PASS REVELATOR

ISO 27001:2013

ISMS MANUAL

PASS REVELATOR

ISO 27001:2013
Information Security
Management
Systems Certified
Business™

1st Edition

ISO 27001:2013

Information Security Management
ISMS Manual

Author: PASS REVELATOR

Version History

Date	Change Notice	Change Description
Thursday, 22 September 2022	1001	Original Release to ISO 27001:2013

Table Of Contents CLICKABLE

1. Introduction

PASS REVELATOR has developed and implemented an Information Security Management System (ISMS) which enables us to:

- assess and treat information security risks in accordance with our particular needs
- demonstrate commitment and compliance to global best practice
- demonstrate to customers, suppliers and stakeholders that security is paramount to the way we operate
- better secure all financial and confidential data, so minimising the likelihood of it being accessed illegally or without permission

This manual describes our ISMS and sets out the authorities and responsibilities of those operating within it, as well as referencing those procedures and activities that fall within its scope.

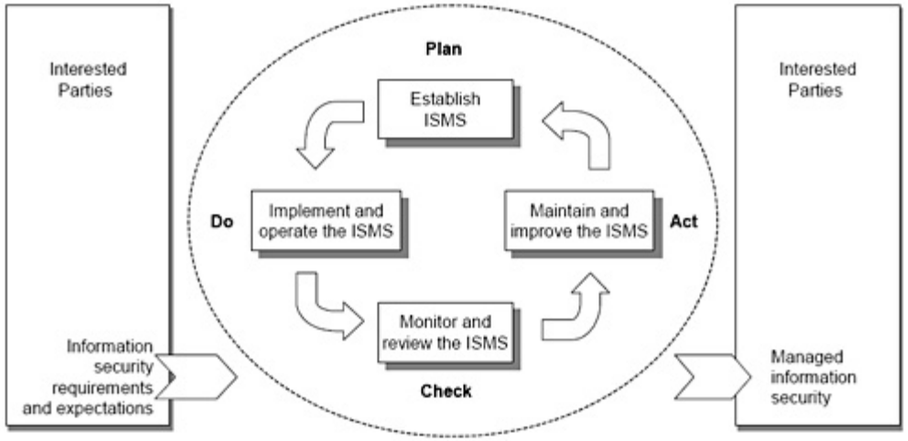
1.1. ISO 27001:2013

Our Information Security Management System (ISMS) has been developed in compliance with the ISO 27001:2013 standard which sets out a process based approach for establishing, implementing, maintaining and continually improving an information security management system within the context of our organisation.

Understanding and managing our interrelated processes as a system enables us to control the interrelationships and interdependencies so that our overall performance is enhanced.

Management of the processes and the system as a whole is achieved using the Plan-Do-Check-Act (PDCA) cycle with an overall focus on using risk based thinking to take advantage of opportunities and prevent undesirable results.

1.2. Plan-Do-Check-Act (PDCA) cycle



2. References

Standard	Title	Description
ISO 27000:2014	Information security management Systems	Overview and vocabulary
ISO 27001:2013	Information security management Systems	Requirements
ISO 27002:2013	Information technology - security techniques	Code of practice for information security controls
ISO 19011:2011	Auditing Management Systems	Guidelines for auditing

3. Terms and Definitions

The terminology used in this ISMS reflects both that used in ISO 27001:2013 and:

- standard business/quality terminology
- terms and vocabulary typically used within our scope of activity
- terms typically used in standards and regulations as they relate to our scope of activity

“we” and “our” refer to “PASS REVELATOR”.

“Top Management” as referred to in ISO 27001:2013 is represented in this ISMS Manual by the “PASS REVELATOR Management Team”.

4. Business Context

Understanding the needs and expectations of interested parties

To fully understand our business we identify all key internal and external issues that are relevant to our operations and which affect our ability to achieve the intended outcomes of this information security management system.

This involves:

- understanding our core products/services/processes
- understanding the scope of our information security management system
- identifying those interested parties ("stakeholders") who are relevant to our information security management system
- identifying and understanding the requirements of those internal and external interested parties relevant to information security

Many such issues are identified through an analysis of risks facing either ourselves or our stakeholders.

Our stakeholders and relevant internal and external issues are identified and are monitored as part of information security management reviews and updated as necessary.

Scope

Our information management security system satisfies the requirements of ISO 27001:2013 and, based on our understanding of our business and the needs and expectations of our stakeholders, addresses and supports our processes for

Information Technology & Services: Password Security Software

When determining this scope, we have considered:

- our organisation and its context (both internal and external issues)
- the needs and expectations of interested parties
- the interfaces and dependencies between activities performed by ourselves, and those that are performed by other organisations

Information security management system

To achieve our Information Security Objectives, we have established, implemented, maintained and continually improve our information security management system, including the processes needed and their interactions.

Our information security management system takes into consideration the needs and expectations of interested parties.

5. Leadership

Leadership and commitment

The PASS REVELATOR Management Team demonstrates leadership and commitment to achieving the objectives of our information security management system by taking accountability for the effectiveness of our information security management system and ensuring that:

- an Information Security Policy and Information Security Objectives are established for the management system and that they are compatible with our strategic direction and context
- our information security management system requirements are integrated into our business processes as appropriate
- our information security management system is suitably resourced
- there is clear communication on the importance of effective information security management and of conforming to the management system requirements
- our information security management system achieves its intended results
- all personnel are encouraged to contribute to the effectiveness of the management system
- continual improvement is actively promoted
- our information security policies, objectives and targets are, where appropriate, reflected in individual responsibilities and performance objectives

Information Security policy

The PASS REVELATOR Management Team has developed our Information Security Policy, which is to establish, monitor and continually improve our safeguards for the confidentiality, integrity and availability of all physical and electronic information assets to ensure that regulatory, operational and contractual requirements are fulfilled.

This policy governs our day-to-day operations to ensure the security of information and is communicated and implemented throughout our organisation. Our Information Security Policy is made available as a stand-alone document and widely distributed, including during induction.

Our Information Security Policy is typically reviewed annually, as part of our information security management review program, or as required to recognise the changing needs and expectations of relevant interested parties or the risks and opportunities identified by the risk management process.

Organisational roles, responsibilities & authorities

The PASS REVELATOR Management Team has assigned responsibilities and authorities for all roles relevant to the full and proper implementation, operation and maintenance of this management system, including the following:

- Determination of organisational context, establishment of overall direction, framing of policies for information security management, and conduct of management review
- Ensuring the promotion of a focus on information security matters throughout the organisation

- Framing of ISMS objectives, targets, and plans
- Control of ISMS documents
- Control of ISMS records
- Information security training, awareness and competence
- Management of internal ISMS audits
- Corrective and/or preventive actions
- Assessment and treatment of information security risks
- Ensuring that our information security management system conforms to applicable standards
- Implementation, operation, monitoring, review, maintenance, and Improvement of the ISMS
- Ensuring that the integrity of our information security management system is maintained when changes are planned and implemented
- Organising of independent review of information security management practices of the company
- Achieving and maintaining appropriate protection of organisational assets, and ensuring that information receives an appropriate level of protection
- Human resources security (prior to employment, during employment, and, on termination or change of employment)
- Physical and environmental security
- Communications and operations management
- Media handling and information exchange
- Network security management and access control
- Acquisition, development, and maintenance of information systems
- Information security incident management
- Business continuity management
- Complying with legal and regulatory requirements regarding information security

- Complying with contractual obligations regarding information security

These responsibilities and authorities are communicated through the combination of our Organisation Chart and internal Job Titles.

All managers are expected to demonstrate their commitment to the development and improvement of our information security management system through:

- the provision of necessary resources
- their involvement in the internal processes
- their proactive involvement in continual improvement activities
- focusing on the improvement of key system processes

All managers are responsible for the implementation of the policies, processes and systems described in this manual and for planning, controlling and resourcing our information security management system processes within their area of responsibility.

All personnel are responsible for the implementation of the policies and procedures applicable to processes they perform and are encouraged to identify and report any known or potential problems and to recommend related solutions.

6. Planning

Addressing risks and opportunities

In creating this information security management system, we have identified the risks and opportunities that need to be addressed, based particularly on: 4. Understanding the needs and expectations of our stakeholders but also including all other aspects of our information security management system. Those risks and opportunities have been addressed to:

- ensure that our information security management system can achieve its intended outcomes
- enhance desirable effects
- prevent, or reduce, undesirable effects
- achieve continual improvement

When managing risks and opportunities we have defined and apply an information security risk assessment process that establishes and maintains information security risk criteria, including both the risk acceptance criteria, and criteria for performing information security risk assessments.

- we consider risks and opportunities when taking actions within our information security management system, as well as when implementing or improving our information security management system
- formal risk management may not be utilised in all circumstances and the level of risk assessment, analysis, actions and recording will be to a level appropriate to each circumstance
- the actions we take to address risks and opportunities are proportionate to the potential impact on information security

We operate and maintain arrangements to identify, assess, evaluate and treat our information security risks and opportunities.

Establishing and achieving Information Security Objectives

The PASS REVELATOR Management Team have developed our Information Security Objectives, which are to:

- ensure that we can continue operations with minimal disruptions
- ensure absolute integrity for all information that we disburse or produce
- manage all information with appropriate confidentiality
- include information security training in our induction process
- minimise information security incidents to less than four per year

These objectives take into account our information security requirements and those risks and opportunities that we have identified.

The PASS REVELATOR Management Team ensures that our Information Security Objectives are:

- consistent with our Information Security Policy
- measurable (if practicable)
- monitored
- communicated
- updated as appropriate

Progress towards achieving each target, and the targets themselves, are reviewed during information security management review meetings by the PASS REVELATOR Management Team and updated as necessary.

These objectives and, where appropriate, the results of the PASS REVELATOR Management Team's reviews, are communicated to all employees, customers, suppliers, contractors, interested parties and the wider community.

We maintain documented information on each of our Information Security Objectives.

When a process does not meet its objective(s), or an unexpected problem is encountered with a process, corrective and preventive actions are employed to research and resolve the issue and, wherever possible, improve the process.

Planning actions to achieve our Information Security Objectives

When planning how to achieve our Information Security Objectives, we determine:

- what will be done
- what resources will be required
- who will be responsible
- when it will be completed
- how the results will be evaluated, including indicators for monitoring progress toward achievement of our measurable Information Security Objectives.

Wherever practicable, we seek to integrate actions to achieve our Information Security Objectives into our business processes.

Periodically, or whenever our Information Security Objectives are changed, we prepare an ISMS Objectives Realisation Plan, which is submitted to the PASS REVELATOR Management Team for approval, implementation and monitoring.

Change management

This manual constitutes our overall plan for establishing, maintaining and improving our information security management system.

Whenever changes are to be made to processes or our information security management system, those changes are planned, implemented, and then verified for effectiveness.

Our information security management review and internal audit processes ensure the continuing integrity of the ISMS when significant changes are planned.

7. Support

Resources

The PASS REVELATOR Management Team ensures that all necessary resources are available to:

- implement and maintain this information security management system
- continually improve its effectiveness

Resources and resource allocation are assessed and monitored during information security management reviews.

Communication

We operate and maintain arrangements to ensure competency, awareness and communication.

These arrangements ensure that:

- all staff are competent to undertake their tasks
- all staff are aware of:
  - our management system(s) and their related policies and objectives
  - their roles and responsibilities
  - their contribution to the effectiveness of our management system(s)
  - the benefits of improved personal performance
  - the importance of complying with our management systems, policies and procedures

  - the consequences of any departure from our management systems, policies and procedures
  - emergency preparedness and response requirements
  - any management system changes
  - the results of the PASS REVELATOR Management Team's annual review of management system(s) compared to their objectives
- training needs are identified
- appropriate training plans are developed and implemented
- each role affecting management system outcomes is recorded

In addition to our staff, awareness programmes are also provided for contractors, temporary workers and visitors etc. as appropriate.

Documentation and records

Our information security management system documentation includes both documents and records.

The PASS REVELATOR Management Team has determined the extent of documented information:

- required by the ISO 27001:2013 International Standard
- necessary for the effectiveness of our information security management system

Based on the following criteria:

- the size of our business
- the scope, complexity and interaction of our processes and products/services
- the need to demonstrate fulfilment of our compliance obligations

- the competence of our personnel

Control of documents

We operate and maintain arrangements for the control of our quality management system documentation.

By means of this procedure we ensure that staff have access to the latest, approved information, and that the use of obsolete information is restricted.

Once established, all documented procedures are implemented and maintained.

Control of records

We operate and maintain arrangements for the identification, storage, retrieval, protection, retention, and disposition of environmental records.

This procedure also defines the methods for controlling records that are created by and/or retained by suppliers.

These controls are applicable to all those records which provide evidence of conformance to our information security management system, Information Security Objectives and regulatory and other obligations.

8. Operations

Operational planning and control

The PASS REVELATOR Management Team ensures that the processes needed to meet our information security management system requirements, to address risks and opportunities and to establish and achieve our Information Security Objectives, are properly planned and controlled.

- we identify, assess and treat our information security risks and opportunities
- we periodically, or whenever Information Security Objectives are changed, prepares an ISMS Objectives Realisation Plan which is submitted to the PASS REVELATOR Management Team for approval, implementation and monitoring
- we retain, analyse and evaluate records to the extent necessary to have confidence that the processes have been carried out as planned
- we control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary
- we control/influence out-sourced processes
- when a process does not meet its objective(s), or an unexpected problem is encountered with a process, corrective and preventive actions are employed to research and resolve the issue and, wherever possible, improve the process
- we review the suitability, adequacy and effectiveness of this management system at planned intervals

- These reviews include assessing the information security management system's continuing alignment to our strategic direction, opportunities for improvement, and the need for changes.

Information security risk assessment

The PASS REVELATOR Management Team ensures that information security risk assessments are undertaken, recorded and retained, both periodically and when significant changes are proposed or occur.

These risk assessments take into account both our agreed risk assessment criteria and criteria for performing information risk assessments.

Information security risk treatment

We manage and control our risks.

9. Performance Evaluation

Monitoring, measurement, analysis and evaluation

To evaluate the performance of our information security management system, we determine:

- what needs to be monitored and measured
- the methods of monitoring, measurement, analysis and evaluation needed to ensure valid results
- the criteria against which we evaluate our information security performance and various indicators
- when such monitoring and measurement should be undertaken
- when the results from monitoring and measurement are to be analysed and evaluated

These activities are used to evaluate:

- the performance and effectiveness of the information security management system
- the effectiveness of actions taken to address risks and opportunities
- the effectiveness of planning
- the performance of external providers
- other improvements to the management system

We operate and maintain arrangements for this monitoring, measuring, analysis and evaluation.

Internal audit

We operate and maintain arrangements for internal auditing at planned intervals.

By means of these audits, we provide information to management and determine whether our information security management system:

- conforms to our own requirements
- conforms to the requirements of the ISO 27001
- is effectively implemented and maintained
- is effective in achieving our management system's policies and objectives

Management review

We operate and maintain arrangements for the review the the suitability, adequacy and effectiveness of our information security management system, at planned intervals.

These reviews include assessing our information security management system's continuing alignment to our strategic direction, opportunities for improvement, and the need for changes.

10. Improvement

We use our information security management system, and other inputs, to continuously improve our information security outcomes.

The improvement opportunities we seek include:

- addressing evolving and future needs and expectations
- correcting, preventing and reducing undesired effects
- improving the performance and effectiveness of this information security management system

Non-conformity and corrective action

We operate and maintain arrangements to take corrective action to eliminate and further prevent the cause of any non-conformity, and preventive action so as to eliminate the causes of potential similar non-conformities.

Continual improvement

We seek to continually improve the suitability, adequacy and effectiveness of this information security management system.

We use the results of analysis and evaluation, and the outputs from information security management review,

to identify needs and opportunities for such improvement.

The overall effectiveness of our program of continual improvement, including both corrective actions and our wider progress in achieving corporate level improvement objectives, is monitored and assessed through our information security management review process.

11. Annex A – Control Objectives and Controls

We adopt those information control objectives set out in Annex A of ISO 27001:2013 as appropriate, and add additional control objectives and controls where necessary.

We set out our approach to the objectives and controls set out in Annex A in our high level control objectives and control documents:

- A6 Organisation of Information Security
- A7 Human Resource Security
- A8 Asset Management
- A9 Access Control
- A10 Cryptography
- A11 Physical and Environmental Security
- A12 Operations Security
- A13 Communications Security
- A14 Acquisition Development and Maintenance of Information Systems
- A15 Information Security in Supplier Relationships
- A16 Information Security Incident Management
- A17 Business Continuity Management
- A18 Information Security Reviews

We detail those operational policies and procedures necessary to ensure the consistent application of appropriate controls across all activities and systems within the scope of our ISMS, in Management Instructions to operatives and users.