



**SMTDATA**

**SMT DATA**

**MANAGEMENT SYSTEM**

**AUDIT REPORT**

ISO/IEC 27001

Initial Certification Audit

For 2025

**DECRYPT**  
COMPLIANCE

# TABLE OF CONTENTS

<b>I. EXECUTIVE SUMMARY.....</b>	<b>4</b>
<b>II. SCOPE OF CERTIFICATION.....</b>	<b>8</b>
<b>III. AUDIT PLANNING.....</b>	<b>8</b>
AUDIT OBJECTIVES.....	8
AUDIT SCOPE.....	9
AUDIT CRITERIA.....	10
AUDIT METHODOLOGY.....	10
AUDIT LOGISTICS.....	11
<b>IV. AUDIT ATTENDEES.....</b>	<b>13</b>
<b>V. AUDIT TEST DETAILS.....</b>	<b>14</b>
CLAUSES.....	14
ANNEX A CONTROLS.....	19
<b>VI. AUDIT FINDINGS - INITIAL CERTIFICATION.....</b>	<b>44</b>
<b>VII. AUDIT FINDING DEFINITIONS.....</b>	<b>44</b>
<b>VIII. STAGE 2 CERTIFICATION AUDIT - FINDINGS AND OUTCOMES.....</b>	<b>45</b>
NONCONFORMITIES.....	45
OPPORTUNITIES FOR IMPROVEMENT.....	47
<b>XI. AUDIT CONCLUSIONS AND AUDIT RECOMMENDATIONS.....</b>	<b>49</b>

# SECTION A: GENERAL INFORMATION

# I. EXECUTIVE SUMMARY

## INTRODUCTION

This executive summary provides an overview of the organization, the audit and outcomes of the ISO/IEC 27001:2022 initial certification audit conducted by Decrypt Compliance. The audit concluded that the organization's ISMS is generally compliant with the requirements of ISO/IEC 27001:2022. Referring to the results of the audit process and the demonstration of the organization's development and maturity, the audit team recommends that your organization's management system should be granted certification for ISO/IEC 27001:2022.

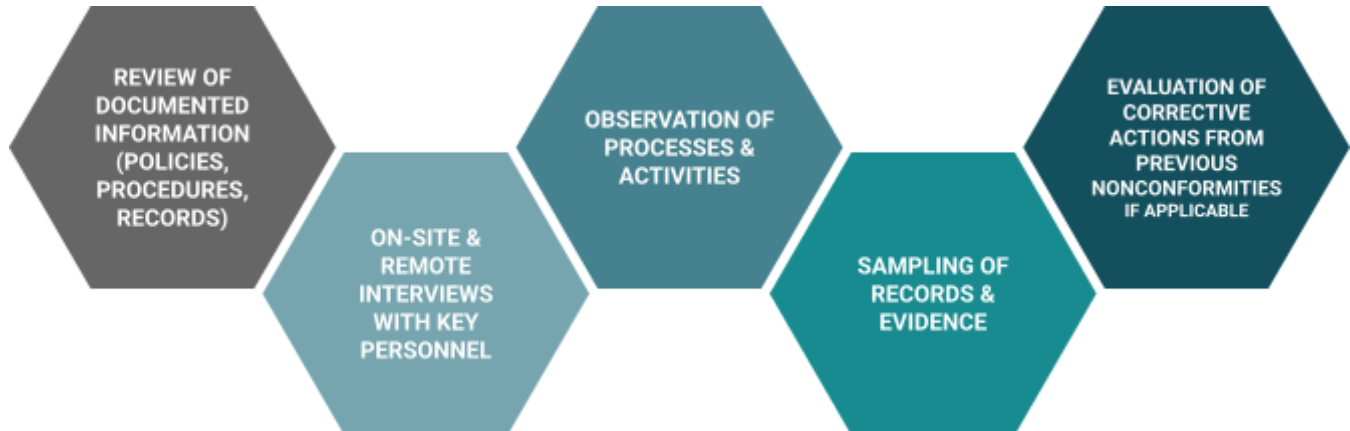
## ORGANIZATION & AUDIT INFORMATION

SMT Data provides capacity management and performance analysis to help larger companies with the performance of their IT infrastructure. SMT Data offers IT Business Intelligence (ITBI™) which enables customers to gather, understand, and optimize their IT capacity and performance costs on both mainframe and midrange platforms.

COMPANY NAME	SMT Data
COMPANY ADDRESS	Kongevejen 400b, 1 sal. 2840 Holte Denmark
WEBSITE	<a href="https://smtdata.com/">https://smtdata.com/</a>
PHONE NUMBER	
CLIENT REPRESENTATIVE NAME	Mads Rasmussen, Kim Mortensen
CLIENT REPRESENTATIVE EMAIL	<a href="mailto:mra@smtdata.com">mra@smtdata.com</a> and <a href="mailto:kmo@smtdata.com">kmo@smtdata.com</a>
TOTAL # OF EMPLOYEES WITHIN SCOPE	22
AUDIT STANDARD	ISO/IEC 27001:2022
AUDIT NUMBER	
AUDIT TYPE	Initial Certification
DURATION	3.5 days
AUDIT DATES	November 11 2024 and November 13 -15 2024
LEAD AUDITOR	Ishan Singh Thakur
ADDITIONAL TEAM MEMBER(S)	Lindisiwe Dube
ADDITIONAL ATTENDEES & ROLES	Rajesh Laskary, Kerem Cimen and Raymond Cheng: Observers
METHOD OF AUDIT	The audit was performed remotely via Google Meet
JOINT, COMBINED, INTEGRATED AUDIT?	N/A

## AUDIT METHODOLOGY

The audit methodology included:



## AUDIT OBJECTIVES

Decrypt Compliance has planned the audit in accordance with ISO/IEC 17021-1, ISO/IEC 27006-1, and Decrypt Compliance’s own policies and procedures to ensure that the following audit objectives are accomplished by the audit:

- Determining the ISMS’s conformity, or parts of it, with the audit criteria (ISO/IEC 27001:2022);
- Determining the ability of the management system to ensure the organization meets applicable, statutory, regulatory, and contractual requirements;
- Determining the effectiveness of management system to ensure the organization can reasonably expect to achieve its specified objectives;
- When applicable, identifying areas for potential improvement of the ISMS.

## AUDIT SCOPE

Decrypt Compliance performed an Initial Certification audit in two stages, Stage 1 and Stage 2. This report details the audit, findings, and outcomes of the Stage 2 audit.

The purpose of the Stage 2 is to evaluate the implementation, including effectiveness, of the client’s ISMS. In addition to evaluating the effective implementation of the ISMS, the objective of the Stage 2 is to confirm adherence to policies, procedures, objectives, and procedures. The Stage 2 Audit focused on the following:

- Information and evidence about conformity ISO/IEC 27001 and/or other normative standards;
- Performance monitoring, measuring, reporting and reviewing against key performance objectives and targets (consistent with the expectations of ISO/IEC 27001 and/or other normative documents);
- The ISMS’s ability and its performance regarding meeting of applicable statutory, regulatory and contractual requirements;
- Operational control of the client’s processes;
- Internal auditing and management review;
- Management responsibility for the client’s policies.

The audit team focused on top management's leadership and commitment to information security objectives; assessment of information security related risks ensuring that the management's assessment process produces consistent, valid and comparable results, if repeated; management's determination of controls based on the information security risk assessment and treatment processes; correspondence between the determined controls of the Statement of Applicability (SoA); the results of the information security risk assessment and treatment process; and the information security policy and objectives. The auditor paid special attention to the implementation of controls considering the external and internal context and related risks, and the monitoring, measurement, and analysis of information security processes and controls to determine whether controls declared as implemented were implemented and effective as a whole. Lastly, the audit was focused on programs, processes, procedures, records, internal audits, and reviews of the ISMS effectiveness to ensure that these are traceable to top management decisions and the information security policy and objectives.

#### AUDIT CRITERIA

The audit criteria (the set of requirements) for this audit include:

- a) All normative clauses of ISO/IEC 27001:2022:
  - Clause 4 – Context of the organization
  - Clause 5 – Leadership
  - Clause 6 – Planning
  - Clause 7 – Support
  - Clause 8 – Operation
  - Clause 9 – Performance evaluation
  - Clause 10 – Improvement
- b) Annex A – Information security controls reference as established in the SoA
- c) Appropriate use of certification marks
- d) Documentation and processes defined in the management system developed by the client.

#### AUDIT TEAM

**Lead Auditor:** Ishan Singh Thakur

**Audit Team Member(s):** Lindisiwe Dube

### FINDINGS SUMMARY

MAJOR NONCONFORMITIES	MINOR NONCONFORMITIES
0	6
OBSERVATIONS	OPPORTUNITIES FOR IMPROVEMENT
0	17

### SUMMARY OF CLIENT RISK ANALYSIS

A risk assessment conducted by SMT Data identified 59 risks across various categories. Out of which, 51 risks have been mitigated, 8 risks are in progress for mitigation, and none remain open. The risk assessment was conducted in accordance with the company's risk assessment practices.

### CONCLUSION

The audit concluded that the organization's ISMS is generally compliant with the requirements of ISO/IEC 27001:2022. Referring to the results of the audit process and the demonstration of the organization's development and maturity, the audit team

### AUDIT CONCLUSION

**AUDITOR RECOMMENDS  
CLIENT FOR CERTIFICATION**





## II. SCOPE OF CERTIFICATION

The scope of the ISO/IEC 27001:2022 certification is limited to information security to the design, development, and operation of all applications, data, and infrastructure utilized by SMT Data A/S in successful delivery of its software solution to its customers and stakeholders. This includes information assets located at our primary locations in Denmark. Departments included within the ISMS are Human Resources, Legal, Finance, Development, and Operations.

**VERSION & DATE OF SOA:** v1.0 - November 6, 2024

LOCATION/ AFFILIATE /SUBSIDIARY	ADDRESS	FUNCTION/ROLE IN ISMS
N/A	N/A	N/A

## III. AUDIT PLANNING

### AUDIT OBJECTIVES

- Stage 1 Audit – Audit management system documentation; evaluation client's location and site-specific conditions and the preparedness for the stage 2 audit; reviewing the client's status and understanding regarding requirements of the standard; collecting necessary information regarding the scope of the management system; reviewing the allocation of resources for stage 2 audit and agree with the client on the details of the stage 2 audit; planning the stage 2 audit; evaluation if the internal audits and management review are being planned and performed.
- Initial Audits/Stage 2 – Evaluation of the conformance and implementation of the management system with applicable standard(s) as well evaluation of the ability of the management system to ensure the client organization meets applicable statutory, regulatory and contractual requirements in order to determine if the facility can be recommended for Certification.
- Recertification Audits – Evaluation the continued fulfillment of all the requirements of the relevant management system standard or other normative document for renewal of the certification. Evaluation of the effectiveness of the management system in its entirety in the light of internal and external changes and its continued relevance and applicability to the scope of certification, evaluation of demonstrated commitment to maintain the effectiveness and improvement of the management system in order to enhance overall performance as well as the effectiveness of the management system with regard to achieving the certified client's objectives and the intended results of the respective management system(s).
- Surveillance – Evaluation of the conformance and effectiveness of the management system with applicable standard(s) for the purpose of continuing the certification as well evaluation of

the effectiveness of the management system to ensure the client organization is continually meeting its specified objectives.

- Special Audit – Evaluation of effectiveness of correction and corrective action implemented in order to close non- conformity issued during previous audit and/or to investigate complaints received and/or in response to changes and/or as follow up on suspended clients.
- Special Audit / Scope Expansion Audit – Evaluation of the conformance and implementation of the management system with applicable standard(s) against with extension application

## AUDIT SCOPE

The Information Security Management System (ISMS) applies to the design, development, and operation of all applications, data, and infrastructure utilized by SMT Data in successfully delivering its solution to its customers and stakeholders. The scope of certification covers various departments, including Human Resources, Legal, Finance, Development, and Operations.

AUDIT SCOPE	ADDITIONAL DETAILS / INFORMATION
The Organizational Units	Human Resources Legal Finance Development Operations
IT Infrastructure	Third party managed - AWS
Software / Service	IT Business Intelligence (ITBITM)
Departments	Human Resources Legal Finance Development Operations
Processes	<ul style="list-style-type: none"> <li>- Regulatory (Compliance)</li> <li>- Internal systems</li> <li>- External systems</li> <li>- Incident management and response processes</li> <li>- Disaster recovery processes</li> <li>- Business continuity processes</li> <li>- Software development processes</li> <li>- Operations security processes</li> <li>- Access Control processes (including user registration and provisioning)</li> </ul>







# SECTION C: AUDIT SUMMARY

## V. AUDIT TEST DETAILS



Conformity



Major Nonconformity



Minor Nonconformity



Observation



Opportunity for Improvement

### CLAUSES

#	CLAUSE REQUIREMENT	FINDING STATUS	AUDIT EVIDENCE (FINDING & JUSTIFICATION)
<b>4. Context of the organization</b>			
4.1	Understanding the organization and its context		Statement of Applicability and Statement Definition
4.2	Understanding the needs and expectations of interested parties		Statement of Applicability and Statement Definition Meetings with external parties could be organized to obtain more specific relevant requirements of interested parties.
4.3	Determining the scope of the ISMS		Statement of Applicability and Statement Definition Scope of the ISMS could be further refined upon identification of additional relevant requirements of interested parties. Scope of the ISMS could be further refined with additional details of external party interfaces and dependences.
4.4	Information security management system		Statement of Applicability and Statement Definition

























#	CONTROL OBJECTIVE & DESCRIPTION	STATUS OF FINDING	AUDIT EVIDENCE (FINDING & ITS JUSTIFICATION)
A.5.20	<p><b>Addressing information security within supplier agreements</b></p> <p><b>Control.</b> Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.</p>		It was observed that Relevant information security requirements are not established and agreed with each supplier based on the type of supplier relationship. Information Security questionnaire for the vendors is not maintained.
A.5.21	<p><b>Managing information security in the information and communication technology (ICT) supply chain</b></p> <p><b>Control.</b> Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.</p>		<ul style="list-style-type: none"> <li>-Third party risk management</li> <li>- List of all IT vendors and status</li> <li>- Information asset inventory.xlsx</li> <li>- Sample of agreements with vendors</li> </ul>
A.5.22	<p><b>Monitoring, review and change management of supplier services.</b></p> <p><b>Control.</b> The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.</p>		It was mentioned that review of change in supplier information security practices and service delivery is done annually. It is recommended to do at the time of onboarding as well and maintain evidence for the same.
A.5.23	<p><b>Information security for use of cloud services</b></p> <p><b>Control.</b> Processes for acquisition, use, management and exit from</p>		<ul style="list-style-type: none"> <li>-Third party risk management</li> <li>- List of all IT vendors and status</li> <li>- Information asset inventory.xlsx</li> <li>- Sample of agreements with vendors</li> </ul>









#	CONTROL OBJECTIVE & DESCRIPTION	STATUS OF FINDING	AUDIT EVIDENCE (FINDING & ITS JUSTIFICATION)
A.6.1	<p><b>Screening</b></p> <p><b>Control.</b> Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.</p>		<ul style="list-style-type: none"> <li>- Human Resource Policy</li> <li>- Candidates pre-employment checks</li> </ul> <p>It was mentioned that background verification of 1 member from Netherlands is pending. Background verification of all the employees should be done prior to joining the organization.</p>
A.6.2	<p><b>Terms and conditions of employment</b></p> <p><b>Control.</b> The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.</p>		<ul style="list-style-type: none"> <li>- Human Resource Policy</li> <li>- List of company employees</li> <li>- Signed NDA</li> <li>- Employment agreement</li> </ul>
A.6.3	<p><b>Information security awareness education and training</b></p>		<ul style="list-style-type: none"> <li>- Human Resources Policy</li> <li>- Security awareness training completion</li> <li>- Security training content</li> </ul>

## XI. AUDIT CONCLUSIONS AND AUDIT RECOMMENDATIONS

### AUDIT CONCLUSION

The Information Security Management System conforms with the requirements of ISO/IEC 27001:2022. SMT Data has implemented adequate internal controls to support implementation and maintenance of the ISMS.



























#	CONTROL OBJECTIVE & DESCRIPTION	STATUS OF FINDING	AUDIT EVIDENCE (FINDING & ITS JUSTIFICATION)
			It was observed that there are a few redundant rules and some rules that have neither destination port nor destination port defined for outbound connection. As a best practice redundant and duplicate rules should be cleaned up periodically.
A.8.21	<p><b>Security of network services</b></p> <p><b>Control.</b> Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.</p>		<ul style="list-style-type: none"> <li>- System and Network Management Policy</li> <li>- VPC firewall rules</li> <li>- Product network architecture diagram</li> </ul>
A.8.22	<p><b>Segregation of networks</b></p> <p><b>Control.</b> Groups of information services, users and information systems shall be segregated in the organization's networks.</p>		<ul style="list-style-type: none"> <li>- System and Network Management Policy</li> <li>- List of Virtual Private Clouds</li> <li>- List of AWS organisation accounts</li> </ul>
A.8.23	<p><b>Web filtering</b></p> <p><b>Control.</b> Access to external websites shall be managed to reduce exposure to malicious content.</p>		<ul style="list-style-type: none"> <li>- System and Network Management Policy</li> <li>- I.COMM10 Block dropbox.docx</li> <li>- I.COMM10 Dropbox.com Block on Client.png</li> <li>- I.COMM09 Web Content Policy.pdf</li> </ul>
A.8.24	<p><b>Use of cryptography</b></p> <p><b>Control.</b> Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.</p>		<ul style="list-style-type: none"> <li>- Encryption Key Management Policy</li> <li>- Application data on transit configuration</li> <li>- Website data on transit configuration</li> <li>- db_encryption.jpg</li> <li>- db_dynamo.jpeg</li> <li>-</li> </ul>







## VI. AUDIT FINDINGS - INITIAL CERTIFICATION

### SUMMARY

Decrypt Compliance strives to be a responsive audit partner by promptly sharing any findings upon identification throughout the audit process to promote communication and alignment among all stakeholders. At closing meetings, audit findings and final conclusions of the audit team were presented to the auditee. Following the closing meeting, a Findings Report was provided to the client to facilitate the Findings Handling Process. Details regarding the findings, as well as their status as of the date of this report, are outlined below.

MAJOR NONCONFORMITIES	MINOR NONCONFORMITIES	OBSERVATIONS	OPPORTUNITIES FOR IMPROVEMENT
0	6	0	17

## VII. AUDIT FINDING DEFINITIONS

The evaluation of the audit findings is based on the following definitions, in accordance with ISO/IEC 17021-1:

- **MAJOR NON-CONFORMITY (MaNC):** A non-conformity that affects the capability of the management system to achieve the intended results.
- **MINOR NON-CONFORMITY (MiNC):** A non-conformity that does not affect the capability of the management system to achieve the intended results.
- **OBSERVATIONS (OBS):** Any issues which are likely to become a NC, if not treated until the next audit are marked as observations. No response is required.
- **OPPORTUNITY FOR IMPROVEMENT (OFI):** An opportunity for improvement is a finding that, should it go unaddressed, could result in more severe findings in subsequent reviews. An OFI can also be used to improve the management system as a whole or named processes. No response is required.











0100000011010010 RESPONSIVE0000001

100110000101101110011001000110111

RESILIENT 0100001000011001110101110111011011

10010000001101000011001010111001001

00010000001100111 RESPONSIBLE

011101000110100001100101001001001011101001

110010010000001110110

0100000011010010 RESPONSIVE0000001

110011000101

100110000101101110011001000110111

RESILIENT 0100001000011001110101110111011011

10010000001101000011001010111001001

00010000001100111 RESPONSIBLE

0111010001101000011001010010010010111010

110010010000001110110

110011000101

00011101101

DECRYPT

COMPLIANCE

decrypt.cpa  
info@decrypt.cpa