spark GROWTH SOLUTIONS

FACT SHEET

ISO 27001:2022

What does my business need to do?

ISO 27001:2022 Information Security Management Systems is the standard that is becoming increasing essential for organisations that manage sensitive data on behalf of their customers. The increasing sophistication of malicious attacks on data security is driving organisations to require their suppliers to demonstrate a systematic and comprehensive approach to the management of information security.

As with all the ISO management system standards, it creates a "closed loop" so that the business learns quickly for its mistakes and reduces the potential that they make the same mistakes again. It is structured on the simply but effective improvement loop:

Plan – planning to deliver for customers and the business.

Do – implement the plan in a systematic way.

Check – check that the system is working.

Act – fix issues as well as identify and implement improvements.

It also ensures that your information security is comprehensive whilst being conducted is a consistent and systematic may to give greater certainty on the results achieved.

The clauses of the ISO 27001:2022 are explained below and gives you a good idea of what you needs to have in place to achieve certification.

CLAUSE 4.1 - UNDERSTANDING THE ORGANISATION AND ITS CONTEXT

The business demonstrates that it understands, monitors, and reviews the internal and external factors that influence the outcomes achieved by the information Security Management System.

CLAUSE 4.2 - UNDERSTANDING THE NEEDS AND EXPECTATIONS OF INTERESTED PARTIES

The understanding, monitoring and review of the key groups of people (e.g., customers, suppliers, regulators, staff) that influence our business and its Information Security Management System.

CLAUSE 4.3 - DETERMINING THE SCOPE OF THE QUALITY MANAGEMENT SYSTEM

The scope of the Information Security Management System is documented and takes account of the internal and external issues, needs of interested parties and the interfaces and dependencies between the business and others.

CLAUSE 4.4 - INFORMATION SECURITY MANAGEMENT SYSTEM

An Information Security Management System has been developed, implemented, maintained, and continually improved by the business.

CLAUSE 5.1 – LEADERSHIP AND COMMITMENT

Top management are committed to the system as demonstrated by:

- The information security policy and objectives are compatible with the strategic direction of the business.
- Integration of the system into business processes.
- The system is adequately resourced to achieve its objectives
- Direction and support to those who contribute to system effectiveness
- Promoting continual improvement.

CLAUSE 5.2 – POLICY

The business has an Information Security Policy that:

- Is appropriate to the business context and strategy.
- Commits to continual improvement.
- Provides a framework for setting quality objectives
- Is communicated, understood and applied.
- Available to interested parties.

CLAUSE 5.3 – ORGANISATIONAL ROLES, RESPONSIBILITIES AND AUTHORITIES

The business has assigned responsibilities and authorities to roles that:

- Ensure the system meets ISO 27001:2022
- Report on system performance and opportunities for improvement

CLAUSE 6.1 - ACTIONS TO ADDRESS RISKS AND OPPORTUNITIES - GENERAL

The business has understood the risks and opportunities and has implemented plans to:

- Ensure the system achieves what is intended.
- Desirable outcomes are more likely.
- Undesirable outcomes are reduced or eliminated.
- Improvements are identified and acted upon.

CLAUSE 6.1.2 - ACTIONS TO ADDRESS RISKS AND OPPORTUNITIES – INFORMATION SECURITY RISK ASSESSMENT

The business has an information security risk assessment process that includes the following characteristics:

- Establishes criteria for risk acceptance and for performing risk assessments.
- Produces consistent produces valid, consistent and repeatable results every time.
- Identifies information security risks that impact confidentiality, integrity and availability as well as the owners of those risks
- Analyses likelihood and consequence to determine the level of risk.
- Prioritises treatment by evaluating information security risks and comparing the risk rating to the risk criteria.

CLAUSE 6.1.3 - ACTIONS TO ADDRESS RISKS AND OPPORTUNITIES – INFORMATION SECURITY RISK TREATMENT

The business has an information security risk treatment process that includes the following characteristics:

- Selects risk treatments options based upon their risk assessment
- Determines the risk treatments choses and ensures they are comprehensive by comparing them to Annex A of ISO27001:2022.
- Maintains a Statement of Applicability that justifies the risk controls and any exclusions to the risk areas contained in Annex A of SIO27001:2022.
- Formulates a security risk treatment plan.
- Approval of risk owners of the treatment plan and of the residual risk

CLAUSE 6.2 – INFORMATION SECURITY OBJECTIVES AND PLANNING TO ACHIEVE THEM

The business has developed, communicated, and regularly reviews its information security objectives. These objectives are consistent with the policy as well as being measured (where possible) and take account of the outcomes of the risk assessment and treatment process.

The business has developed and implemented plans to achieve the objectives with actions, resources, responsibility, date of completion and evaluation criteria.

CLAUSE 6.3 - PLANNING OF CHANGES

Changes to the ISMS need to be carried out in a planned manner.

CLAUSE 7.1 – RESOURCES

The business has determined and provided the people, infrastructure, and environment to implement and improve the system to ensure it meets requirements.

CLAUSE 7.2 – COMPETENCE

The business has determined the competencies (qualifications, skills, and experience) that affects its information security performance. The business recruits new or trains existing staff to ensure these competencies are available and evaluate the effectiveness of recruitment or training.

CLAUSE 7.3 – AWARENESS

The business has ensured that staff, contractors, and suppliers understand the information security policy and objectives, their role within the system and their impact on information security performance.

CLAUSE 7.4 – COMMUNICATION

The business understands what information is communicated to whom, the person responsible for each communication, how they will communicate and when it will be communicated.

CLAUSE 7.5 – DOCUMENTED INFORMATION

The business has the documented information required by the standard and the documented information necessary to understand the effectiveness of its system. This includes a procedure that covers how system documents are created, their format, reviewed and approved for use. The business also has documented how it:

- Provides access
- Protects it (e.g. authentication and back ups)
- Stores it (e.g. filing system and server or cloud based environment)
- Control of changes
- Determines what is retained and for how long (how it is disposed of)
- Legislation, regulations, standards, codes and other external requirements are made available and kept up to date

CLAUSE 8.1- OPERATIONAL PLANNING AND CONTROL

The business has documented evidence that is has implemented and controlled its processes including:

- Establishing criteria for processes and implementing according to these criteria.
- Implementation of the actions in our Statement of Applicability (Section 6.1) to meet our information security requirements.
- Achieving our information security objectives (Section 6.2)
- Control changes through planning as well as reviewed the consequences on unintended changes to mitigate adverse effects.
- Ensuring that outsourced processes are known and controlled.

CLAUSE 8.2 – INFORMATION SECURITY RISK ASSESSMENT

Information security risk assessments are being performed at planned intervals and when significant changes occur. We can produce evidence that these are being done.

CLAUSE 8.3 – INFORMATION SECURITY RISK TREATMENT

The business has implemented its information security risk treatment plan and can produce evidence that it has been done.

CLAUSE 9.1 – MONITORING, MEASUREMENT, ANALYSIS AND EVALUATION

The business evaluates its information security performance and effectiveness of its information security management system including.

- Monitoring and measuring information security including processes and controls
- Monitoring and measuring methods produce comparable and reproducible results
- The timing and responsibility for monitoring and measurement
- The timing and responsibility for the analysis and evaluation of the results of this monitoring and measurement

CLAUSE 9.2 – INTERNAL AUDIT

The business must conduct internal audits at regular intervals to assess whether the information security management system is effectively implemented and maintained so that it conforms to the information security requirements of the business and ISO27001:2022. The business has a document that describes:

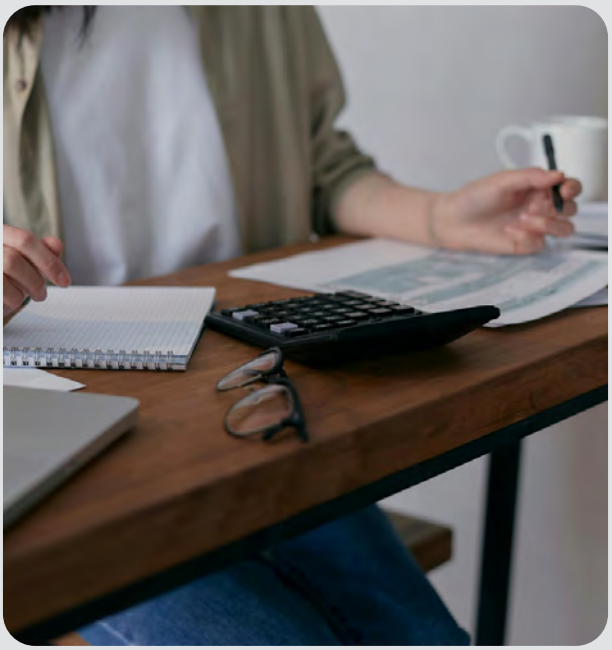
- Audit criteria including standard and your system requirements.
- Scope of each audit and methodology to be used
- Calendar of audit dates.
- Objectivity, impartiality and competency of the auditor.
- Reports are available for review by management.
- How issues are promptly fixed.

CLAUSE 9.3 – MANAGEMENT REVIEW

Top management of the business conducts at least an annual management review of the information security management system. This review must include:

- Status of actions from previous management reviews.
- Consideration of changes in the needs and expectations of interested parties relevant to the ISMS
- Internal or external changes relevant to the management system.
- Feedback on performance of the information security management system including non conformities, corrective actions, monitoring and measurement results, audit results (internal and external) and achievement of system objectives.
- Feedback from interested parties.
- Results of risk assessment and status of the risk treatment plan
- Ideas for improvement.

The outputs of the review need to include improvement plans, the needs for changes to the information security management system and any change required to resources.



CLAUSE 10.1 – NON CONFORMITY AND CORRECTIVE ACTION

The business has in place the means to identify a failure to meet the requirements (non conformance) to the requirements of the information security management system.

The business needs to have a process to address a non-conformance when it occurs – a corrective action process. The characteristics of this corrective action process includes:

- Review and analysis including the how common the issue is.
- The underlying cause (root cause) of the issue.
- Identify actions to fix the issue.
- Implement actions to fix the issue.
- Review the effectiveness of the action to fix the issue.
- Make changes to the information security management system, when necessary

The business needs to be able to prove that it has implemented a logical procedure with these characteristics and makes use of it.

CLAUSE 10.2– CONTINUAL IMPROVEMENT

The business needs to be able to demonstrate that it is continually improving its quality management system to minimise rework and maximise customer satisfaction.

ANNEX A – Reference Control Objectives and Controls

This Annex is an essential checklist of the ISO 27001:2022 standard for Clause 6.1.3 Information Security Risk Treatment.

To achieve certification the business will need to consider every one of these risks and controls through their Statement of Applicability.

The business cannot be certified without this essential piece of analysis and decision-making.

If the business excludes any of the risks and their controls, they need to be able to justify it. During certification, your auditor will review these decisions and may insist on their inclusion should they assess that it is relevant to the business.

A.5 ORGANISATIONAL CONTROLS

A5.1 - Policies For Information Security

A set of policies for information security shall be defined, approved by management, published, and communicated to employees and relevant external parties. The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.

A.5.2 - Information Security Roles & Responsibilities

All information security responsibilities shall be defined and allocated.

A.5.3 - Segregation of Duties

Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets.

A5.4 - Management Responsibilities

Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organisation.

A5.5 - Contact with Authorities

Appropriate contacts with relevant authorities shall be maintained.

A5.6 - Contact with Special Interest Groups

Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.

A5.7 - Threat Intelligence

The organisation is required to have information sources on information security threats, and these should be analysed to produce threat intelligence

A5.8 - Information Security in Project Management

Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.

A5.9 - Inventory of Information & Other Related Assets

Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained. Assets maintained in the inventory shall be owned.

A5.10 - Acceptable Use of Information & Other Associated Assets

Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented, and implemented.

A5.11 - Return of Assets

All employees and external party users shall return all the organisational assets in their possession upon termination of their employment, contract, or agreement.

A5.12 - Classification of Information

Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.

A5.13 - Labeling of information

An appropriate set of procedures for information labeling shall be developed and implemented in accordance with the information classification scheme adopted by the organisation.

A5.14 - Information Transfer

Formal transfer policies, procedures and controls shall be in place to protect the transfer of information using all types of communication facilities. Agreements shall address the secure transfer of business information between the organisation and external parties

A5.15 - Access Control

Rules are required to control physical and logical access to information and other assets in line with business and information security requirements

A5.16 - Identity Management

The full lifecycle of identities need to be managed.

A5.17 Authentication Management

The organisation needs to control the allocation and management of authentication information including advice to personnel on appropriate handling.

A5.18 - Access Rights

The organisation is required to have topics-specific policy on and rules for access control including provisioning, review, modification, and removal of access.

A5.19 - Information Security in supplier relationships

Information security requirements for mitigating the risks associated with supplier's access to the organisation's assets shall be agreed with the supplier and documented.

A5.20- Addressing security within supplier agreements

All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organisation's information.

A5.21 - Information and communication technology supply chain

Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.

To maintain an agreed level of information security and service delivery in line with supplier agreements.

A5.22 - Monitoring, Review and Change of Supplier Services.

Organisations shall regularly monitor, review and audit supplier service delivery. Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures, and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.

A5.23 - Information Security for Cloud Services

The organisation is required to have processes for acquisition, management and exit from cloud services in line with information security requirements.

A5.24 - Information Security Incident Planning & Preparation

Planning and preparing for information security events by defining, establishing, and communicating incident management processes, roles, and responsibilities.

A5.25 - Assessment and decision on Information Security Events

The organisation should have documented procedures for response to information security events.

A5.26 - Response to Information Security Incidents

Events should be responded to using the incident management procedures.

A5.27 - Learning from Information Security Incident

The organisation should use the knowledge gained from incidents to strengthen its information security.

A5.28 - Collection of Evidence

The organisation shall define and apply procedures for the identification, collection, acquisition, and preservation of information, which can serve as evidence.

A5.29 - Information Security During Disruption

The organisation shall establish, document, implement and maintain processes, procedures, and controls to ensure the required level of continuity for information security during an adverse situation.

A5.30 - ICT Readiness for Business Continuity

The organisation shall establish, document, implement and maintain processes, procedures, and controls to ensure the required level of continuity for information security during an adverse situation.

A5.31 - Legal, Statutory, Regulatory and Contractual Requirements

All relevant legislative, statutory, regulatory, and contractual requirements and the organisation's approach to meet these requirements shall be explicitly identified, documented, and kept up to date.

A5.32 - Intellectual Property Rights.

Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements related to intellectual property rights and use of proprietary software products.

A5.33 - Protection of Records

Records shall be protected from loss, destruction, falsification, unauthorised access, and unauthorised release, in accordance with legislatory, regulatory, contractual, and business requirements.

A5.34 - Privacy and Protection of Personally Identifiable Information.

Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation and contractual requirements, where applicable.

A5.35 - Compliance with Security Policies, Rules, and Standards.

The organisation shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards, and any other security requirements.

A5.36 - Documented Operating Procedures.

Operating procedures shall be documented and made available to all personnel who need them.

A.6 PEOPLE CONTROLS

A6.1 - Screening

Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

A6.2 - Terms and Conditions of Employment

The contractual agreements with employees and contractors shall state their and the organisation's responsibilities for information security.

A6.3 - Information Security Awareness, Education and Training

All employees of the organisation and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organisational policies and procedures, as relevant for their job function.

A6.4 - Disciplinary Process

There shall be a formal and communicated disciplinary process in place to act against employees who have committed an information security breach.

A6.5 - Responsibilities after Termination or Change of Employment

The organisation shall communicate information security responsibilities and duties that remain valid after termination or changes to employment

A6.6 - Confidentiality or Non-Disclosure Agreements.

Requirements for confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information shall be identified, regularly reviewed, and documented.

A6.7 - Remote Working

The organisation shall implement security measures when information is being accessed, processes or stored outside the organisation's premises.

A6.8 - Information Security Event Reporting

The organisation shall provide a mechanism for actual or potential information security events to be reported through appropriate channels as quickly as possible.

A.7 PHYSICAL CONTROLS

A7.1 Physical Security Perimeter

Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.

A7.2 - Physical Entry

The organisation will have entry controls for secure areas and access points.

A7.3 - Securing Offices, Rooms, and Facilities.

Physical security for offices, rooms and facilities shall be designed and applied.

A7.4 - Physical Access Monitoring

The organisation shall continuously monitor access for unauthorised physical entry.

A7.5 - Protecting against external and environmental threats

Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.

A7.6 - Working in Secure Areas

Procedures for working in secure areas shall be designed and applied.

A7.7 - Clear desk and clear screen policy.

A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.

A7.8 - Equipment Siting and Protection.

Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access.

A7.9 - Security of Equipment and Assets OffPremises.

Security shall be applied to off-site assets considering the different risks of working outside the organisation's premises.

A7.10 - Storage Media

The organisation shall manage storage media through their lifecycle from acquisition, use, transportation, and disposal considering the classification scheme and handling requirements.

A7.11 - Supporting Utilities

Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.

A.7.12 - Cabling Security

Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference, or damage.

A7.13 - Equipment Maintenance

Equipment shall be correctly maintained to ensure its continued availability and integrity.

A7.14 - Secure Disposal or Reuse of Equipment.

Security shall be applied to off-site assets considering the different risks of working outside the organisation's premises

A.8 TECHNOLOGICAL CONTROLS

A.8.1 - User End Point Devices

The organisation needs to protect information stored on, processed or accessible through user end point devices.

A8.2 - Privileged Access Rights

The organisation shall restrict and manage the allocation and use of privileged access rights..

A8.3 - Information Access Restriction

The organisation requires a topic-specific access control policy to determine restriction of access to information and relate assets.

A8.4 - Access to Source Code

The organisation shall appropriately manage read and write access to source code, development tools and software libraries.

A8.5 - Secure Authentication

The organisation shall ensure secure authentication technologies and procedures to in line with its information access restrictions and topic-specific access control policy.

A8.6 - Capacity Management

The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.

A8.7 - Controls Against Malware

Detection, prevention, and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

A8.8 - Management of Technical Vulnerabilities

Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organisation's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

A8.9 - Configuration Management

The organisation shall establish, document, implement, monitor, and review configurations of hardware, software, services, and networks.

A8.10 - Information Deletion
The organisation is required to delete information when it is no longer required.

A8.11 - Data Masking
The organisation shall mark data in line with the topic specific access control policy, business, and legislative requirements.

A8.12 - Data Leakage Prevention
The organisation shall deploy preventative measures to systems, networks and any other devices that process ,store and/or transmit sensitive information.

A8.13 - Information Backup
Backup copies of information, software and systems shall be taken and tested regularly in accordance with an agreed backup policy.

A8.14 - Redundancy of Information Processing Facilities.
Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.

A8.15 - Logging
Event logs recording user activities, exceptions, faults, and information security events shall be produced, kept, and regularly reviewed.

A8.16 - Monitoring Activities
The organisation shall monitor networks, systems and applications for anomalous behaviour and actions taken to evaluate potential information security incidents.

A8.17 - Clock synchronisation
The clocks of all relevant information processing systems within an organisation or security domain shall be synchronised to a single reference time source.

A8.18 - Use of Privileged Utility Programs
The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.

A8.19 - Installation of software on operational systems.
Procedures and measures shall be implemented to control the installation of software on operational systems.

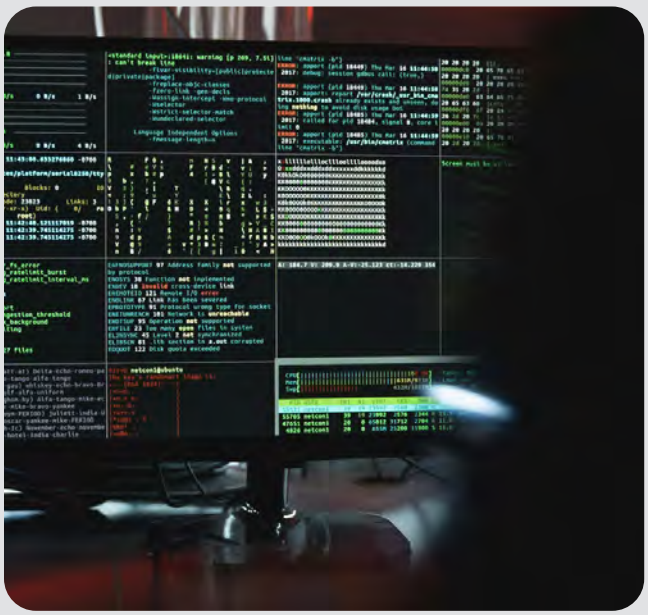
A8.20 - Networks Security
The organisation needs to ensure that networks and network devices shall be managed and controlled to protect information in systems and applications.

A8.21 - Security of network Services
The organisation needs to identify, implement, and monitor network security mechanisms, service levels and requirements

A8.22 - Segregation of Networks
Groups of information services, users and information systems shall be segregated on networks.

A8.23 - Web Filtering
The organisation shall manage access to external websites to reduce exposure to malicious content.

A8.24 - Use of Cryptography
There needs to be rules defined and implemented on the use of cryptography and key management.



A8.25 - Secure Development Lifecycle

Rules for the development of software and systems shall be established and applied to developments within the organisation.

A8.26 - Application Security Requirements

Organisations shall identify, specify, and approve information security requirements when acquiring and/or developing applications.

A8.27 - Secure System Architecture and Engineering Principles

There needs to be principles established, maintained, and applied for engineering secure systems during any information system development.

A8.28 - Secure Coding

Secure coding principles shall be applied to software development.

A8.29 - Security Testing in Development and Acceptance

The organisation shall define and implement security testing processes in the development lifecycle.

A8.30 - Outsourced Development

The organisation shall supervise and monitor the activity of outsourced system development.

A8.31 - Separation of Development, Test and Production Environments

The organisation must segregate and secure development, testing and production environments.

A8.32 - Change Management

The organisation will use change management procedures when making changes to information processing facilities and information systems.

A8.33 - Test Information

The organisation shall select, protect, and manage test information.

A8.34 - Protecting of Information Systems During Audit Testing

Assurance activities including testing and assessment of operational systems need to be planned and agreed between tester and responsible management.

spark
GROWTH SOLUTIONS

Empowering organisations to manage risk, build resilience and growth with confidence in an increasingly complex and challenging threat environment.

GET STARTED