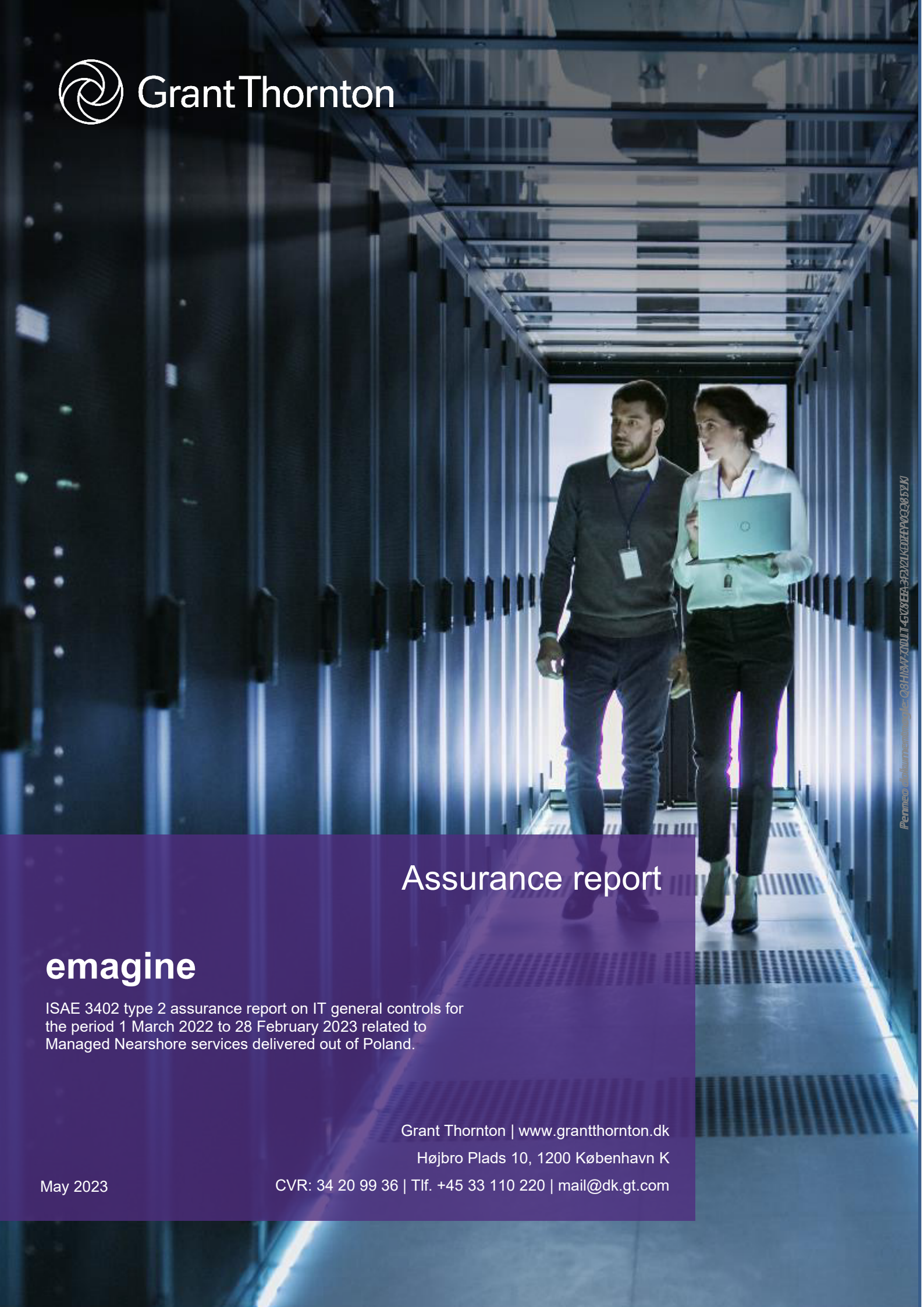


Assurance report

emagine

ISAE 3402 type 2 assurance report on IT general controls for the period 1 March 2022 to 28 February 2023 related to Managed Nearshore services delivered out of Poland.

Grant Thornton | www.grantthornton.dk
Højbro Plads 10, 1200 København K
CVR: 34 20 99 36 | Tlf. +45 33 110 220 | mail@dk.gt.com

May 2023

Table of contents

Section 1: Description of emagine Consulting A/S' (hereinafter referred to as "emagine") services in connection with operating of hosting-platform, and related IT general controls

Introduction

This Assurance Report covers the following ISO-27001:2013 controls:

4. Risk assessment and handling (limited to the physical security)
5. Information security policies (general policies)
6. Organization of information security (limited to 6.1)
7. Employee safety (7.1 and 7.2, with focus on screening and awareness training)
8. Asset management (limited to 8.1 and 8.3)
9. Access management (limited to 9.1, 9.2 (limited controls) and 9.3 in relation to staff with physical access/access to access card and video surveillance systems if applicable)
11. Physical hedging and environmental protection (primary area)
12. Reliability (limited to 12.4)
13. Communication security (limited to 13.1 in relation to segmentation and in relation to own Wi-Fi, etc.)
15. Supplier relationship (limited to relation to supplier of fibre)
16. Information security breach management (handling and reporting of security incidents)
17. Information security aspects of emergency, emergency, and recovery management (focus on the physical environment)
18. Internal compliance monitoring

The purpose of this document is to inform emagine's Clients and auditors about emagine's IT general controls and compliance measures implemented to meet the requirements listed in the international standard on assurance engagements, ISAE 3402. The description focuses on design and efficiency of emagine's IT general controls regarding the company's services rendered in Nearshore Centre, throughout the period of 1. March 2022 to 28. February 2023.

Furthermore, this document will outline specific security aspects related to the processing of data in the engagement between emagine and the customers, including a high-level description of how emagine's systems and processes support the rights of the registered individuals, and secure general compliance of emagine's services with legislative requirements such as GDPR.

Our Services

emagine's services are all related to helping customers acquire IT and Business consultants according to the customer's specific requirements. Services are delivered directly in all the countries where emagine operates, except for nearshore services which are supplied out of our locations in Poland and offshore services in India.

In addition to these services focusing individual consultants, emagine delivers Managed Services to a number of customers in several custom-made service offerings.

Customers place a request with emagine to supply several consultant CV's eligible for the specific request, and after interviewing the relevant candidates, contracts between the customer and emagine as well as between emagine and the consultant are agreed and executed.

In direct support of the consultant deliveries, emagine will register the delivered hours, follow-up on quality and invoice the services rendered.

All the above-mentioned services are supported by and registered in an internally developed ERP system named ProManagement (PM). For all process steps the required controls and implementation of the registered individuals' rights are supported by IT functionality.

General compliance with legislative requirements is reported and controlled by specific individuals appointed in the organization and audited by external professionals yearly.

Polices and processes in support of emagine's Information Security Management

Information Security policies and operations:

emagine implemented the following written policy framework to govern compliance to the scope of the Information Security Management System implemented.

Policies in the framework:

- Information Security Policy
- Access Control Policy
- Physical Security Policy
- Internet Acceptable Use Policy
- Cloud Computing Policy
- Teleworking Policy
- Social Media Policy
- Security Breach Policy
- Security Incident and Event Management Policy

Procedures implemented to support the policy framework:

- Asset Handling Procedure
- Information Labelling Procedure
- Change Management Procedure

All policies and procedures are reviewed once a year and updated by the Compliance Team. Employees are obligated to report any procedural discrepancies to the management of emagine. The updated policy framework is approved by CEO.

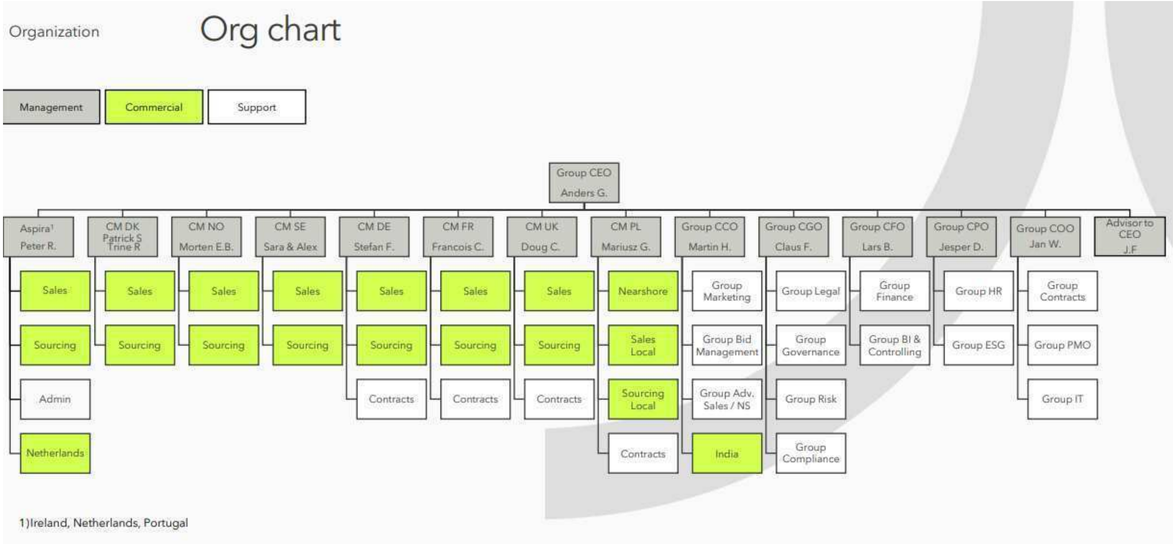
Risk Management

emagine conducts a Group level risk assessment as a foundation for determining relevant security policies and controls to mitigate identified risks. This document is a risk assessment of emagine risks in regard to information security. This document forms the basis for determining the content of emagine's risk management and internal control procedures in regard to information security.

Organization of Information Security

Internal Organization

To ensure consistency of the management of Information Security, IT security, and the inherited risk to Business Operations that rely on processing information assets, emagine implemented an organizational structure based on role segregation, clear accountability rules, governance of business development including IT change projects, and a sustainable and effective risk mitigating control environment.



The CEO is ultimately accountable for Information Security in emagine.

The COO role is responsible for management of Information Security in emagine. The COO is a member of the CxO group accountable for setting the directions and articulating targets for Business Development, Information and IT Security, and the day-to-day Business Operation. The CxO group meetings are set to discuss and decide on all principal questions regarding Information and IT security.

The COO and IT Director are accountable for the IT Operation, IT Security level, Change Advisory Board, and the IT teams. Representatives on the Change Advisory Board meetings are the business and IT change manager. Security events are logged on an ongoing basis and reported to the CxO group on the CxO group meetings.

All activities including daily work in emagine are based on written security policies, including the IT policy, with off set in the ISO 27001 standard, and the Employee Handbook to govern Information Security. The COO will, based on risk assessment minimum once a year or as consequence of major change, review and if necessary, update all implemented security policies and procedures to ensure sustainable compliance to external obligations, legal requirements, and contracts.

It is the responsibility of the employee's daily manager to communicate the updated content of the policies that relates to the work to be carried out on department level, ensure that procedures are followed, and risk mitigation controls documented. It's also the responsibility of the individual employee to report to the management of emagine if policies and procedures are not followed. Employees must as part of the onboarding procedure to all levels of the organization be trained in information security.

Information security roles and responsibilities

We have a clearly defined organization structure (see above). All information security responsibilities are defined and allocated. Comprehensive descriptions of roles and responsibilities are in place regarding all major roles, starting from management through the operations and support functions. At the same time, we have processes to handle key staff dependencies.

Grant Thornton

Human resource security

Prior to employment

Screening
We have procedures in place governing recruitment of employees and collaboration with externals ensuring that we recruit the right candidate based on background and skills. We have descriptions of roles and responsibilities for employees and employee categories to ensure that all employees are aware of their responsibilities. When joining the company, all employees are reviewed, and a registration form is followed.

Terms and conditions of employment
General terms of employment, including confidentiality regarding internal and customer matters, are described in each employee's employment contract where terms of all areas of the employment, including termination and sanctions in case of potential security breaches, are laid down.

During employment

Management responsibilities
In connection with employment, the new employee signs a contract. The contract states that the employee must observe the current policies and procedures. Moreover, it is clearly defined as part of the contract material what the employee's responsibilities and role comprise.

Disciplinary process
General terms of employment, including confidentiality about customer relationships, are described in each employee's employment contract, in which matters relating to all aspects of the employment, including termination and penalties in case of security breaches, are specified.

Termination or change of employment responsibilities.
In the event of termination of employment, we have a thorough procedure which must be observed to ensure that the employees return all relevant assets, including portable media, etc. and to ensure that all employees' access to buildings, systems and data are revoked. The overall responsibility for securing the performance of all controls related to the termination process lies with the company's COO.

General IT security

Asset Management

Inventory of assets
Managing the assets of emagine uniquely identifying software, servers, physical infrastructure, cloud solutions, and laptops is being done by having them inventoried and controlled in the configuration and by change management processes. The documentation is a core component in managing information security and is continuously updated and reviewed by the IT Department.

Ownership of assets
All production systems are hosted in Microsoft Azure. Central network devices, servers, peripherals, systems, and data are controlled by system administrators in emagine.

Asset protection and security is the accountability of the COO ensuring and overseeing clear ownership and classification of information asset.

Acceptable use of assets
Acceptable use of the assets is elaborated in the Employee Handbook as part of the onboarding procedure, and in our internal policies.

Return of assets
Offboarding procedure is in place and includes returning emagine's assets and revoking the provisioned role-based access rights to accommodation, systems, and information.

Management of removable media
emagine's internal IT department is accountable for secure configuration and maintenance of company's portable equipment, such as laptops, mobile phones and similar. Such protection is mandatory and includes necessary updates for media carrying data when new security measures are introduced.

Disposal of media
Reuse or disposal of all physical equipment carrying information assets erased or destroyed is enabled and handled only by the IT department. Hardware is destroyed by certified external company. Access Control

Access control policy
Access control is governed by the emagine's Access Control Policy and the IS-Policy, which outline the requirements for granting, modifying, and revoking access rights to our systems and data. The policies are reviewed at least once a year.

Access to network and network services
We have implemented process and controls to restrict access to our network, systems, and data to authorized individuals only.

User registration and de-registration
Users accounts are registered and unregistered in accordance with the formal procedure we have in place and implemented to enable assignment of access rights.

User access provisions
Access provisioning process has been established and is followed for each user. Based on our controls, it is the accountability of the business line manager to request provisioning and withdrawal of standard role-based access rights on behalf of the employee, with the target to limit access to information. The access is assigned and revoked by the IT team as requested by the business line manager, after IT team validation. All provisioning of access rights is segregated by duties.

Management of privileged access rights
Privileged access rights are granted in a restricted and controlled manner to the authorized personnel only. Such access is reviewed on a regular basis.

Management of secret authentication information of users
Initial password allocation and further requirements are controlled through Group's Access Control Policy. As a rule, all personal logons are only known by the individual employee.

Review of user access rights
The review of access rights is done at least once a year and is the accountability of the business line manager.

Removal or adjustment of access rights
Access rights are removed and adjusted immediately upon user's termination of employment at emagine or upon change of the role and thus the needed adjustment of the access scope.

We have defined procedure for external party users to our information assets ("Just-in-time").

User responsibilities

Use of secret authentication information
All users must follow emagine's practices and password requirements as described in Group's Access Control Policy. Users are required to keep their authentication information secret and are instructed never to share their passwords with anyone. Such requirements are also highlighted by regular information security trainings.

Physical and environmental security

Physical security perimeter

We have defined and used security perimeters to distinguish and appropriately protect areas where either sensitive or critical information can be stored. Our Physical Security Policy is applicable in this regard and for overall physical security on our premises.

Physical entry control

The physical building and access points are anti-theft protected with window and door locks, cameras, and access control mechanisms in two levels.

The first level of access control mechanism is the requirement of access key card and visitor registration including validation of identification artefact in the staffed reception area at the entrance to the building. The second level is applied at emagine’s accommodation facilities entrance and consists of access key card, badge, and biometric control.

Securing offices, rooms, and facilities

Physical security of our offices, rooms and facilities has been designed and applied accordingly. PL Nearshoring Centre is subject to additional internal procedures (higher security level) due to the nature of the work, and there are additional access control systems installed compared to other Group offices.

Protection against external and environmental threats

We have designed and applied physical protection against natural disasters, malicious attacks, or accidents.

Visitors are monitored by emagine’s employee, and they are never left unattended, including 3rd party service suppliers.

Maintenance and support plans are in place for the building security facilities. Written procedures are in place for issuing access permission and withdrawal thereof. Fire detection alarms and enlightened escape routes are in place. Evacuation plans, test and service plans and procedures are updated and available. Physical and environmental security is the responsibility of the Facilities Office Managers.

Equipment sitting and protection

Physical infrastructure and local servers are protected in locked rooms inside the premises to limit the risks of environmental hazards such as heat, fire, smoke, water, dust and vibrations, and unauthorized access. Locked cabinets, for example for laptop storage, are available and in usage.

Supporting utilities (security of supply)

We have an uninterruptible power supply (UPS) secured and in use.

Cabling security

All cabling is secured in a manner that prevents unauthorized access or tampering. Access to cabling is limited to authorized personnel only. Cabling is regularly inspected to ensure that it remains secure and in good shape.

Equipment maintenance

All equipment is regularly maintained in line with manufacturer recommendations and company policies.

Removal of assets

Assets are only removed from the premises with the prior approval management. Asset removal is documented and recorded.

Security of equipment and assets off-premises

Security has been applied to off-site assets considering the different risks of working outside the organization’s premises.

Secure disposal or re-use of equipment

All equipment is disposed of or re-used in a manner that is secure and complies with company policies and relevant legislation.

All items of equipment containing storage media are verified to ensure that any sensitive data and licensed software have been removed or securely overwritten prior to disposal or re-use.

Clear desk and clear screen policy

Computer screen lock is mandatory when computers are not in active use and attended by employees. Clear desk policy for paper files and removable storage media is enforced.

Operations security

Event logging

We maintain logs recording user activities exceptions, faults, and information security events. These logs are securely stored and monitored regularly.

Protection of log information

We take measures to protect logging facilities and log information from tampering an unauthorized access.

Administrator and operator logs

We maintain logs of system administrator and system operator activities to monitor and detect any potential misuse of privileges or unauthorized access. These logs are kept protected and reviewed.

Clock synchronization

Clock synchronization is an important aspect of operational security control. It ensures that all relevant systems and devices within the organization have accurate time stamps, which is critical for event logging, correlation, and investigation.

All relevant information processing system within our organization have been synchronised through the use of single reliable time source.

Installation of software on operational systems

We have procedures in place to monitor and control the installation of new and unauthorized software on operational systems.

Management of technical vulnerabilities

We are proactively identifying and addressing vulnerabilities in our systems and applications. This includes internal assessments and testing to identify potential weaknesses, prioritizing vulnerabilities based on risk and developing and implementing plans to remediate those vulnerabilities in a timely manner.

Communications security

Network security management

A physical topology separating infrastructure networks has been implemented, and all logins to management network segments require 2 factor authentication. Production networks may only be accessed from specific IP-addresses under IT Security governance.

We have set up monitoring and logging of network traffic followed and managed by our operations department.

Granting remote VPN connection with Multi Factor Authentication system access follows the formal procedure of access provisioning, after whitelisting and contracting the specific services, including 3rd party vendors.

Segregation of networks

Groups of information services users and information systems are segregated on networks. Use of portable devices is segregated from internal network and all access is governed via VPN connections.

Information security incident management

Responsibilities and procedures

We have established clear responsibilities and procedures for information security incident management to ensure a quick, effective, and orderly response to information security incidents. This includes defining roles and responsibilities for incident response team, as well as procedure for incident identification, assessment, and response.

We have defined a separate policy for security breaches involving personal data, so as to take appropriate steps that are proportionate to the data subjects' risks.

Technical measures are implemented to automatically detect and report any incidents, discrepancies, or deviations from normal operations of services. Designated members of the IT team monitor the potential threats on a regular basis. Moreover, all employees are obliged to report any potential incident, and they are informed about the channels they should use. This is especially the case for incidents that cannot be detected by technical and automated tools.

Reporting information security events

Information security incidents are being reported internally through designated channels as quickly as possible. Our data processors are obliged under the data processing agreements in place to report security events relevant to their processing in a timely manner allowing emagine as a data controller for evaluation and response, as well as reporting to the authorities if needed in due time.

Reporting security weaknesses

Employees and Clients using emagine's information systems and services are encouraged to inform the IT or Compliance team about any security weakness they may identify from their own observations. Such reports are assessed at CAB meetings and given priority if needed.

Assessment of and decision on information security events

Information security events are assessed, and it is decided if they are to be classified as information security incidents. This includes evaluating the potential impact of the incident and determining the root cause of the incident. Monitoring and assessment of events and potential information security breaches is processed in a weekly CAB meeting revisiting all events from the Operations-log and securing RCA and mitigations are being implemented.

Response to information security incidents

Our Incident Response Team follows established procedures for responding to information incidents, including containing the incident to prevent further damage, collecting evidence, and restoring affected systems and data to a secure state.

Should the operational staff determine a possible information security breach, the Information Security Incident response procedure will be initiated.

Information security aspects of business continuity management

Planning information security continuity

The needs and requirements for information security continuity in case of various adverse events, such as internet local power failure, internet failover, emergency re-location etc., have been evaluated and decided upon. The aim of our business continuity planning is to restore full operational status, i.e., the availability and integrity of core services, as quickly as possible, following any business activity interruption.

Implementing information security continuity

Data protection and Business continuity is implemented to meet a strategic target of recovering business functionality within 3 hours and with a potential data loss minimized to 15 min. Processes, procedures, and controls to ensure the required level of continuity for information security during an adverse situation are established, documented, implemented, and maintained.

Verify review and evaluate information security continuity

We verify on a regular basis the established and implemented information security continuity controls to ensure that they are valid and effective during adverse situations.

Compliance

emagine continuously develop the scope of compliance, and currently deploy the following standards which are regularly audited by external professionals:

- ISAE3000 GDPR
- ISAE3402 Operations
- ISO14001 (Poland, Denmark, Norway, in progress – the whole Group)
- ISO9001 (Poland, Denmark, Norway, in progress – the whole Group)
- ISO 27001 (currently Germany, France, UK, planned - certification of the whole Group)
- TISAX (Germany)

Significant changes during the period

Throughout the period. of 1. March 2022 to 28. February 2023, we have undergone the following significant changes:

- Infrastructure topology was updated to M354 E5 Security and all communication protocols were updated to VPN and MFA protocols,
- The System platform PM was upgraded according to overall Roadmap releasing Request-Module, Sourcing-Module, and new Integrated CRM functionality.

Complimentary Controls

In support of emagine's security and control measures, an important responsibility lies with our Clients in the Nearshore facility to administer and communicate the following controls on personnel and access control.

- Authentication of users in the client's domain
- Authorization of the user's access
- Monitoring of users starting or ending their employment with the Client.
- Information of and training in the Clients specific Security Controls if any.
- Revocation of authorization

The execution and results of these controls are communicated to emagine's personnel administering the physical issuance and governance of Access control cards to clients secured areas.

Section 2: emagine Consulting A/S' (hereinafter referred to as "emagine") statement

The accompanying description has been prepared for customers who have used emagine's hostingplatform, and their auditors who have a sufficient understanding to consider the description along with other information about controls operated by customers themselves, when obtaining an understanding of customers' information systems relevant to financial reporting.

emagine confirms that:

(a) The accompanying description in Section 1 fairly presents the IT general controls related to emagine's hostingplatform, processing customer transactions throughout the period 1 March 2022 to 28 February 2023. The criteria used in making this statement were that the accompanying description:

  (i) Presents how the system was designed and implemented, including:
  - The type of services provided
  - The procedures within both information technology and manual systems, used to manage IT general controls
  - Relevant control objectives and controls designed to achieve these objectives
  - Controls that we assumed, in the design of the system, would be implemented by user entities, and which, if necessary, to achieve the control objectives stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved by us alone
  - Other aspects of our control environment, risk assessment process, information system and communication, control activities, and monitoring controls that were relevant to IT general controls

  (ii) Contains relevant information about changes in the IT general controls, performed during the period 1 March 2022 to 28 February 2023

  (iii) Does not omit or distort information relevant to the scope of the system being described, while acknowledging that the description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the system that each individual customer may consider important in their own particular environment

(b) The controls related to the control objectives stated in the accompanying description were suitably designed and functioning during the period 1 March 2022 to 28 February 2023. The criteria used in making this statement were that:

  (i) The risks that threatened achievement of the control objectives stated in the description were identified

  (ii) The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved

  (iii) The controls were used consistently as drawn up, including the fact that manual controls were performed by people of adequate competence and authorization, during the period from 1 March 2022 to 28 February 2023

Copenhagen, 9 May 2023
emagine

Anders Gratte
CEO

Section 3: Independent service auditor's assurance report on the description of controls, their design and functionality

To emagine Consulting A/S, (hereinafter referred to as "emagine"), their customers and their auditors.

Scope

We have been engaged to report on emagine's description in Section 1 of its system for delivery of emagine's services throughout the period 1 March 2022 to 28 February 2023 (the description) and on the design and operation of controls related to the control objectives stated in the description.

Some of the control objectives stated in emagine's description in Section 1 of IT general controls, can only be achieved if the complementary controls with the customers have been appropriately designed and works effectively with the controls with emagine. The report does not include the appropriateness of the design and operating effectiveness of these complementary controls.

emagine's responsibility

emagine is responsible for preparing the description (section 1) and accompanying statement (section 2) including the completeness, accuracy, and method of presentation of the description and statement. Additionally, emagine is responsible for providing the services covered by the description; stating the control objectives; and for the design, implementation, and effectiveness of operating controls for achieving the stated control objectives.

Grant Thornton's independence and quality control

We have complied with the independence and other ethical requirements of the International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants (IESBA Code), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour and ethical requirements applicable to Denmark.

Grant Thornton applies International Standard on Quality Control 1[1] and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Auditor's responsibility

Our responsibility is to express an opinion on emagine's description (Section 1) as well as on the design and operation of the controls related to the control objectives stated in that description based on our procedures. We conducted our engagement in accordance with ISAE 3402, "Assurance Reports on Controls at a Service Organisation", issued by International Auditing and Assurance Standards Board.

This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are suitably designed and operating effectively.

[1] ISQC 1, Quality control for firms that perform audits and reviews of financial statements, and other assurance and related services engagements.

An assurance engagement to report on the description, design, and operating effectiveness of controls at a service organisation involves performing procedures to obtain evidence about the disclosures in the service organisation's description of its system, and the design and operating effectiveness of controls. The procedures selected depend on the service auditor's judgement, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved.

An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein, and the suitability of the criteria specified by the service organisation in section 2.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Limitations of controls at a service organisation

emagine's description in section 1, is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the systems that each individual customer may consider important in their own particular environment. Also, because of their nature, controls at a service organisation may not prevent or detect all errors or omissions in processing or reporting transactions.

Furthermore, the projection of any functionality assessment to future periods is subject to the risk that controls with service provider can be inadequate or fail.

Opinion

Our opinion has been formed based on the matters outlined in this report. The criteria we used in forming our opinion were those described in emagine's statement in Section 2 and based on this, it is our opinion that:

(a) The description of the controls, as they were designed and implemented throughout the period 1 March 2022 to 28 February 2023, is fair in all material respects.
(b) The controls related to the control objectives stated in the description were suitably designed throughout the period 1 March 2022 to 28 February 2023 in all material respects.
(c) The controls tested, which were the controls necessary for providing reasonable assurance that the control objectives in the description were achieved in all material respects, have operated effectively throughout the period 1 March 2022 to 28 February 2023.

Description of tests of controls

The specific controls tested, and the nature, timing and results of these tests are listed in the subsequent main section (Section 4) including control objectives, test, and test results.

Intended users and purpose

This assurance report is intended only for customers who have used emagine and the auditors of these customers, who have a sufficient understanding to consider the description along with other information, including information about controls operated by customers themselves. This information serves to obtain an understanding of the customers' information systems, which are relevant for the financial reporting.

Copenhagen, 9 May 2023

Grant Thornton
State Authorised Public Accountants

Kristian Randløv Lydolph State Authorised Public Accountant	Basel Rimon Obari Executive director, CISA, CISM

Section 4: Control objectives, controls, and service auditor testing

4.1. Purpose and scope

A description and the results of our tests based on the tested controls appear from the tables on the following pages. To the extent that we have identified significant weaknesses in the control environment or deviations therefrom, we have specified this.

Controls, which are specific to the individual customer solutions, or are performed by emagine Consulting A/S (hereinafter referred to as "emagine") customers, are not included in this report.

4.2. Tests

We performed our test of controls at emagine, by taking the following actions:

Method	General description
Inquiries	Interview with appropriate personnel at emagine regarding controls.
Observation	Observing how controls are performed.
Inspection	Review and evaluation of policies, procedures and documentation concerning the performance of controls. This includes reading and assessment of reports and documents in order to evaluate whether the specific controls are designed in such a way, that they can be expected to be effective when implemented. Further, it is assessed whether controls are monitored and controlled adequately and with suitable intervals.
Re-performance	Re-performance of controls in order to verify that the control is working as assumed.

4.3. Results of tests

Below, we have listed the tests performed by Grant Thornton as basis for the evaluation of the IT general controls with emagine.

A.5 Information security policies			
A.5.1 Management direction for information security Control objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations			
No.	***emagine's control***	***Grant Thornton's test***	***Test results***
5.1.1	*Policies for information security* A set of policies for information security is defined and approved by management, and then published and communicated to employees and relevant external parties.	We have inquired about the preparation of a risk analysis, and we have inspected the risk analysis. We have inquired about evaluation of the IT risk profile within the period, and we have inspected documentation that this has been reviewed and approved by management during the period. We have inspected the information security policy and we have inspected documentation for management approval of the information security policy.	No deviations noted.
5.1.2	*Review of policies for information security* The policies for information security are reviewed at planned intervals or if significant changes occur, to ensure their continuing suitability adequacy and effectiveness.	We have inspected that the information security policy has been reviewed to ensure that it still is suitable, adequate, and effective. We have inquired about evaluation of the IT risk profile within the period, and we have inspected documentation that this has been reviewed and approved by management during the period.	No deviations noted.

A.6 Organisation of information security

A.6.1 Internal organisation
Control objective: To establish a management framework to initiate and control the implementation and operation of information security within the organisation

No.	emagine's control	Grant Thornton's test	Test results
6.1.1	*Information security roles and responsibilities.* All information security responsibilities are defined and allocated.	We have inspected the organization chart. We have inspected the guidelines for information security roles and responsibilities.	No deviations noted.

A.7 Human ressource security

A.7.1 Prior to employment
Control objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered

No.	emagine's control	Grant Thornton's test	Test results
7.1.1	*Screening* Background verification checks on all candidates for employment is being carried out in accordance with relevant laws regulations and ethics and are proportional to the business requirements the classification of the information to be accessed and the perceived risks.	We have inquired into the procedure for employment of new employees and the security measures needed in the process. We have by sample test inspected documentation that new employees have been screened during the period.	We have been informed that for seven samples out of ten, documentation for screening of new employees has been deleted in accordance with the controller's retention scheme. No further deviations noted.
7.1.2	*Terms and conditions of employment* The contractual agreements with employees and contractors are stating their and the organisation's responsibilities for information security.	We have by sample test inspected a selection of contracts with employees and consultants in order to determine whether these are signed by the employees. We have by sample test inspected that the onboarding process has been followed during the period.	No deviations noted.

A.7.2 During employment Control objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities			
No.	**emagine's control**	**Grant Thornton's test**	**Test results**
7.2.1	*Management responsibility* Management is requiring all employees and contractors to apply information security in accordance with the established policies and procedures of the organisation.	We have inquired about procedure concerning establishing requirements for employees and partners. We have inquired into whether management has required that employees follow the IT-security policy	No deviations noted.
7.2.2	*Information security awareness education and training* All employees of the organisation and where relevant contractors, are receiving appropriate awareness education and training and regular updates in organisational policies and procedures as relevant for their job function.	We have inquired about procedures to secure adequate training and education (awareness training). We have inspected documentation for activities developing and maintaining security awareness with employees.	No deviations noted.
7.2.3	*Disciplinary process* There is a formal and communicated disciplinary process in place, to act against employees who have committed an information security breach.	We have inspected sanctioning guidelines and ensured that the employees can be sanctioned.	No deviations noted.

A.7.3 Termination and change of employment Control objective: To protect the organisation's interests as part of the process of changing or terminating employment			
No.	***emagine's control***	***Grant Thornton's test***	***Test results***
7.3.1	*Termination or change of employment responsibility* Information security responsibilities and duties that remain valid after termination or change of employment have been defined, communicated to the employee or contractor, and enforced.	We have inquired about employees and contractors' obligation to maintain information security in connection with termination of employment. We have by sample test ensured that confidentiality is enforced in regard to employees.	No deviations noted.

A.8 Asset management

A.8.1 Responsibility for assets
Control objective: To identify organisational assets and define appropriate protection responsibilities

No.	emagine's control	Grant Thornton's test	Test results
8.1.1	*Inventory of assets* Assets associated with information and information processing facilities have been identified and an inventory of these assets has been drawn up and maintained.	Vi have inspected records of assets and ensured that relevant assets have been identified.	No deviations noted.
8.1.2	*Ownership of assets* Assets maintained in the inventory are being owned.	We have inspected record of asset ownership and ensured that relevant assets have an assigned owner.	No deviations noted.
8.1.3	*Acceptable use of assets* Rules for the acceptable use of information and of assets associated with information and information processing facilities are being identified, documented, and implemented.	We have inquired about asset use guidelines, and we have inspected the guidelines.	No deviations noted.
8.1.4	*Return of assets* All employees and external party users are returning all the organisational assets in their possession upon termination of their employment contract or agreement.	We have inquired into the procedure for securing the return of assets, and we have inspected the procedure. We have by sample test inspected the return of assets during the period, in order to ensure that the procedure has been followed.	No deviations noted.

A.8.3 Media handling Control objective: To prevent unauthorised disclosure, modification, removal, or destruction of information stored on media			
No.	***emagine's control***	***Grant Thornton's test***	***Test results***
8.3.1	*Management of removable media* Procedures have been implemented for the management of removable media in accordance with the classification scheme adopted by the organisation.	We have inspected the guidelines for transportable media, and we have inspected documentation for the implementation.	We have been informed that no media has been removed during the period and therefore we have not been able to test the effectiveness of the company's procedures. No deviations noted.
8.3.2	*Disposal of media* Media are being disposed of securely when no longer required using formal procedures.	We have inquired about media disposal guidelines. We have inquired about equipment destroyed during the period	We have been informed that no media has been removed during the period and therefore we have not been able to test the effectiveness of the company's procedures. No deviations noted.

A.9 Access control

A.9.1 Business requirements of access control Control objective: To limit access to information and information processing facilities			
No.	***emagine's control***	***Grant Thornton's test***	***Test results***
9.1.1	*Access control policy* An access control policy has been established, documented, and reviewed based on business and information security requirements.	We have inquired into the policy of managing access control in order to establish whether it is updated and approved.	No deviations noted.
9.1.2	*Access to network and network services.* Users are only being provided with access to the network and network services that they have been specifically authorized to use.	We have inquired about managing access to networks and network services, and we have inspected the solution. We have inspected list of users and inspected documentation for work-related need for access.	No deviations noted.

A.9.2 User access management Control objective: To ensure authorised user access and to prevent unauthorised access to systems and services.			
No.	***emagine's control***	***Grant Thornton's test***	***Test results***
9.2.1	*User Registration and de-registration* A formal user registration and de-registration process has been implemented to enable assignment of access rights.	We have inspected the procedure for access management. We have by sample test inspected documentation for user registration and de-registration of users during the period.	No deviations noted.
9.2.2	*User access provisioning* A formal user access provisioning process has been implemented to assign or revoke access rights for all user types to all systems and services	We have inspected the procedure for access control. We have by sample test inspected documentation for user registration during the period.	No deviations noted.
9.2.3	*Management of privileged access rights* The allocation and use of privileged access rights have been restricted and controlled.	We have inquired about procedures for allocation of user rights, use and limitation of privileged access rights. We have inspected a sample of privileged users to establish whether the procedure has been followed.	No deviations noted.
9.2.4	*Management of secret-authentication information of users* The allocation of secret authentication information is controlled through a formal management process.	We have by sample test inspected implementation of password requirements.	No deviations noted.
9.2.5	*Review of user access rights* Asset owners are reviewing user's access rights at regular intervals.	We have inquired into review of user access during the period. We have inspected a sample of review of user access during the period.	We have observed that the user review has only included review of the list of users. We have observed that the system owner has not signed off the review of users. No further deviations noted.

No.	emagine's control	Grant Thornton's test	Test results
9.2.6	*Removal or adjustment of access rights* Access rights of all employees and external party users to information and information processing facilities are being removed upon termination of their employment contract or agreement or adjusted upon change.	We have inquired into procedures about discontinuation and adjustment of access rights. We have by sample test inspected a list of resigned employees and we have inspected whether their access rights have been removed.	No deviations noted.

A.9.3 User responsibilities Control objective: To make users accountable for safeguarding their authentication information			
No.	***emagine's control***	***Grant Thornton's test***	***Test results***
9.3.1	*Use of secret authentication information.* Users are required to follow the organisations' s practices in the use of secret authentication information.	We have inspected the policy for passwords. We have by sample test inspected password and by sample test ensured that it is implemented in accordance with the guidelines.	No deviations noted.

A.11 Physical and environmental security			
A.11.1 Secure areas Control objective: To prevent unauthorised physical access, damage and interference to the organisation's information and information processing facilities			
No.	***emagine's control***	***Grant Thornton's test***	***Test results***
11.1.1	*Physical security perimeter* Security perimeters have been defined and used to protect areas that contain either sensitive or critical information and information.	We have inspected the policy for physical security. We have inspected documentation for implementation of the policy.	No deviations noted.
11.1.2	*Physical entry control* Secure areas are protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	We have inspected access to selected server rooms.	No deviations noted.
11.1.3	*Securing offices, rooms, and facilities* Physical security for offices rooms and facilities has been designed and applied.	We have inspected the policy for physical security. We have inspected documentation for implementation of the policy.	No deviations noted.
11.1.4	*Protection against external and environmental threats.* Physical protection against natural disasters, malicious attack or accidents has been designed and applied.	We have inspected documentation for protection against external and environmental threats.	No deviations noted.

A.11.2 Equipment Control objective: To prevent loss, damage, theft or compromise of assets and interruption to the organisation’s operations			
No.	***emagine’s control***	***Grant Thornton’s test***	***Test results***
11.2.1	*Equipment sitting and protection* Equipment is sited and protected to reduce the risks from environmental threats and hazards and opportunities for unauthorized access.	We have inquired into the procedure concerning placement and protection of equipment. We have inspected selected equipment.	No deviations noted.
11.2.2	*Supporting utilities (security of supply)* Equipment is protected from power failures and other disruptions caused by failures in supporting utilities.	We have inspected documentation for test of UPS during the period.	No deviations noted.
11.2.3	*Cabling security* Power and telecommunications cabling carrying data or supporting information services are being protected from interception	We have inspected the protection of selected power and telecommunications cabling in order to establish whether the cables are secure.	No deviations noted.
11.2.4	*Equipment maintenance* Equipment is being correctly maintained to ensure its continued availability and integrity.	We have by sample test inspected service reports concerning maintenance of selected equipment, in order to determine whether relevant equipment has been maintained.	No deviations noted.
11.2.5	*Removal of assets* Equipment information or software is not taken off-site without prior authorization.	We have inspected the policy for asset removal. We have inquired about removal of equipment and assets.	We have been informed that there has been no removal of assets during the period and therefore we have not been able to test the effectiveness of the company's procedures. No deviations noted.
11.2.6	*Security of equipment and assets off-premises* Security has been applied to off-site assets taking into account the different risks of working outside the organisation’s premises.	We have inspected the policy for acceptable use. We have inquired about securing of equipment and assets outside the company’s premises.	No deviations noted.

No.	emagine’s control	Grant Thornton’s test	Test results
11.2.7	*Secure disposal or re-use of equipment* All items of equipment containing storage media have been verified to ensure that any sensitive data and licensed software have been removed or securely overwritten prior to disposal or re-use.	We have inspected the procedure for handling assets. We have inquired about destroyed equipment during the period.	We have been informed that there has been no removal of media during the period and therefore we have not been able to test the effectiveness of the company's procedures. No deviations noted.
11.2.9	*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 has been adopted.	We have inquired into the policy of tidy desk and clear screen. We have inspected documentation for mandatory screen saver.	No deviations noted.

A.12 Operations security

A.12.4 Logging and monitoring
Control objective: To record events and generate evidence

No.	emagine’s control	Grant Thornton’s test	Test results
12.4.1	*Event logging* Event logs recording user activities exceptions faults and information security events shall be produced, kept, and regularly reviewed.	We have by sample test inspected logging of user activity regarding the physical security.	No deviations noted.
12.4.2	*Protection of log information* Logging facilities and log information are being protected against tampering and unauthorized access.	We have inquired into a selection of logging configurations in order to establish whether login information is protected against manipulation and unauthorized access.	No deviations noted.

No.	emagine's control	Grant Thornton's test	Test results
12.4.3	*Administrator and operator logs* System administrator and system operator activities have been logged and the logs are protected and regularly reviewed.	We have by sample test inspected logs on the doors, in order to establish whether the actions of administrators are logged.	No deviations noted.
12.4.4	*Clock synchronization* The clocks of all relevant information processing systems within an organisation or security domain have been synchronised to a single reference time source.	We have inquired into synchronization against a reassuring time server, and we have inspected the solution.	No deviations noted.

A.13 Communications security

A.13.1 Network security management
Control objective: To ensure the protection of information in networks and its supporting information processing facilities

No.	emagine's control	Grant Thornton's test	Test results
13.1.1	*Network controls* Networks are managed and controlled to protect information in systems and applications.	We have inspected the guidelines for network equipment and ensured that it covers relevant areas.	No deviations noted.
13.1.2	*Security of network services* Security mechanisms service levels and management requirements of all network services are identified and included in network services agreements whether these services are provided in-house or outsourced.	We have inspected documentation that the internal network is behind a firewall.	No deviations noted.

No.	emagine's control	Grant Thornton's test	Test results
13.1.3	*Segregation of networks* Groups of information services users and information systems are segregated on networks.	We have inspected a range of network components in order to establish that the network is segregated	No deviations noted.

A.15 Supplier relationships

A.15.1 Information security in supplier relationships
Control objective: To ensure protection of the organisation's assets that are accessible by suppliers

No.	emagine's control	Grant Thornton's test	Test results
15.1.1	*Information security policy for supplier relationships* Information security requirements for mitigating the risks associated with supplier's access to the organisation's assets have been agreed with the supplier and documented.	We have inspected policies for supplier relations.	No deviations noted.
15.1.2	*Addressing security within supplier agreements* All relevant information security requirements are established and agreed with each supplier that may access process store communicate or provide IT infrastructure components for the company's information.	We have inspected a list of suppliers. We have by sample test inspected data processing agreements with suppliers	No deviations noted.

15.2 Supplier service delivery management Control objective: To maintain an agreed level of information security and service delivery in line with supplier agreements			
No.	***emagine's control***	***Grant Thornton's test***	***Test results***
15.2.1	*Monitoring and review of third-party services* Organisations are regularly monitoring review and audit supplier service delivery.	We have inquired into whether the procedure for monitoring and review of services from subcontractors is according to the contract. We have inspected documentation for audit of relevant suppliers during the period.	No deviations noted.

A.16 Information security incident management

A.16.1 Management of information security incidents and improvements Control objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses			
No.	***emagine's control***	***Grant Thornton's test***	***Test results***
16.1.1	*Responsibilities and procedures* Management responsibilities and procedures are established to ensure a quick effective and orderly response to information security incidents.	We have inquired about the responsibilities and procedures of information security incidents, and we have inspected documentation for the distribution of responsibilities. Further, we have inspected the procedure for handling information security incidents.	No deviations noted.
16.1.2	*Reporting information security events* Information security events are being reported through appropriate management channels as quickly as possible.	We have inquired into guidelines for reporting information security incidents and weaknesses, and we have inspected the guidelines. We have by sample test inspected that information security events have been responded to, in accordance with the documented procedures.	No deviations noted.

No.	emagine's control	Grant Thornton's test	Test results
16.1.3	*Reporting security weaknesses* Employees and contractors using the organisation's information systems and services are required to note and report any observed or suspected information security weaknesses in systems or services.	We have inspected the procedure for reporting incidents, and we have ensured that employees are obligated to rapport incidents.	No deviations noted.
16.1.4	*Assessment of and decision on information security events* Information security events are assessed, and it is decided if they are to be classified as information security incidents.	We have inquired into the procedure for assessment, response, and evaluation of information security breaches. We have by sample test inspected the ongoing control of incidents during the period.	No deviations noted.
16.1.5	*Response to information security incidents* Information security incidents are responded to in accordance with the documented procedures.	We have inquired about information security incidents in the period.	We have been informed that there have not been any incidents during the period, and we have therefore not been able to test the effectiveness of the procedures. No deviations noted.

A.17 Information security aspects of business continuity management

A.17.1 Information security continuity
Control objective: Information security continuity should be embedded in the organisation's business continuity management systems

No.	emagine's control	Grant Thornton's test	Test results
17.1.1	*Planning information security continuity* Requirements for information security and the continuity of information security management in adverse situations e.g., during a crisis or disaster has been decided upon.	We have inquired about the preparation of a contingency plan to ensure the continuation of operations in the event of crashes and the like, and we have inspected the plan.	No deviations noted.

No.	emagine's control	Grant Thornton's test	Test results
17.1.2	*Implementing information security continuity* Processes procedures and controls to ensure the required level of continuity for information security during an adverse situation are established, documented, implemented, and maintained.	We have inquired about procedures to ensure that all relevant systems are included in the contingency plan, and we have inspected that the contingency plan is properly maintained.	No deviations noted.
17.1.3	*Verify review and evaluate information security continuity* The established and implemented information security continuity controls are verified on a regular basis to ensure that they are valid and effective during adverse situations.	We have inquired about test of the BCP during the period.	We have observed that the BCP has not been tested during the period. No further deviations noted.

A.17.2 Redundancies Control objective: To ensure availability of information processing facilities			
No.	**emagine's control**	**Grant Thornton's test**	**Test results**
17.2.1	*Availability of information security processing facilities* Information processing facilities have been implemented with redundancy sufficient to meet availability requirements.	We have inquired about the availability of redundance and by sample test inspected that redundance has been tested in the period.	No deviations noted.

A.18 Compliance

A.18.2 Information security reviews
Control objective: To ensure that information security is implemented and operated in accordance with the organisational policies and procedures

No.	emagine's control	Grant Thornton's test	Test results
18.2.1	*Independent review of information security* Processes and procedures for information security) (control objectives, controls, policies, processes, and procedures for information security) are reviewed independently at planned intervals or when significant changes occur.	We have observed that independent evaluation of information security has been established.	No deviations noted.
18.2.2	*Compliance with security policies and standards* Managers are regularly reviewing the compliance of information processing and procedures within their area of responsibility with the appropriate security policies standards and any other security requirements.	We have inquired for internal controls to ensure compliance with security policies and procedures, and we have inspected selected controls.	No deviations noted.

PENNEO

The signatures in this document are legally binding. The document is signed using Penneo™ secure digital signature. The identity of the signers has been recorded, and are listed below.

"By my signature I confirm all dates and content in this document."

Anders Gratte
Underskriver 1

Pending Signature

Basel Obari
Underskriver 2

Pending Signature

Kristian Lydolph
Underskriver 3

Pending Signature

PENNEO

The signatures in this document are legally binding. The document is signed using Penneo™ secure digital signature. The identity of the signers has been recorded, and are listed below.

"By my signature I confirm all dates and content in this document."

ANDERS GRATTE
Underskriver 1
Serial number: 19740606xxxx
IP: 90.235.xxx.xxx
2023-05-14 11:02:58 UTC

Basel Rimon Obari
Underskriver 2
Serial number: 7a620960-cd2a-41f1-82f4-f2021d544570
IP: 62.243.xxx.xxx
2023-05-15 07:08:48 UTC

Kristian Lydolph
Underskriver 3
Serial number: CVR:34209936-RID:43340328
IP: 62.243.xxx.xxx
2023-05-15 09:31:24 UTC