Information Security Management System Scope

ISO27001:2022

Information Security in all aspects of Security & Fire Detection Systems

Document Details

Title	Scoping Document
Date of Issue	06/2023
Authorised By	Andrew Matthews

Version	Date	Comment on change
1.0	June 23	First Issue
1.1	July 23	Minor changes

Contents Table

1 Scope of the ISMS

The scope of this management system is:

The information security management system relating to the installation, configuration, commissioning, integration and maintenance of Security & Fire Detection Systems to public and private sector organisations and services tailored to client's specific requirements. This is in accordance with the latest version of the Statement of Applicability.

2 Corporate Overview and Context

ASL have been operating internationally out of Birmingham since 1999 and have expertise in all aspects of installation, programming, commissioning, integration and maintenance of Security & Fire Detection Systems. ASL have a long-standing relationship with a wide range of public and private sector organisations and offer a wide range of services tailored to client's specific needs.

To support the management of the security of information, ASL has taken the step to implement an information security management system (ISMS) against the requirements of ISO27001:2022 to ensure that confidentiality, integrity and availability, integral to our business, services and products are managed and preserved.

The ISMS applies to all information assets used or supported by ASL throughout its business. This includes the supply, installation and maintenance of Security & Fire equipment as well as Specialist Support Services offered by ASL.

The sectors in which ASL operate include:

- Infrastructure and Utilities
- Retail
- Stadiums
- Education
- Commercial
- Charities

This Scoping Document gives a broad overview of the management system in context to ASL.

The locations of our premises are:

19 Chelmsley Wood Industrial Estate,
Waterloo Avenue
Birmingham
B37 6QQ

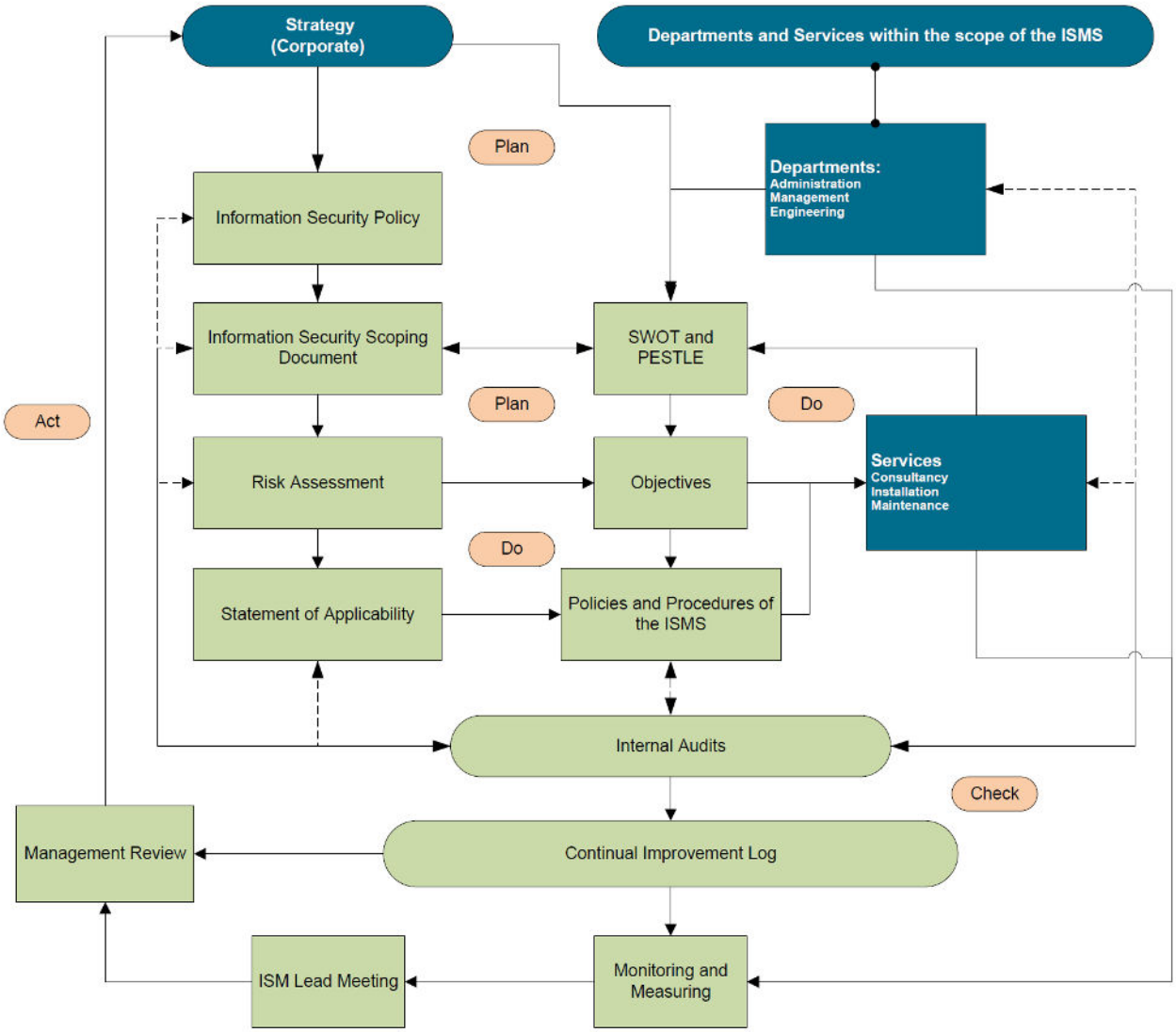
3 Interested Parties and their Needs

ASL have determined the interested parties that are relevant to the Information Security Management System and defined the needs and expectations of these parties as defined below:

Interested Parties	Interest	Expectations of interested parties	Expectations of ASL
Employees (Internal)	Responsible for service delivery, ASL reputation and image Handling of small amounts of information	Provided with correct information for task. Correct tools and equipment. Continued payment/job, paid, development and training	Information is held correctly and managed. Loyalty and trust in employee, 100% output, image and reputation positivity
Shareholders/ owners of the business (Internal)	Financial growth Reputational	Key for the business to operate securely in all aspects. ISMS, delivery of service etc.	Provide shareholders and management with confidence and demonstratable improvements to the way in which the business operates
Landlord	Income generation	Sustainable income and keep unit in good state of repair	Retain lease and cooperate with building regulations and changes
Government agencies/regulators (External)	Securing information and improving security	Service providers to national infrastructure requires levels of protection and controls - demonstratable evidence required in certain circumstances Reporting of incidents and experiences	Support from government agencies and technical partners. Relationships building and networking to improve controls and response to incidents
Certification bodies (External)	Continuity of improvement, engagement, understanding of requirements	Continuation of relationship, continual improvement, progression in standards	Continual improvement, engagement rather than enforcement
Media (External)	Looking for interesting news and stories	Positive and negative media attraction	Reputational issues relating to media use
Suppliers and partners (External)	Supply of goods and services	Longevity, correct information, and storage of information	Relationship, longevity, confidence, trust
Retail Clients	Receive service	Timely service, low cost, QUENSH, secured information ISO27001 principles, Cyber Essentials, SSAIB	Customer Satisfaction, Excellent Relationships
Infrastructure Clients	Receive service	Timely service, low cost, QUENSH, secured information ISO27001 principles, Cyber Essentials, SSAIB	Customer Satisfaction, Excellent Relationships, Trust

All of the needs and expectations in the table above are expected to be supported by the Information Security Management System and the requirements of ISO27001

Interaction Map:



4 Leadership Commitment

ASL's top management team are committed to the development and implementation of an ISMS which is compatible with the strategic direction and context of the organisation, the whole system is frequently reviewed to ensure conformance with ISO/IEC 27001:2022 standard. Responsibility has been assigned to ensure that the business conforms to the requirements of the standard.

The Managing Director at ASL will ensure the staff are aware of the importance of meeting customer requirements as well as the statutory and regulatory requirements. The Managing Director is responsible for ensuring the ISMS objectives are aligned to the organisation's strategic direction.

The Senior Management Team will ensure:

- The Company has a designated management representative who is responsible for the maintenance and review of the ISMS. Namely the Operations Manager.

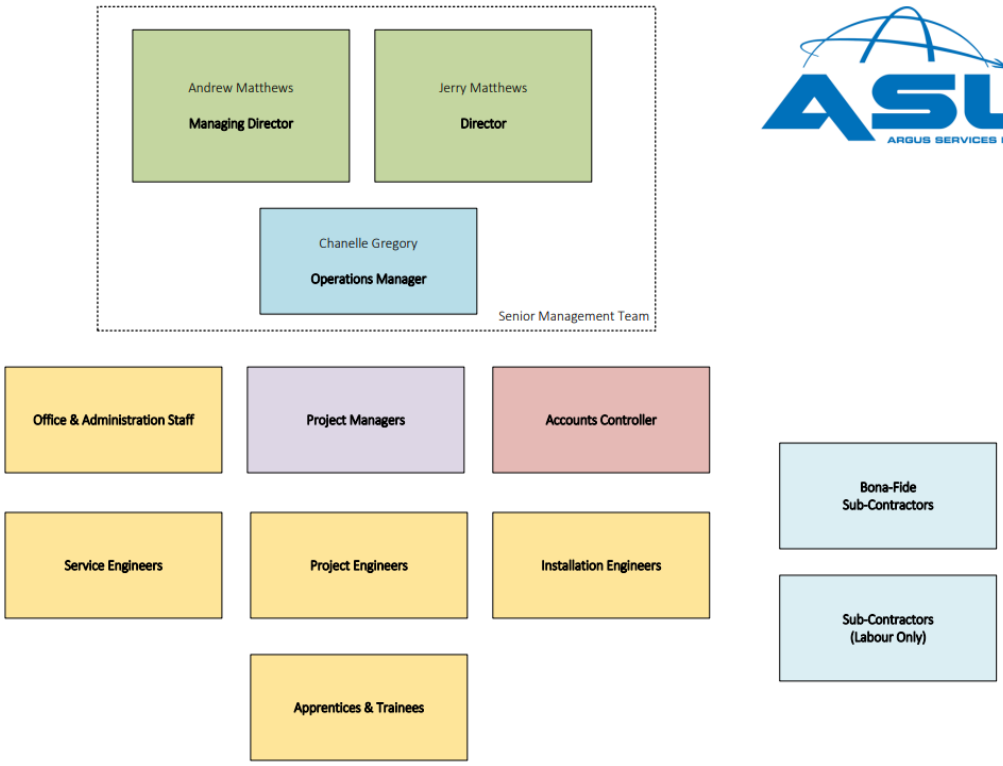
- The Company has a designated management representative who is responsible for the implementation of the ISMS and the technical controls. Namely the Managing Director.
- Ongoing activities of ASL are reviewed regularly and that any required corrective action is adequately recorded, implemented and review to establish an effective preventative process.
- Resources needed for the ISMS are available and employees have the necessary training, skills and equipment to effectively carry out their work.
- Internal audits are conducted regularly to review progress and assist in the improvement of processes and procedures.
- Objectives are reviewed and, if necessary amended, at regular management review meetings and the performance communicated to all staff.
- The information security policy and objectives are established in line with the strategic direction of the organisation and that intended outcomes are achieved.
- Communication covering the importance of effective ISMS and conformance to ISMS requirements are in place.
- Continual improvement promoted.
- The risks and opportunities that can affect conformity of services and the ability to enhance customer satisfaction are determined and addressed.
- The focus on consistently providing services that meet / exceed customer and applicable statutory and regulatory requirements are maintained.

5 Roles and Responsibilities of Information Security

To ensure that ISMS activities are coordinated and executed in compliance with the Information Security Policy and associated management system requirements, the following roles and responsibilities have been assigned to representatives of ASL:

Information Security roles, responsibilities and authorities have been assigned to ensure the continuing maintenance and improvement of the ISMS.

- **ISMS Organisational Chart**



Role	Responsibility	Authorised to:
Managing Director	• Overall responsibility for the ISMS • Providing strategic direction • Attending management review meetings • Provision of resources required by the ISMS	• Approve significant changes to the ISMS • Approve budgets & spends for the ISMS • Invoke BCP arrangements • Refer for disciplinary action
Directors	• Day – to – day management and oversight of effectiveness of the ISMS • Identification & treatment of information security risk • Management of ISMS objectives • Management of ISMS measurement & monitoring activities • Creation & maintenance of ISMS documents & records • Management of incidents, events & weaknesses	• Approval of changes to ISMS documentation • Liaise / communicate requirements of the ISMS to employees • Liaise / communicate with third parties in relation to the requirements of the ISMS • Invoke BCP arrangements in the absence of the COO

	• Management of corrective actions (audit & incident) • Chair management review meetings • Hosting of internal & external auditors • Management of the ISMS internal & external audit schedule & audit results •	• Approve, amend, or deny recommendations of Risk Board
Directors	• Periodic review of ISMS risk landscape • Attendance at risk review meetings • Management of actions as a result of risk assessment (at board level) • Creation & monitoring of risk reports • Communication of risk levels & mitigations to employees they affect	• Follow up and implement agreed risk mitigation plans
Legal Team (Senior Management Team)	• Identification of applicable legislation & guidance • Maintenance & updates to legal register • Evaluation of legal compliance • Communication of legal changes & updates	• Reporting to authorities in the event of a data breach which involves personal data • Reporting to police where criminal activity is suspected • Speak to the media in the event of an incident
IT Team	• Log, respond & correct information security incidents • Identify & manage change requests • Manage access provisioning, changing & revoking requests • Manage software licensing • Managing operational network & applications	• Use privileged utility programs
ISMS Auditors	• Conduct audits as per the Internal Audit Schedule • Identification of nonconformity & opportunities for improvement • Creation of internal audit reports	• View confidential or sensitive data for the purposes of audit sampling
All Employees	• Adhere to all ISMS policies & procedures • Report information security events, weaknesses & incidents • Attend ISMS awareness training and complete knowledge checks when required • Protect ASL systems from unauthorised access and improper use	• Carry out business functions in line with ASL policies and procedures

ASL have several policies specific to employee responsibilities in certain areas of the business such as, Acceptable Use Policy for IT Devices and Information which is communicated to relevant staff. Each employment contract also states that the employee has responsibilities to keep data and information relating to ASL and/or its customers confidential.

The management team at ASL help to reduce the risk of disruption of business operations by providing advice and support on all aspects of security including:

- Security Awareness
- Data Confidentiality and Privacy
- Logical Access
- Data Communications
- Systems and Data Integrity
- Physical Security
- Personal and Procedural Controls
- Contingency planning

All Staff

ASL sees that all employees have a responsibility for ensuring Company systems and data are protected from unauthorised access and improper use. If an employee is unclear about any of the security policies and procedures, they are advised to seek advice and guidance from their manager. Information Security and the appropriate protection of information is the responsibility of all users and individuals are always expected to act in a professional and responsible manner. Staff shall ensure that they understand their role and responsibilities, and that failure to comply with this policy may result in disciplinary action. This will be reinforced by yearly mandatory training / awareness.

6 Contact with Authorities and Special Interest Groups

The Senior Management Team are responsible for contacting authorities in the event of a data breach which is deemed reportable under ICO rules. The Legal Team are also responsible for making reports to police where criminal activity is suspected.

Appropriate contacts are maintained with the following service

- Internet Service Provider – Directors
- Hardware – Directors
- Utilities – Operations Manager
- Local authorities – Operations Manager

Responsibility for any other services which fall under the information security preview, but not mentioned above would be assigned to the Senior Management Team. This is necessary to ensure that appropriate actions can be promptly taken, and advice obtained in the event of any security incident. Management are consulted on all third-party contracts and agreements.

7 Monitoring, Measurement, Analysis & Evaluation

Various monitoring & measurement activities are conducted to continually monitor the performance of the ISMS (IT Monitoring Tasks Schedule).

The I.T. team will perform analysis on the monitoring activities in order to identify trends. Trends may be noted within the risk register and reviewed by the risk board for further action, and will highlight trends and proposed or implemented corrective actions in management reviews.

8 Threat Intelligence

To ensure that the organisation keeps up to date with the information security threat landscape, the Operations Manager and the Service Manager monitors information services including:

- NCSC news - NCSC.GOV.UK
- Latest Warnings – Krebs on Security

Additionally, Windows Defender is operating across the network to identify threats to ASL systems and services and provide alerts and continual threat monitoring.

Newly identified threats which pose a risk to the organisation are reviewed by the Operations Manager and the Service Manager and added to the risk assessment. The Operations Manager and the Service Manager will assess the risk and assign security controls in order to reduce the chance of the threat becoming an event. The Operations Manager and the Service Manager will ensure that newly identified threats are reported to the wider management team during risk reviews.

9 Risk

Two risk assessment approaches have been used in this management system:

- SWOT and PESTLE have been used to identify the internal and external issues that could impact the effectiveness of the ISMS to deliver expected outcomes.
- Information and Data Risk Assessment has been used to assess the risks associated with the loss of confidentiality, integrity and availability for information within the scope of this ISMS.

10 Management Review

Management review is conducted at planned intervals and follows a set agenda which can be added to as required. The results of management reviews shall be documented and include decisions made in relation to continual improvement any changes to the ISMS.

11 Principles of Information Security Management

ASL has developed an ISMS around the requirements of ISO27001:2022 and understands that information takes many forms and includes data printed or written on paper, stored electronically, transmitted over computer networks, by post or using electronic means, stored on all removable digital media and video tape as well as spoken in conversation.

The protection of information is central to the requirements of this management system. Whilst information can be written on paper, stored electronically, transmitted by mail, by electronic means, or spoken in conversation, the management system goes beyond this to ensure the confidentiality, integrity and availability of information.

Confidentiality

The information, in any form, while in storage, being processed or communicated, should be protected to ensure it is only available to those that are authorised by the organisation and/or the information owners to have access to, and use of, the information.

Integrity

This is about ensuring that information in storage, being processed or communicated is accurate and complete; that it is correctly processed and has not been modified in any unauthorised way. The integrity of the networks and information systems that they connect to are also important to ensure that these are what the organisation intends them to be.

Availability

This is about ensuring that information is available to the organisation and its users who are authorised to have access to it, when and where they need to use and process it. In practice, Argus Services Ltd has established a system of controls to ensure that information continues to be available for those who are authorised to use it.

12 Key Applications and Systems

Key Applications and Systems used to support services include:

Application / System	Purpose	Location
Sage Line 50	Accounts	On-prem
BigChange	Service Management System	Cloud
Microsoft 365 Apps	MS Applications	On-Prem on endpoint devices
Microsoft 365 Defender and Intune	Anti-malware & MDM	Cloud and endpoint devices
Acrobat Reader	PDF Viewer	
Chrome	Web Browser	
Avigilon Control Centre	CCTV Software	On-Prem and cloud
BlueBeam Revu	PDF Editor	
WinPak 4.4	Access Control Software	On-Prem
SharePoint	Business Documentation and Records	
TeamViewer	Remote access and administration, cloud backup, system monitoring	Cloud and on-Prem on endpoint devices

13 Services/Products

The services of Argus Services Limited (ASL) are fully defined on the company's website

14 Exclusions from Scope

All exclusions from the management system have been identified in the current Statement of Applicability (SoA). Employees work a hybrid of home and office and whilst the assets used by employees are within scope their homes are not within scope of the ISMS but there are policies are in place in respect of the management and security of information in a hybrid environment.

15 References

ISO27001:2022 Information security management systems requirements
ISO27002:2022 Code of practice for information security controls in ISO27001