity or a place and it can be either tangible or intangible.
Information security	**Information security** is about protecting and preserving the confidentiality, integrity, authenticity, availability, and reliability of information.
Information security event	An **information security event** indicates that the security of an information system, service, or network may have been breached or compromised.

Information security incident	An **information security incident** is made up of one or more unwanted or unexpected information security events that could very likely compromise the security of information and weaken or impair business operations.
ISMS	Information security management system
Integrity	To preserve the **integrity** of information means to protect the accuracy and completeness of information and the methods that are used to process and manage it.
Non-repudiation	**Non-repudiation** techniques and services are used to provide undeniable proof that an alleged event actually happened or an alleged action was actually carried out and that these events and actions were actually carried out by a particular entity and actually had a particular origin. **Non-repudiation** is a way of guaranteeing that people cannot later deny that an event happened or an action was carried out by an entity.
Owner	In the context of ISO 27001 an **owner** is a person or entity that has been given formal responsibility for the security of an asset. It does not mean that the asset belongs to the owner in a legal sense. Asset owners are formally responsible for making sure that assets are secure at all times.
Phishing	The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal confidential information such as passwords and credit card numbers
Requirement	A **requirement** is a need, expectation, or obligation. It can be stated or implied by an organization, its customers, or other interested parties. There are many types of requirements. Some of these include security requirements, contractual requirements, management requirements, regulatory requirements, and legal requirements.
Risk	In ISMS terms **risk** is usually defined in terms of the consideration of an event. Risk as based on probability and potential negative impact and cost. A high risk event would have both a high probability of occurring and a big negative impact if it occurred.
Risk acceptance	**Risk acceptance** is part of the risk treatment decision process. Risk acceptance means that you've decided that you can accept a particular risk.
Risk treatment	Risk treatment is a decision making process. For each risk, risk treatment involves choosing amongst at least four options; **1. Accept** the risk**, 2. Avoid** the risk, **3. Transfer** the risk, or **4. Reduce** the risk.
Stakeholder	A stakeholder is a person or an organization that can affect or be affected by a decision or an activity. Stakeholders also include those who have the perception that a decision or an activity can affect them.
Statement of Applicability (SoA)	**Statement of Applicability** lists the information security control objectives and controls for the organisation derived from the output of the risk assessment/ risk treatment plan. This is based on the list of suggested controls detailed in **Annex A of ISO 27001.**
Threat	A **threat** is a potential event that may cause harm
Vulnerability	A **vulnerability** is a weakness in an asset or group of assets. An asset's weakness could allow it to be exploited and harmed by one or more threats.

8.2 Information Security Arrangements

Responsibility: IT Systems Manager

8.2.1. Information Security Arrangements for Staff and other Personnel

Staff Awareness / Disciplinary Procedure

All workers are given information security awareness training and any workers who cause or commit a security breach will be subject to disciplinary action.

Contribution and Participation

An Information Security Governance Group has been established to facilitate contribution to the effectiveness of the ISMS. Meetings are scheduled regularly and documented.

Managing User Accounts, Leavers and Role Change

Ref. 3.1 Management of Staff and Company Personnel for further details of managing staff accounts / logins including staff leaving procedure.

User accounts are managed with details of all active user accounts maintained.

Staff leaving - access permissions will be deactivated if the member of staff leaves.

Staff moving - if a member of staff changes roles and has restricted access in old or new roles their access to restricted folders will be reviewed.

Access Control and Management of Logins

A register of relevant login accounts will be maintained and logins will be reviewed with every role change or if a staff member leaves.

Access to all systems with controlled information are monitored Use of privileged utility programmes and superuser accounts will be restricted and monitored as appropriate.

Ref. 8.5 - Access Control Policy.

Use of secret authentication information - in any circumstances where it may be necessary to validate the identity of a member of staff or other personnel the details held on their personal file should be used i.e. they should be asked to confirm date of birth and / or postcode. For higher security requirements a pass code will be setup and retained.

Ref. 8.5 - Use of Secret Authentication Information Policy

Confidentiality / Non-Disclosure Agreements

All workers / contractors who are required to access confidential information are required to sign non-disclosure or confidentiality agreements (this may be included in contract / processing agreement).

8.2.2. Information Security Arrangements for Management of Data and Information

Acceptable use of Information Assets

Information assets are identified and managed to ensure they are adequately protected with checks completed on an ongoing basis. Assets must be used in accordance with company policies and procedures.

Information Assets & Data Classification - Data assets are listed on the **Information Security Risk Assessment** including data classification, protection and owner. The owner is responsible for restricting access as required.

Documents that include sensitive or confidential information will be marked ***'Confidential'*** in the document footer and stored securely. Documents for business use will be marked ***'Business Use'*** and public documents marked ***'Public'.***

Protected **(Confidential)** information assets must be held securely to prevent unauthorised access and must not be taken off-site or disclosed to any other person or organisation without prior authorisation and adequate protection measures must be in place.

Ref. 1.5 Management of Documented Information and Data

Ref. 8.5 - IT Equipment Policy, Information Classification and Protection Policy

Data Backup Business Continuity / Disaster Recovery

Data backup systems are in place and continuity arrangements are summarised in F-IMS21 Business Continuity Register

Ref. 8.5 - Data Backup Policy

8.2.3. Information Security Incidents - Ref. 5.2 Control of Nonconforming Outputs, Problems and Complaints
All significant information security weaknesses or events are logged on the **Issues Register**. If the event or incident is serious, Senior management must be immediately informed and all work on systems affected by the issue will be suspended or controlled to ensure the issue is contained. Any evidence relating to the event or incident shall be compiled and retained for review.

8.2.4. Information Security arrangements with third parties
Communications / Information Transfer
Details of authority and responsibility for communications detailed in **3.3 Management System Communication.**
Protected information must not be shared without authorisation and use of IT and communications facilities must be in accordance with information security procedures to ensure adequate protection of information is in place during transfer. Where required a formal data transfer and processing agreement will be prepared covering the secure transfer of information with approved 3rd parties.
Ref. 8.5 - Communications Policy, Information Transfer Policy, Internet / Electronic Messaging Policy

Information Security in Supplier Relationships
Suppliers or any other party who can access, store, communicate or provide IT infrastructure components for any information assets will have information security requirements agreed and documented. The documented agreement will include details of controls related to any information security risks identified. Ongoing services will be monitored to ensure effective management of changes and reappraisal of risks.
All interactions with any other organisation or outside entity involving non-public information assets are subject to the scope of this Information Security Management System and are covered by our operational procedures.
Ref. 4.2 Control of Purchasing and Outsourced services.
Ref. 8.5 - Supplier Security Policy

8.2.5. Information Security Software and Systems
Management of Software
IT Systems maintenance are responsible for installation of all software and maintenance of list of approved software / purchased licences **(ER10)**. Users with administrator privileges may install approved software on their allocated device(s). If software not currently approved is required the Information Security Lead should be notified to complete an appraisal and approval of the Software prior to use.
Ref. 8.5 - Software Policy, Anti-Malware Policy

System acquisition, development and maintenance
Any changes to IT system will be planned and monitored as per change control procedure **Ref. 4.4 Management of Change, Variations and Design** and consideration of information security across the system development life cycle will be paramount in any development. Any development that is outsourced will only be completed by an approved contractor and monitoring, testing and acceptance criteria will be established. When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security. Modifications to software packages must be approved by Information Security Lead.
Ref. 8.5 - Secure development Policy

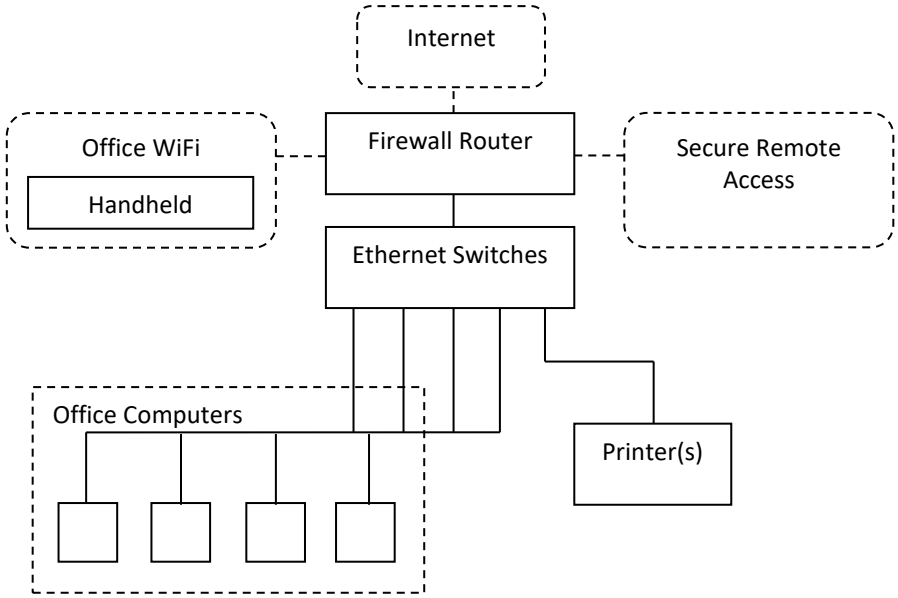
Cloud Computing Systems
Risk assessments should be completed and reviewed periodically to identify and review risks associated with cloud computing. Only approved cloud computing services can be used and will be reviewed for security and suitability prior to approval. What data can be stored in the cloud will be documented.
Ref. 8.5 - Cloud Computing Policy

8.3 IT Equipment and Physical Security

Responsibility: IT Systems Manager

8.3.1 Network Management and Infrastructure

Basic Diagram



Network Monitoring and Maintenance

Network monitoring software is used to monitor network traffic on an ongoing basis and log reviewed and any suspicious activity investigated and if relevant logged as a security incident.

8.3.2 IT Equipment

All IT equipment used to hold or access company data is listed on **Asset Management List (SharePoint)**
This equipment register is the physical asset register used in the risk assessment process. All equipment is uniquely identified and location and owner recorded. Logins used to access network or web based resources are also logged.
Ref. **3.2 Management of Equipment, 8.5 - IT Equipment Policy.**

Systems Monitoring

Audit completed at least annually of IT systems; Software licensing, Antivirus / Firewall and other checks.
Other monitoring and checks are detailed on **Information Security Risks** and checks documented using **F-Q25 IT Systems Monitoring / F-Q26 Premises Monthly Checklist** if required.
Event logs detailing user activities any other significant events are reviewed on an ongoing basis and retained.

Handheld Devices / Laptops / Workstations

All equipment used to access company files must be password protected. Equipment removed from the premises must be encrypted or set to not store any files on the device.
Ref. **8.5 - Mobile Device Policy.**

Management of Removable Media

Any removable media used to store confidential information should be protected and if to be removed from the premises must be encrypted. Only removable media approved and supplied by the organisation may be used. Where there is a risk of unauthorised transfer of files to removable media external ports will be removed / deactivated and equipment locked.

Encryption and Encryption Key Management

To ensure information transmitted over public networks or stored on media devices is secured encryption is used to secure this data. Details of encryption used and management of encryption keys detailed on **ER10.**
Ref. **8.5 - Cryptographic Policy.**

8.3.3 Physical Security

Access to the premises is controlled. The office is kept locked at all times and details of all equipment issued, including office keys, is recorded on the Equipment issued register.

All visitors are escorted throughout the premises and accompanied at all times. Premises will be locked when not in use and all confidential documents are stored securely.

Ref. **IT Equipment Policy**

Confidential Documents

All confidential documents are locked away when not being used as per our **Clear Desk / Screen policy**. Any confidential waste is shredded.

Ref. **Clear Desk / Screen Policy**

Disposal of Media Equipment

Any media equipment will be disposed of using approved contractor for secure disposal of IT equipment and details of company will be held on file / added to approved supplier list to ensure secure destruction and compliance with WEEE and other environmental regulations. Equipment list should be updated once equipment disposed of.

Cabling Security

Ongoing checks should be made of cabling to ensure cabinets are locked and no evidence of any tampering with network cables.

8.3.4 Other Security Arrangements

Password Security

All workers must read and follow the password policy which details arrangements for password security including use of secure passwords, regular changing of passwords, protection and management of passwords.

Ref. **Password Policy**

Management of Technical Vulnerabilities

The Information Security Lead is responsible for the identification of technical vulnerabilities with the information systems which should be logged on **Information Security Risks** with details of measures taken to address any risk associated with the identified technical vulnerability.

Penetration Testing

Penetration testing is completed on an ongoing basis with frequency determined by risk and data security requirements. Where possible this is completed by an independent 3rd party.

Ref. **8.5 - Technical Vulnerability Management Policy**

Remote Working / Security of Equipment and Assets off-premises

Any remote working that requires access to protected information or taking off-site of any assets that hold or can access protected information requires prior approval and authorisation and all necessary information security controls must be in place for remote working.

Ref. **Teleworking Policy.**

Cyber Crime Attacks

All workers should be aware of the risks and actions to take if a cyber crime attack is suspected or detected. All such attacks must be logged and investigated.

8.4 Information Security Risk Management

Responsibility:

8.4.1. Risk Assessment Methodology

Risk assessments are completed to identify and document all the IT Security risks faced by the organisation. Risk assessments will consider all IT equipment and information assets (**ER10 & F-IMS25**), vulnerabilities and all potential threats including internal and external threats.

As well as consideration of IT equipment and information assets all logged issues / actions, problems and IT Security incidents are also taken into account when identifying risks (**Issues Register**).

8.4.2. Risk Assessment

All identified risks are documented on the **Information Security Risks Register** with summary of the risk, potential consequences and a Risk Level score based on likelihood and level of harm. Risk owner is also identified.

Current Controls

Controls in place to reduce or manage the identified risk are detailed in **Information Security Risks Register** as well the residual Risk Level.

If the Risk Level after taking the controls into account is unacceptable then it should be raised as problem as per **5.2 Control of Nonconforming Outputs, Problems and Complaints** and additional Risk Treatment plan prepared and actions taken to reduce risk to acceptable level.

decision

All Risks assessed and listed on Information Security Risks Register?

No

YES

Review risks and update **Information Security Risks Register**

8.4.3. Risk Treatment Plan

Risk Mitigation options include **1. Transfer the risk** (appoint 3rd party to manage), **2. Reduce** - control measures put in place, **3. Avoid** - review activities to avoid being exposed to this risk or **4. Accept** the risk if no further risk mitigation is practicable

Risk treatment actions will be logged on issue tracker / risks register **Information Security Risks Register.**

Once treatment plan has been completed the risk owner must give approval that residual risk is acceptable.

decision

All Risks reduced to acceptable level?

No

YES

Further actions necessary - raise any new actions and return to 8.4.2 once completed.

8.4.3. Risk Review

The Information Security Risks Register, IT Security Incidents and any relevant findings from Internal audits should all be reviewed and residual risks identified on the Risk Register are approved during management review.

8.4.4. Monitoring, Measurement, Analysis and Evaluation

Based on risk the organisation has determined what needs to be monitored and measured. The methods for monitoring, frequency and person responsible are outlined in **Information Security Risks Register**.

All risks and monitoring activity will be reviewed on an ongoing basis and formally reviewed, at least annually, during management review.

8.5 Information Security Procedures and Policies

Responsibility: Technical & Compliance Manager

The following policies relate to Information Security Management and are part of this ISMS.

Details	Relevant Policy / Policy-Procedure
IT Equipment Policy Software, physical security use and disposal of IT equipment.	**PIP 82 – Asset Management**
Clear Desk / Screen Policy Physical security of workstations and paper documents.	**PIP 86 – Clear Desk**
Password Policy Password security and management of passwords.	**PIP 90 – Network Access Control**
Teleworking Policy Remote working and remote access of information.	**P-28 Teleworking Policy**
Mobile Device Policy Controls for mobile devices.	**P-29 Mobile Device Policy**
Cryptographic Policy Use of encryption to protect information.	**PIP 87 - Cryptography**
Communications Policy Management of internal and external communications.	**PIP 28 – Communications and Consultation**
Data Backup Policy Management, testing and restoration of backups.	**PIP 88 – Information Backups**
Anti-Malware Policy Malware protection and prevention.	**PIP 95 – Virus Protection**
Software Policy Control of software and associated risks.	**PP-8-03 Software Policy Procedure** **P-38 Software Installation Policy**
Access Control Policy Access control, user accounts, physical access.	**PIP 81 – Building Physical Security** **PIP 90 – Network Access Control**
Internet / Electronic Messaging Policy Management of Electronic messaging and associated risks.	**PIP 83 – Acceptable Usage**
Information Transfer Policy Management of risks associated with information transfer.	**PP-8-06 Information Transfer Policy Procedure** **P-39 Information Transfer Policy**
Technical Vulnerability Management Policy Management of Technical Vulnerabilities.	**PIP 94 – Technical Vulnerability & Patch Management**
Cloud Computing Policy Use of cloud computing and controls	**PP-8-09 Cloud Computing Policy Procedure**
Use of Secret Authentication Information Use and management of secret authentication information.	**PIP 87 - Cryptography**
Supplier Security Policy Management of risks associated with outsourcing.	**PIP 09 – Control of Suppliers and Contractors**
Information Classification and Protection Policy Data classification and storage based on classification.	**PP-8-12 Information Classification and Protection Policy Procedure**

SECTION 9 Business Continuity Management

It is our policy to ensure all necessary arrangements are made for maintaining normal business operations and continuity of service. Continuity of service is of critical importance which is why comprehensive Business Continuity Plans have been developed to ensure adequate arrangements for business continuity in response to any unplanned incidents that could affect normal operations are in place. This also includes a comprehensive strategy for the consideration and avoidance of disruptive incidents and consideration of business continuity is incorporated into overall management systems.

Disruptive Incidents

A disruptive incident is defined as any unplanned event that can affect or prevent the us from providing or continuing with normal provision of services. Some incidents may be entirely out with our control but consideration is still required to ensure adequate provisions are in place for recovery of operations.

Business Continuity Arrangements

Continuity arrangements are documented and included as part of our overall management systems and are continually reviewed and tested.

Continuity arrangements include;

- Overview of Continuity Responsibilities;
- Provision of resources and training required for ensuring continuity;
- Emergency Recovery Teams - details and responsibilities;
- Business Continuity Procedures including detailed arrangements for activation of continuity plans / emergency response;
- Business Continuity / Disaster Recovery Plans;
- Risk Register which includes review of potential disruptive incidents and Business Impact Analysis;
- Procedures for ongoing testing of business continuity arrangements.

Business Continuity Management

A Business Continuity Lead has been appointed and they are responsible for reviewing and maintaining overall business continuity arrangements, business continuity objectives and achieving continual Improvement of continuity arrangements.

APPENDIX i MANAGEMENT SYSTEM REGISTERS

The below registers form a key part of the Integrated Management System

IMS Registers

Details	File Location
F-IMS20 - Document Register Document Register	**\1 - IMS Documentation\IMS Registers**
F-IMS21 - Business Continuity Register Continuity / Backup / Disaster recovery overview	**\1 - IMS Documentation\IMS Registers**
F-IMS22 - Interested Parties Listing of Interested Parties	**\1 - IMS Documentation\IMS Registers**
F-IMS23 - Opportunities Risks Register SWOT analysis / Overall Risks Register	**\1 - IMS Documentation\IMS Registers**

Environmental Registers

Details	File Location
F-ENV2 - Waste Matrix Overview of waste and disposal	**\11 - Environmental Records**
F-ENV4 - Environmental Aspects Register Environmental Impacts Register	**\11 - Environmental Records**

Health & Safety Registers

Details	File Location
ER14 - Hazard Risk Assessment Register Overview of Hazards and Risks	**\6 - Audits and Monitoring**

Information Security Registers

Details	File Location
F-IMS25 - Information Assets Register Listing of Information Assets	**\1 - IMS Documentation\IMS Registers**
F-IMS26 - Statement of Applicability **Information Security** controls in place including all the ISO 27001:2013 Annex A controls	**\1 - IMS Documentation\IMS Registers**
ER10 - IT Equipment Logins Register IT Equipment and logins	**\8 - Equipment**
ER15 - Information Security Risks Register Information Security Risks Register	**\1 - IMS Documentation\IMS Registers**

Business Continuity Registers

Details	File Location
Business Impact Analysis and Risk Assessment Overview of Hazards and Risks	
Business Critical Function Analysis	