DIGITAL MODUS

Digital Modus Ltd

Information Security Management (ISM) System Manual DM/110/04

ISO/IEC 27001:2022

1 ISM01 - Document Information

1.1 Document Control

This manual is controlled as defined in Documents & Data Control Procedure [ISP08].

Version	Date	Author	Comments
DM/110/00	27 Jun 2022	Peter Digby	First version
DM/110/01	27th July 2023	Kerry Brannigan	Reviewed, Google Approval Requested from Directors
DM/110/02	7th Sept 2023	Kerry Brannigan	Scope amended, Approval Requested from Directors
DM/110/03	*26th Sept 2023*	Peter Digby	Removed duplicated responsibilities section
DM/110/04	30th June 2024	Kerry Brannigan	Annual Review: ● Added cert details for 1.2 ● external audit added 8.6.3 ● revised responsibilities for ISMR & ISMC in 5.3 ● grammar improvements
DM/110/xx	30th June 2025		Annual Review:

Distribution List

Name	Role
Staff	All Staff employed by Digital Modus must-read.
Contractors	All people involved on behalf of a subcontractor contracting with Digital Modus must-read.
Suppliers	Shared with Suppliers as part of Digital Modus supplier onboarding.
Customers	Shared with all Customers on request.

1.2 Controlled Distribution

The current approved version of this document in PDF format is held on the Cybersmart Smart Policies platform and accessible to all employees.

https://app.cybersmart.co.uk/0d464863-06cc-4b53-ae39-0af9f77ce6ee/policies/

The working version of the document is held in a restricted access folder. All changes are tracked.

The scope of the processes covered by this Information Security Manual is defined as:

THE PROVISION OF DIGITAL TRANSFORMATION, SALESFORCE SERVICES AND DATA SCIENCE SERVICES FOR ORGANISATIONS IN THE PUBLIC AND PRIVATE SECTOR

in accordance with the latest issue of the company's statement of applicability

The Information Security Management System is designed to meet the requirements of:

Standard/Authority	Certificate Number	Valid Until
ISO/IEC 27001:2022	190608	1 November 2026

This scope was determined taking into account the organisation and its context, needs and expectations of interested parties, the organisation's boundaries, the interfaces and dependencies of activities performed by the organisation and those that are performed by other organisations.

2 ISM02 - Contents

1 ISM01 - Document Information 2
1.1 Document Control 2
Distribution List 2
1.2 Controlled Distribution 3
2 ISM02 - Contents 4
3 ISM03 - Amendments 6
4 ISM04 - Company Profile 7
4.1 Our Experience 7
4.2 Our Approach 7
4.3 Strategic Objectives 8
5 ISM05 – Company Structure and Responsibilities 9
5.1 Company Structure 9
5.2 Responsibilities 9
5.3 Organisation Responsibilities 10
5.3.1 Directors: 10
5.3.2 Information Security Management Representative: 11
5.3.3 Information Security Competent Person: 11
5.3.4 All Personnel (including third party users): 12
5.3.5 Assigned Information Security Management System Responsibilities: 13
5.4 Information Security Management System Structure 13
6 ISM06 - INFORMATION SECURITY OBJECTIVES 14
7 ISM07 – INFORMATION SECURITY POLICY 16
8 ISM08 - ISM SYSTEM REQUIREMENTS 18
8.1.1 Organisation and Context 18
8.1.2 Understanding the needs and expectations of interested parties 19
8.1.3 Scope of the Information Security Management System 19
8.1.4 Information Security Management System 20
8.2 LEADERSHIP 21
8.2.1 Leadership and Commitment 21
8.2.2 Policy 21
8.2.3 Organisational roles, responsibilities and authorities 22
8.3 PLANNING 22
8.3.1 Actions to address risks and opportunities 22

8.3.1.1 General 22
8.3.1.2 Information security risk assessment 22
8.3.1.3 Information security risk treatment 23
8.3.2 Information security objectives and plans to achieve them 24
8.4 SUPPORT 24
8.4.1 Resources 24
8.4.2 Competence 24
8.4.3 Awareness 25
8.4.4 Communication 25
8.4.5 Documented information 25
8.5.5.1 General 25
8.5.5.2 Creating and updating 25
8.5.5.3 Control of Documented Information 25
8.5 OPERATIONS 26
8.5.1 Operational planning and control 26
8.5.2 Information security risk assessment 26
8.5.3 Information security risk treatment 26
8.6 PERFORMANCE EVALUATION 27
8.6.1 Monitoring, measurement, analysis and evaluation 27
8.6.2 Internal audit 27
8.6.3 External audit 28
8.6.4 Management review 28
8.7 IMPROVEMENT 28
8.7.1 Nonconformity and corrective action 28
8.7.2 Continual improvement 29

3 ISM03 - Amendments

All copies of this manual must be kept under strict control to prevent the System from becoming unreliable. The following Procedures will ensure that the system remains current and valid.

The current approved version of this document in PDF format is held on the Cybersmart Smart Policies platform and accessible to all employees.

https://app.cybersmart.co.uk/0d464863-06cc-4b53-ae39-0af9f77ce6ee/policies/

The working version of the document is held in a restricted access folder. All changes are tracked.

In addition:

- Each page in the manual will carry its own number.
- The Information Security Management Representative will be responsible for all revisions and additions being recorded.
- Changes can be suggested by any Employee but must receive management review and approval before being entered into the Manual.
- All changes must be recorded on the version control history of this document.

4 ISM04 - Company Profile

4.1 Our Experience

Digital Modus has been integral in establishing both digital standards and transformation of services across the UK Government's Digital Services, Departments, Agencies, Health Organisations and Local Councils.

We have:

- Replaced paper processes with online digital services used by over 20 million citizens
- Modernised and replaced mission critical, legacy systems
- Transformed operating models and organisation culture to focus on digital delivery
- Insourced, remodelled and disaggregated large IT outsourcing Contracts worth over £4 billion
- Delivered large omni-channel Contact Centre and Operational capability

We were a part of the leadership team that established the UK Government Digital Service, delivering transformational Digital change for citizens across all Government Departments and Agencies.

We have also delivered large and complex change programmes into the Insurance, Finance and Energy Sectors.

4.2 Our Approach

Digital Modus focuses on delivery. We take a customer-centric view. We start small, get consensus, demonstrate early, and deliver results.

Our Digital Delivery Services enable organisations to save money, be agile, while empowering citizens, users and customers to serve themselves.

We deliver digital transformation through the following:

- Building user and citizen centric Digital Services
- Creating agile and delivery focussed teams and organisations
- Agreeing flexible and cost effective commercial outsourcing agreements
- Providing shared, common, cloud and digital services
- Enabling omni-channel Customer Engagement

4.3 Strategic Objectives

We understand the challenges in delivering digital transformation and change across government institutions and large federated organisations. The factors that need to be aligned are not just the technology but also the political, organisational, culture, and commercial factors.

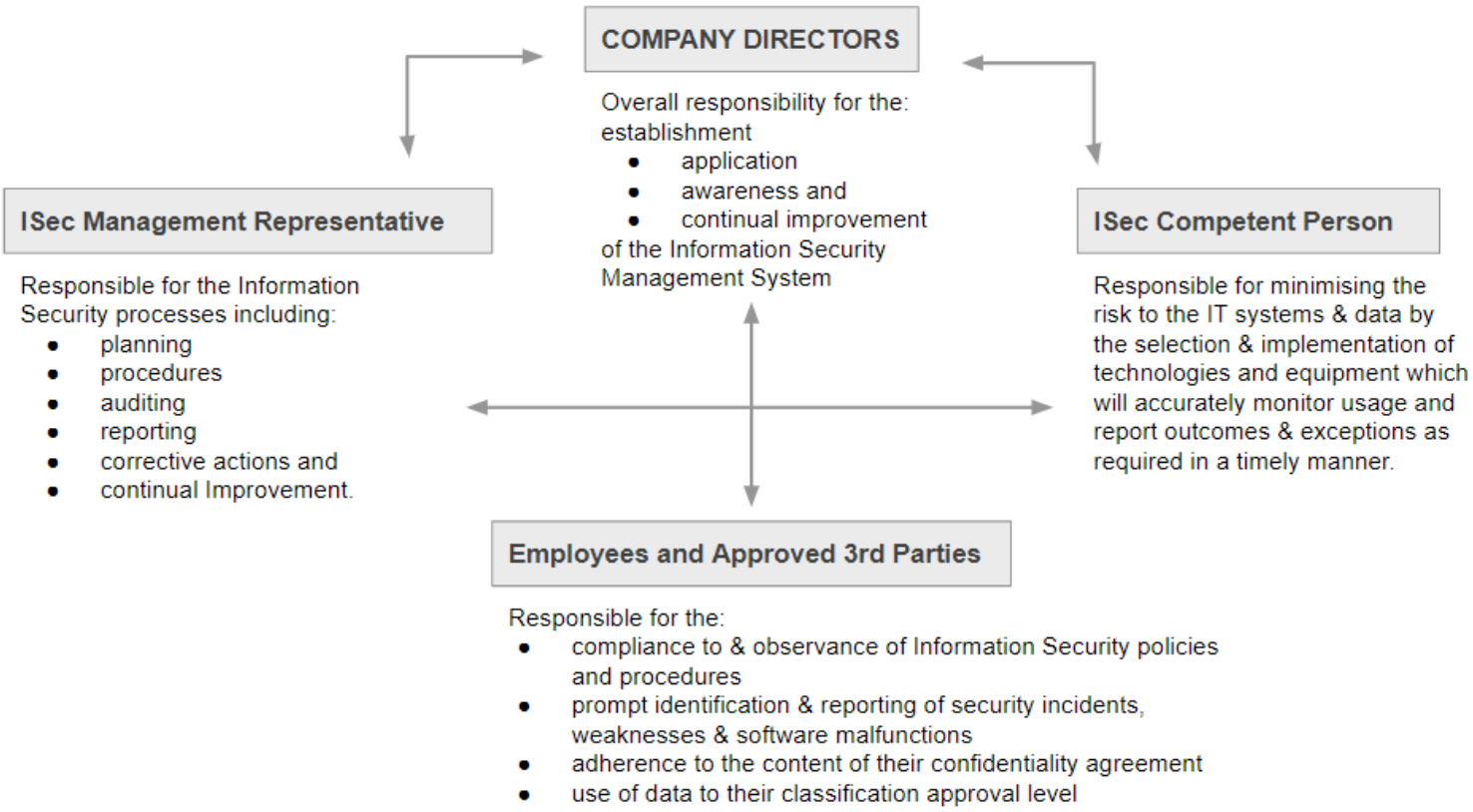
We believe in and promote ethics, standards and best practices, technology knowledge, and organisational experience. We apply the lessons we have learned in delivering large digital transformation services across federated organisations.

An essential requirement of the continuing maintenance and development of the organisation's objectives is the installation of an Information Security Management System registered to ISO 27001:2022 status.

5 ISM05 – Company Structure and Responsibilities

5.1 Company Structure

Organisational structure and summary of responsibilities:



5.2 Responsibilities

CEO/Chair

- Company strategy
- Finance and planning

Directors

- Business administration
- Health & Safety
- Marketing and Sales

- Resources management
- Standards

Information security management representative

- Information Security

Technical/IT Manager

- Client liaison
- Contract management
- Information security competent person

5.3 Organisation Responsibilities

While the detailed information security management system states specific titles for certain actions, other persons may need to carry out the actions in the short-term absence of the stated person.

The Directors will determine who will be delegated to perform the required responsibilities and authorities.

The short-term delegation of the actions to another person does not mean that the person holding the Post Title relinquishes the responsibility and must monitor all actions carried out on their behalf.

For long-term absences, the Directors will be responsible for passing the responsibilities of the Post Title to another suitable and qualified member of staff.

Information Security Management System responsibilities are described as follows:

5.3.1 Directors:

Responsible for:

- the overall application of the Information Security Management System;
- Ensuring adequate and effective planning, organisation and monitoring of Information Security in accordance with relevant legislation.
- Ensuring sufficient financial, physical and labour resources and time are available to meet Information Security requirements.
- Establishing the Information Security Policy, establishing Information Security Management System objectives and plans in support of the Policy.
- Ensuring the awareness of all employees of the Information Security Policy, and supporting objectives, and their duties towards it.

- Ensuring all reported Information Security issues are reviewed and remedial action applied when necessary.
- Ensuring data and Information Security equipment used within the company is properly protected and control systems are regularly inspected and maintained.
- Ensuring contractors employed on Information Security matters are competent and understand the company Information Security requirements.
- Ensuring risk assessments are undertaken to assist in the implementation of a comprehensive Information Security Management System

5.3.2 Information Security Management Representative:

Responsible to the Directors for:

- Ensuring there are effective arrangements, planning, organisation, control and monitoring of Information Security within the company and that corrective and preventive measures are maintained and legal requirements met.
- Acting on incident reports and reporting back to the Directors.
- Ensuring that Information Security is taken into account in new projects and all other company dealings and that competent advice is available as required.
- Ensuring that employees, subcontractor and on site contractors are aware of their Information Security duties and that they comply with the requirements of the Policy.

5.3.3 Information Security Competent Person:

Responsible for:

- Planning and managing the Information Security Management System, including maintaining and controlling the Manual and any associated procedures and documentation.
- Supporting the Directors and & ISMR in the general duties to ensure the Information Security Policy is implemented and maintained.
- Preparing and implementing a program of internal audits and reviews of the Information Security Management System to ensure compliance with the BS ISO/IEC 27001:2022 standard.
- Providing, as required, timely, accurate and current information to ensure the completeness of the company's Information Security systems.
- Ensuring reporting relationships are clear and unambiguous.

- Ensuring sufficient resources and authority are available to perform the task
- Reporting to the Directors & ISMR on patterns, trends and other quantifiable measurements to ascertain the effectiveness of the System in meeting the Company's Information Security Policy and objectives and the requirements of Customers.

5.3.4 All Personnel (including third party users):

Responsible for:

- Providing truthful and accurate information as requested at the time of the job application and in the application form and supporting documentation.
- The compliance to and maintenance of, those aspects and requirements of the Company's Information Security Management System and associated procedures in which they are involved.
- Being aware of and applying the requirements of the Company's Information Security Management System Policy and for upholding its principles.
- The processing or use of data to the classification level for which they have approval.
- Observing the content of their confidentiality agreement with the company.
- The prompt identification and reporting of security incidents.
- Co-operating with the Company initiatives in responding to incidents.
- Identifying and reporting any actual or suspected security weaknesses.
- Identifying and reporting software malfunctions.
- Ensuring all reports of incidents, weaknesses and malfunctions are made through the appropriate management channel or to the Information Security management representative.

5.3.5 Assigned Information Security Management System Responsibilities:

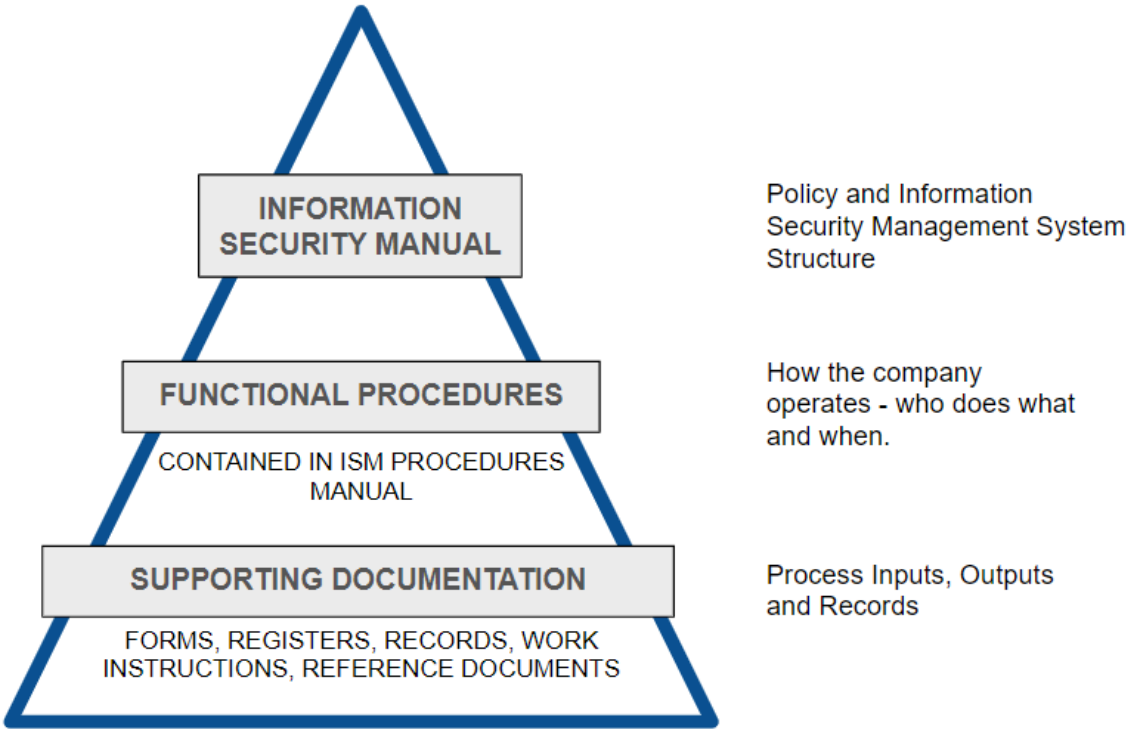
In accordance with the procedures defined in the authorised Information Security and Procedures Manuals, including the Internal Audit Procedure, the following personnel are appointed as Information Security Management Representative, Internal Information Security Auditors, and Information Security Competent Persons see:
Assigned Responsibilities Register

Note: for the details of any external personnel utilised for their specialist information technology/security skills and experience, see: DM Certifications and Skills Planning

5.4 Information Security Management System Structure

The formal Information Security Management System has been developed with the following basic structure:

International Standard ISO/IEC 27001:2022	Defines International System requirements
Customer Specifications & Special Information Security Conditions	Defines Customer Requirements



6 ISM06 - INFORMATION SECURITY OBJECTIVES

The Company is dedicated to establishing an Information Security Management System that includes the setting, measuring and monitoring of Information Security objectives.

The Company will:

- Protect all forms of information from a wide range of threats.
- Recognise information can be printed or written on paper, stored electronically, transmitted via post or using electronic means, shown in films or spoken in conversation.
- Maintain confidentiality by ensuring information is accessible only to those authorised to have access.
- Maintain integrity by safeguarding the accuracy and completeness of information and processing methods by protecting against unauthorised modification.
- Maintain availability by ensuring that authorised users have access to information and associated assets when required.
- Ensure business continuity, minimise business damage and maximise return on investments and business opportunities.
- Ensure information security is seen as essential to maintain competitive edge, cash flow, profitability, legal compliance and commercial image.
- Set out clearly the nature of the threats faced by the organisation and the possible costs, in both financial and non-financial terms, of information security breaches.
- Identify the processes involved in providing products and services and will establish systems to ensure Information Security requirements are met efficiently and economically, including customer, regulatory and other contractual requirements.
- Provide clear leadership to ensure all employees are able to focus on a prevention rather than detection philosophy and that it is applied throughout the company.
- Operate a system of education and training for Information Security improvement.
- Review the Information Security Management System to identify opportunities for improvement and to maintain progress and continual improvement.
- Ensure all Information Security objectives are measurable and consistent with the Information Security Policy.

Achieving these objectives will demonstrate management's dedication to applying a systematic approach to the establishment and maintenance of an Information Security Management System and to demonstrate the determination to consistently provide products and services that meet Customer and applicable regulatory requirements.

7 ISM07 – INFORMATION SECURITY POLICY

The top management of Digital Modus understands the information security needs and expectations of its interested parties both within the organisation and from external parties including, amongst others, clients, suppliers, regulatory and Governmental departments.

The company recognises that the disciplines of confidentiality, integrity and availability of information in information security management are integral parts of its management function and view these as their primary responsibility and fundamental to best business practice.

To this end Digital Modus has produced this information security policy aligned to the requirements of ISO/IEC 27001: 2022 to ensure that the Company:

- Complies to all applicable laws and regulations and contractual obligations
- Implements Information Security Objectives that take into account information security requirements following the results of applicable risk assessments
- Communicates these Objectives and performance against them to all interested parties
- Adopts an information security management system comprising a security manual and procedures which provide direction and guidance on information security matters relating to employees, customers, suppliers and other interested parties who come into contact with its work
- Works closely with Customers, Business partners and Suppliers in seeking to establish appropriate information security standards
- Adopts a forward-thinking approach on future business decisions, including the continual review of risk evaluation criteria, which may impact on information security
- Instructs all members of staff in the needs and responsibilities of information security management
- Constantly strives to meet and where possible exceed its customer's expectations
- Implements continual improvement initiatives, including risk assessment and risk treatment strategies, while making best use of its management resources to better meet information security requirements

Responsibility for upholding this policy is truly company-wide under the authority of the directors who encourage the personal commitment of all staff to address information security as part of their skills.

8 ISM08 - ISM SYSTEM REQUIREMENTS

General Introduction

DIGITAL MODUS Ltd recognises its responsibility as a Data Analytics Specialist and has developed and documented an Information Security Management System which complies with the international standard BS ISO/IEC 27001:2022, Information technology – Security techniques – Information security management systems – Requirements.

The purpose of this manual is to provide comprehensive evidence to all customers, suppliers, interested parties and employees of which specific controls are implemented to ensure information security.

This manual also governs the creation of information security related documents. It will be revised, as necessary, to reflect the information security management system currently in use. It is issued on a controlled copy basis to all internal functions affected by the information security management system and on an uncontrolled copy basis to customers, suppliers and other interested parties. It may be issued to customers on a controlled copy basis upon customer request.

The remaining part of this section follows the structure of the ISO27001: 2022 standard.8.1 CONTEXT OF THE ORGANISATION

8.1.1 Organisation and Context

The organisation shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.

The scoping requirements are an essential part of the management system. Its function is to describe the organisation it is intended to protect, bring into focus any specific types of information assets that are to be protected and crucially describe the boundaries inside of which the information assets are protected by default excluding information outside of that boundary.

This sets in place the basis on which the management system is designed, implemented and audited both internally and externally. The scope of the management system has been structured in such a way that stakeholders can at a high level understand the type of organisation that is covered, the types of information assets covered and the boundaries within which it operates.

External and internal issues have been considered when determining the scope.

See Control Procedure ISP01.

8.1.2 Understanding the needs and expectations of interested parties

The organisation shall determine interested parties that are relevant to the information security management system and the requirements of these interested parties relevant to information security; the requirements of interested parties may also include legal, regulatory requirements and contractual obligations.

Interested parties could include:

- Clients, including corporate, public and Government organisations

Their expectations could include:

- Legislation:
  The organisation adheres to the regulations contained in the register of legislation contained in its ISO 27001:2022 management system.
- Information managed:
  The organisation manages/has access to sensitive information for its clients.
- How information is managed: The organisation manages its client's processes through dedicated portals with full security protocols contained within and without the portal.
- Contractual obligations:
  Contractual obligations are contained within its contracts with client organisations
- Types of information assets to that are protected by the ISMS:
  for example Data, Physical documents, PCs and Networks, Portals, People.
- The boundaries within which the information security management system operates could cover: Main office; Satellite offices; Home users; Remote sites; Hosting locations both internal and external network boundaries (these are within dedicated portals)
- Connectivity: service provider
- Technology: hardware and software
- People

See also QM04

8.1.3 Scope of the Information Security Management System

The organisation's scope shall determine the boundaries and applicability of the information security management system to establish its scope.

The organisation's scope is as displayed on their issued certificate and detailed on the front pages of this manual.

8.1.4 Information Security Management System

DIGITAL MODUS Ltd is committed to establishing, implementing, maintaining and continually improving an effective information security management system to provide control of information security, on behalf of the Company and all interested parties, of the highest standard to meet both regulatory and interested party requirements.

This manual has been prepared to satisfy the requirements of BS ISO/IEC 27001: 2022 Information Technology – Security Techniques – Information Security Management Systems Requirements and identifies and covers the processes and activities carried out at the Company's sites of operation.

The Information Security Management System:

- Identifies the controls needed for the Information Security Management System and their application throughout the organisation
- Determines criteria and methods required to ensure the effective operation and management of these controls;
- Ensures the availability of resources and information necessary to support the operation and monitoring of these controls;
- Monitors, measures, and analyses the effectiveness of controls, and implements actions necessary to achieve planned results and continual improvement.

The method of meeting the requirements is stated briefly in this manual and the more detailed requirements are described in the Information Security Control Procedures Manual.

Information Security controls are integrated into any existing management systems including ISO 9001: 2015 and ISO 14001:2015 where practical and cross-referenced for ease of interpretation.

The effective implementation of the Information Security Management System will be verified by regular inspections, reviews and audits both internal and external which will compare management practices against the requirements of the written procedures and regulatory requirements. Corrective action will be taken where necessary and will be subsequently reviewed for effectiveness.

Where the phrase Information Security is used it refers to the security of Information, in electronic, hard copy or word of mouth form associated with the overall service and/or product delivery and not only computer based information.

The service and/or product delivery may involve working with the Customer's information on the Customer's or Company facilities by Company or sub-contracted personnel.

8.2 LEADERSHIP

8.2.1 Leadership and Commitment

Top management demonstrates its leadership and commitment with respect to the information security management system by:

a) Ensuring the information security policy and the information security objectives have been established and are compatible with the strategic direction of the organisation;

b) Ensuring the integration of the information security management system requirements into the organisation's processes;

c) Ensuring that the resources needed for the information security management system are available;

d) Communicating the importance of effective information security management and of conforming to the information security management system requirements;

e) Ensuring that the information security management system achieves its intended outcome(s);

f) Directing and supporting persons to contribute to the effectiveness of the information security management system;

g) Promoting continual improvement;

h) Supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility. Relevant to information security and are assigned and communicated.

Top management has assigned the responsibility and authority for:

a) Ensuring that the information security management system conforms to the requirements of this International Standard;

b) Reporting on the performance of the information security management system to top management.

Top management may also assign responsibilities and authorities for reporting performance of the information security management system within the organisation

See Section ISM05 for details of management structure and responsibilities

8.2.2 Policy

Top management has established an information security policy that:

a) Is appropriate to the purpose of the organisation.

b) Includes information security objectives (see section 6) and provides the framework for setting information security objectives.

c) Includes a commitment to satisfy applicable requirements related to information security.

d) Includes a commitment to continual improvement of the information security management system.

The information security policy is:

a) Available as documented information;

b) Has been communicated within the organisation;

c) Is available to interested parties, as appropriate.

8.2.3 Organisational roles, responsibilities and authorities

Top management has assigned the responsibilities and authority for:

a) Ensuring that the information security management system conforms to the requirements of this international standard;

b) Reporting on the performance of the information security management system to top management

See Section ISM05 for details of management structure and responsibilities

8.3 PLANNING

8.3.1 Actions to address risks and opportunities

8.3.1.1 General

When planning for the information security management system, the organisation has considered the issues referred to in 8.1.1 and the requirements referred to in 8.1.2 and determined the risks and opportunities that need to be addressed to ensure the information security management system can achieve its intended outcome(s); prevent, or reduce undesired effects and achieve continual improvement.

The organisation has planned actions to address these risks and opportunities; and how to integrate and implement these actions into its information security management system processes and evaluate the effectiveness of these actions

8.3.1.2 Information security risk assessment

The organisation has defined and applied an information security risk assessment process that establishes and maintains information security risk criteria.

These criteria include the risk acceptance criteria and the criteria for performing information security risk assessments.

The process ensures that repeated information security risk assessments produce consistent, valid and comparable results, and identify the information security risks.

The information security risk assessment process is designed to:

- identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system
- identify the risk owners
- analyse the information security risks
- assess the potential consequences that would result if the risks identified in ISO 27001:2022 clause 6.1.2 c) 1) were to materialise.
- assess the realistic likelihood of the occurrence of the risks identified in clause 6.1.2 c) 1)
- determine the levels of risk
- evaluate the information security risks
- compare the results of risk analysis with the risk criteria established in clause 6.1.2 a);
- prioritise the analysed risks for risk treatment.

The organisation retains documented information about the information security risk assessment process.

8.3.1.3 Information security risk treatment

The organisation has defined and applied an information security risk treatment process to select appropriate information security risk treatment options, taking account of the risk assessment results.

Based on that, the organisation has determined all necessary controls to implement the information security risk treatment option(s) chosen.

The organisation has designed controls as required and/or identified them from other sources.

It has compared the controls determined in ISO 27001:2022 (clause 6.1.3 b) in the Standard with those in the Statement of Applicability and verifies that no necessary controls have been omitted.

The organisation has produced a Statement of Applicability that contains the necessary controls and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from the Statement of Applicability.

The organisation has also formulated an information security risk treatment plan; obtained risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks.

The organisation retains documented information about the information security risk treatment process.

The information security risk assessment and treatment process aligns with the principles and generic guidelines provided in ISO 31000.

8.3.2 Information security objectives and plans to achieve them

The organisation has established information security objectives at relevant functions and levels, which are:

a) Consistent with the information security policy;
b) Measurable where practical
c) Take into account
    - applicable information security requirements
    - risk assessment
    - risk treatment results;
d) Communicated to the relevant people
e) Updated as appropriate

When planning how to achieve its information security objectives, the organisation has determined:

a) What will be done;
b) What resources will be required;
c) Who will be responsible;
d) When it will be completed; and
e) How the results will be evaluated.

The organisation retains documented information on the information security objectives.

8.4 SUPPORT

8.4.1 Resources

The organisation has determined and provided the resources needed to establish, implement, maintain, and continuously improve the information security management system.

8.4.2 Competence

The organisation has determined the necessary competence of person(s) doing work under its control that affects its information security performance, ensured that these persons are competent on the basis of appropriate education, training, or experience and where applicable, taken actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken whilst retaining the appropriate documented information as evidence of competence.

8.4.3 Awareness

Persons doing work under the organisation's control shall be aware of the following:

a) the information security policy

b) their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance and

c) The implications of not conforming to the information security management system requirements.

8.4.4 Communication

The organisation has determined the need for internal and external communications relevant to the information security management system, including what to communicate, when to communicate, with whom to communicate, who shall communicate and the processes by which communication shall be effected.

See ISP11.

8.4.5 Documented information

8.5.5.1 General

The organisation's information security management system includes documented information required by this International Standard and documented information determined by the organisation as being necessary for the effectiveness of the information security management system.

The extent of the documentation considers the size of the organisation and its type of activities, processes, products and services, the complexity of processes, their interactions and the competence of persons.

8.5.5.2 Creating and updating

When creating and updating documented information, the organisation has ensured the following:

- appropriate identification and description (e.g. a title, date, author, or reference number)
- format (e.g. language, software version, graphics)
- media (e.g. paper, electronic)
- review and approval for suitability and adequacy.

8.5.5.3 Control of Documented Information

Documented information required by the information security management system and by this International Standard will be controlled to ensure it is available and suitable for use,

where and when it is needed audit is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

For the control of documented information, the organisation has addressed the following activities, as applicable:

- distribution, access, retrieval and use;
- storage and preservation, including the preservation of legibility;
- control of changes (e.g. version control);
- retention and disposition.

Documented information of external origin, determined by the organisation as necessary for the planning and operation of the information security management system, has been identified as appropriate and controlled.

Security classifications have been considered and imply a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information, etc.

8.5 OPERATIONS

8.5.1 Operational planning and control

The organisation has planned, implemented, and controlled the processes needed to meet information security requirements and has implemented the actions determined in this section. It has also implemented plans to achieve the information security objectives determined in section 6.

The organisation keeps documented information necessary to ensure that the processes have been carried out as planned. They control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects as necessary.

The organisation has ensured that outsourced processes are determined and controlled.

8.5.2 Information security risk assessment

The organisation has carried out information security risk assessments at planned intervals and when significant changes are proposed or occur, taking account of the criteria established in ISO 27001:2022 clause 6.1.2 a).

The organisation retains documented information of the results of the information security risk assessments.

8.5.3 Information security risk treatment

The organisation shall implement the information security risk treatment plan.

The organisation retains documented information of the results of the information security risk treatment.

8.6 PERFORMANCE EVALUATION

8.6.1 Monitoring, measurement, analysis and evaluation

The organisation evaluates the information security performance and the effectiveness of the information security management system and has determined:

a) What needs to be monitored and measured, including information security processes and controls;

b) The methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;

c) When the monitoring and measuring shall be performed

d) Who shall monitor and measure

e) When the results from monitoring and measurement shall be analysed and evaluated

f) Who shall analyse and evaluate these results

The methods selected produce comparable and reproducible results that can be considered valid and the organisation retains appropriate documented information as evidence of the monitoring and measurement results.

8.6.2 Internal audit

The organisation conducts internal audits at planned intervals to provide information on whether the information security management system conforms to the organisation's requirements for its information security management system, the requirements of this International Standard and is effectively implemented and maintained.

The organisation:

- Plans, establishes, implements and maintains an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting.
  The audit programme(s) takes into consideration the importance of the processes concerned and the results of previous audits;
- defines the audit criteria and scope for each audit;
- selects auditors and conduct audits that ensure objectivity and the impartiality of the audit process;
- ensures that the results of the audits are reported to relevant management; and
- Retains documented information as evidence of the audit programme(s) and results.

8.6.3 External audit

External audits are conducted by third-party auditors to assess an organization's ISO compliance. Certification and surveillance audits also fall under the umbrella of "external audit.". A certification body will conduct an audit and issue a certificate of compliance that is good for three years. In turn, Digital Modus commits to keeping up the processes, product controls, and systems covered by that certificate. The initial certification audit reviews the ISMS in totality, focusing on policies and procedures, and then two subsequent years of surveillance audits will be conducted.

Any other cyber related audits will be managed via the Internal Audit Programme.

8.6.4 Management review

Top management reviews the organisation's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness. The management review shall include consideration of:

1. the status of actions from previous management reviews;
2. changes in external and internal issues that are relevant to the information security management system;
3. feedback on the information security performance, including trends in:
4. nonconformities and corrective actions;
5. monitoring and measurement results;
6. audit results;
7. fulfilment of information security objectives;
8. feedback from interested parties;
9. results of risk assessment and status of risk treatment plan;
10. Opportunities for continual improvement.

The outputs of management review include decisions related to continued improvement opportunities and any needs for changes to the information security management system with the organisation retaining documented information as evidence of the results of management review.

8.7 IMPROVEMENT

8.7.1 Nonconformity and Corrective Action

When nonconformity occurs, the organisation will react to the nonconformity, and as applicable, take action to control and correct it and deal with the consequences, evaluate the need for action to eliminate the causes of nonconformity, so that it does not recur or occur elsewhere, by reviewing the nonconformity, determining the causes of the nonconformity and determining if similar nonconformities exist, or could potentially occur.

The organisation will implement any action needed, review the effectiveness of any corrective action taken and make changes to the information security management system, if necessary; any corrective actions shall be appropriate to the effects of the non-conformities encountered.

The organisation shall retain documented information as evidence of the nature of the nonconformities, any subsequent actions taken, and the results of any corrective action.

8.7.2 Continual improvement

The organisation continually improves the information security management system's suitability, adequacy and effectiveness.