Assurance report

emagine Consulting A/S

ISAE 3402 type 2 assurance report on IT general controls for the period from 1 March 2024 to 28 February 2025 related to physical security in Poland

May 2025

Grant Thornton | www.grantthornton.dk
Lautrupsgade 11, 2100 København Ø
CVR: 34 20 99 36 | Tlf. +45 33 110 220 | mail@dk.gt.com

Table of contents

Section 1: emagine Consulting A/S' statement

The accompanying description has been prepared for customers who have used emagine Consulting A/S' physical security in Poland, 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.

Some of the control areas, stated in emagine Consulting A/S' description in Section 3 of IT general controls, can only be achieved if the complementary user entity controls with the customers are suitably designed and operationally effective with emagine Consulting A/S' controls. This assurance report does not include the appropriateness of the design and operating effectiveness of these complementary user entity controls.

emagine Consulting A/S confirms that:

(a) The accompanying description in Section 3 fairly presents the IT general controls related to emagine Consulting A/S' physical security in Poland throughout the period from 1 March 2024 to 28 February 2025. 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 from 1 March 2024 to 28 February 2025

   (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 from 1 March 2024 to 28 February 2025 if the customers have performed the complementary controls, assumed in the design of emagine A/S' controls throughout the period from 1 March 2024 to 28 February 2025. 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 consistently applied as designed, including that manual controls were applied by individuals who have the appropriate competence and authority, throughout the period from 1 March 2024 to 28 February 2025

Copenhagen, 14 May 2025
emagine Consulting A/S

Anders Gratte
CEO

Section 2: Independent service auditor's assurance report on the description of controls, their design and operating effectiveness

To emagine Consulting A/S, their customers and their auditors.

Scope

We have been engaged to report on a) emagine Consulting A/S' description in Section 3 of its system for delivery of emagine Consulting A/S' physical security in Poland throughout the period from 1 March 2024 to 28 February 2025 and about (b+c)) the design and operational effectiveness of controls related to the control objectives stated in the description.

Some of the control objectives stated in emagine Consulting A/S' description in Section 3 of IT general controls, can only be achieved if the complementary user entity controls with the customers have been appropriately designed and works effectively with the controls with emagine Consulting A/S. The report does not include the appropriateness of the design and operating effectiveness of these complementary user entity controls.

emagine Consulting A/S' responsibility

emagine Consulting A/S is responsible for preparing the description (Section 3) and accompanying statement (Section 1) including the completeness, accuracy, and method of presentation of the description and statement. Additionally, emagine Consulting A/S 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 Management 1, ISQM 1, requiring that we maintain 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 Consulting A/S' description (Section 3) 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.

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 3.

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 Consulting A/S' description in Section 3, 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 Consulting A/S' statement in Section 1 and based on this, it is our opinion that:

(a) the description fairly presents how the IT general controls in relation to emagine Consulting A/S' physical security in Poland were designed and implemented throughout the period from 1 March 2024 to 28 February 2025.

(b) the controls related to the control objectives stated in the description were suitably designed and implemented throughout the period from 1 March 2024 to 28 February 2025 in all material respects, and

(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, operated effectively throughout the period from 1 March 2024 to 28 February 2025.

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 Consulting A/S' services and their physical premises in Warsaw 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, 14 May 2025

Grant Thornton
Godkendt Revisionspartnerselskab

Kristian Randløv Lydolph
State Authorised Public Accountant

Martin Brogaard Nielsen
Partner, CISA, CIPP/E, CRISC

Section 3: Description of emagine Consulting A/S' services in connection with operating of physical security in Poland, and related IT general controls

The purpose of this description is to inform emagine's clients and auditors about emagine Group's IT-controls and compliance measures implemented to meet the requirements listed in the international standard on assurance engagements, ISAE 3402. This description focuses on design and efficiency of emagine's IT-controls, including physical security, regarding the company's services rendered in emagine Nearshoring Centre in Warsaw, Poland, throughout the period from 1 March 2024 to 28 February 2025.

Specific security aspects related to the processing of personal data in the engagement between emagine Group and client, including a high-level description of how emagine Group's systems and processes support the rights of the registered individuals, and compliance of emagine Group's services with legislative data protection requirements, such as GDPR, are further described in Statement of Applicability ISAE 3000 documents.

Our Services

emagine Group services are all related to helping clients acquire IT and business consultants according to clients' specific requirements. Sectors with a strong presence include finance/banking, IT/telecom, energy, telecom, media, transport, and the public sector. Services are delivered directly in all the countries where emagine Group operates, as well as delivered through our Bestshore services which are supplied out of our locations in Poland, UAE, and India. Depending on the location of emagine's clients and supplied consultants, such Bestshore services can be further categorised as "Nearshore," "Offshore" or "Remote" consulting.

Clients place a request with emagine Group to supply a number of consultant profiles eligible for the specific request, and after interviewing the relevant candidates, contracts between the client and emagine Group, as well as between emagine Group and the consultant, are agreed and executed.

In direct support of the consultant services, emagine registers the delivered hours, does a follow-up on quality, and invoices the services rendered.

In addition to these services focusing on offering individual consultants' expertise, emagine Group delivers Managed Services to several clients in various custom-made service offerings.

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 functionalities.

General compliance with legislative requirements is reported and controlled by appointed internal employees in emagine Group and audited by external professionals on a yearly basis.

Polices and processes in support of emagine Group's information security management

Information security policies and operations
emagine Group implemented the following written policy framework to govern compliance to the scope of the information security management system.

Most important policies in the ISMS framework:

- Information security policy
- Access control policy
- Backup policy
- Change management policy
- Control of documented information
- Development and acquisition policy
- Encryption policy
- Group business continuity plan

- Group data protection policy
- HR disciplinary policy
- Information classification policy
- Information security & data protection awareness policy
- Information security compliance policy
- Information security governance policy
- Internal controls and audit policy
- ISMS policy
- IT asset management security policy
- IT charter for emagine employees
- IT devices and operation procedures
- Logging policy
- Operations security policy
- Personal data breach policy
- Physical security policy
- Security incident and event management policy
- Social media policy
- Supplier management policy
- Teleworking policy
- Threat intelligence policy

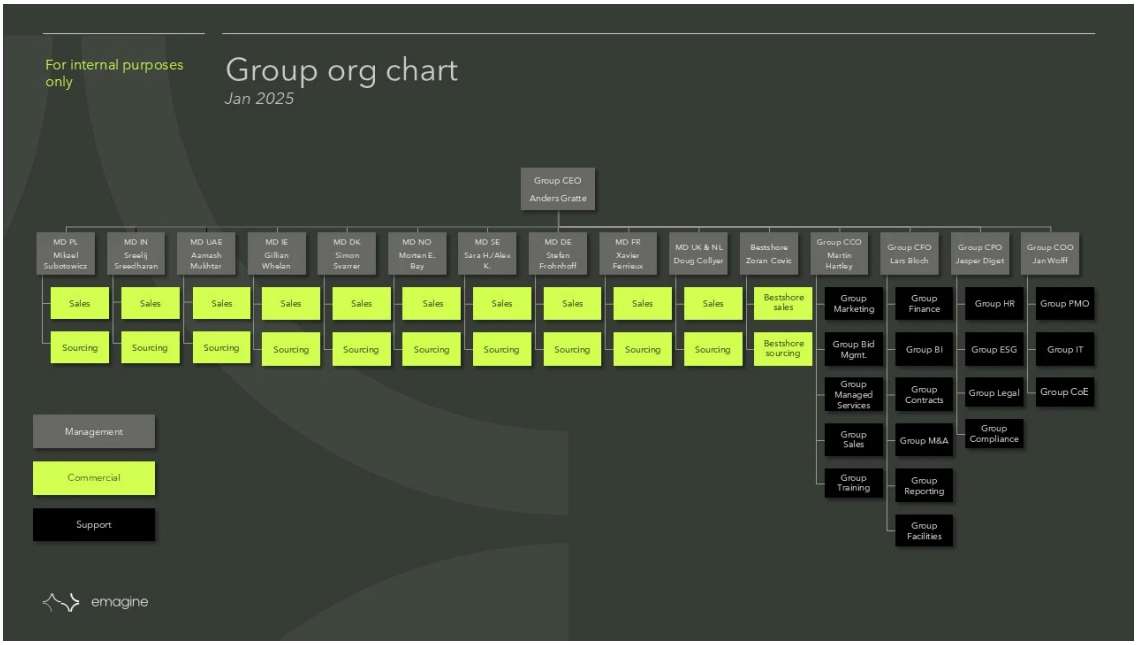
Risk management

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

Organisation of information security

Internal organisation

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 Group implemented an organisational 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 Group.

The COO role is responsible for management of information security in the Group. 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 Head of Security and Operations are accountable for the IT Operations, IT Security level, Change Advisory Board, and the IT Support Team.

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 Group are based on written security policies based on the ISO 27001 standard. Additionally, the Employee Handbook governs and provides guidelines in information security aspects.

The Compliance Team in cooperation with Head of Security and Operations and COO will, based on risk assessment done by COO 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 is also the responsibility of the individual employee to report to the management of emagine Group if policies and procedures are not followed. Employees at all levels of the organisation must as part of the onboarding procedure be trained in information security. Additionally, all the IS policies, contacts, and educational materials are available to emagine's internal employees on the Intranet on a rolling basis.

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.

Segregation of duties
Overlapping duties and areas of responsibility are segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisations' assets.

Teleworking
emagine's employees have the possibility of remote work in specified cases. We have implemented policy and supporting security measures to protect information accessed, processed, and stored at teleworking sites. The equipment allowed for teleworking usage has been defined. Portable devices are protected with logon and encryption. Virtual Private Network (VPN) must be used each time when connecting from remote site. Two-factor authentication is required when a connection comes from an unusual site.

Human resource security

Prior to employment

Screening
We have procedures in place governing recruitment of employees and collaboration with external professionals applying for the internal roles, ensuring that we recruit the right candidate based on background and skills needed. We have descriptions of main roles and responsibilities for employees and employee categories to ensure that all employees are aware of their duties. When joining the company, all employees are interviewed in a HR-owned process, and a registration form is followed.

Terms and conditions of employment
General terms of employment, including confidentiality regarding internal and customer matters, are governed by each employee's employment contract. Terms of employment, such as termination and sanctions in case of potential security breaches are laid down either in the contract, or in the work regulations that constitute the part of the employment relationship by the virtue of the law. In all instances employees are regularly reminded of their confidentiality and data security obligations by compulsory trainings and internal communication.

During employment

Management responsibilities
In connection with employment, the new employee signs a contract. The contract or accompanying work regulations explicitly state 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
The disciplinary process within our organisation is outlined in the Group HR Disciplinary Policy with the possible necessary modifications stipulated in the local legislation, which are then reflected in employment agreements or local work regulations. All employees are expected to comply with the organisation's information security policy and supporting policies. Information security policy details scenarios of possible data security infringements and associated disciplinary consequences.

Termination or change of employment responsibilities
In the event of termination of employment, we have defined a procedure that must be observed to ensure that the employees return all relevant assets, including portable media, and to ensure that all employees' access to buildings, systems and data are revoked. Post-termination confidentiality duty is binding on employees by virtue of direct contractual provisions and/or work regulations and national legislation. The overall responsibility for securing the performance of all controls related to the termination process lies with the company's COO and CPO.

General IT security

Asset management

Inventory of assets
Assets associated with information and information processing facilities, including physical infrastructure and laptops, are continuously identified and inventoried. These assets are controlled through configuration and change management processes. Records of assets are available and kept up to date.

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

Asset protection and security is the responsibility 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 Group'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 the 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 Group's Access Control Policy which outlines the requirements for granting, modifying, and revoking access rights to our systems and data. Additionally, our Physical Security Policy specifies physical access controls. Both 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 authorised individuals only. Network access is provisioned via a configuration profile automatically deployed during the device enrolment process. Network / technical rooms are classified as secure areas requiring special protection of access keys, according with our physical security policy.

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.

In relation to the physical security, valid access card is required to enter emagine's Warsaw office premises. Card provisioning, lifecycle and loss procedures have been described in our physical security policy.

Management of privileged access rights
Privileged access rights are granted in a restricted and controlled manner to the authorised 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 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
Each of emagine's physical offices and access points has implemented access control mechanisms at two levels.

The first level of access control is applied at the entrance to the building. Depending on the localisation it can include the key card requirement, and/or visitor registration and validation of ID in the staffed reception area. Buildings where emagine has its offices are anti-theft protected by door locks and building entrance areas and common areas such as elevators are CCTV-surveilled in most instances (including Nearshoring Centre in Poland).

The second level is applied at emagine's office entrance, and consists of either access key card, badge, or secret authentication code changed periodically. Additionally, CCTV and biometric controls are in place. For example, both are in place at the entrance to emagine PL Warsaw office spaces, whereas CCTV is used at the entrance to DK Copenhagen office spaces.

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 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 is 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 unauthorised access or tampering. Access to cabling is limited to authorised 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 organisation'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

Physical security events are logged, and evidence is generated and kept within configured setup. Logs cannot be changed, deleted, or manipulated.

Protection of log information

We take measures to protect logging facilities and log information from tampering an unauthorised 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 unauthorised access. These logs are kept protected and reviewed.

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.

Learning from information security incidents

After an information security incident has been resolved, a post-incident review is conducted to identify any possible lesson learned and areas of improvement. Depending on the scale and impact of the incident, the post-review evaluates the effectiveness of incident response procedures, potential gaps in security controls and provides a suggestion whether an update of incident response procedure is needed.

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 minimised 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 obligations

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

- ISAE3000 GDPR (DK – SE – NO – PL – FRA – UK – DE – NL – IE emagine entities)
- ISAE3402 Operations (emagine PL)
- ISO 27001 (DK – SE – NO – PL – FRA – UK – DE – NL – IE emagine entities)
- TISAX (emagine DE)
- ISO14001 (DK – SE – NO – PL – FRA – UK – DE – NL – IE emagine entities)
- ISO9001 (DK – SE – NO – PL – FRA – UK – DE – NL – IE emagine entities)
- ISO 45001 (DK – SE – NO – PL – FRA – UK – DE – NL – IE emagine entities)
- EcoVadis Platinum Medal

Changes during the period

Throughout the period from 1 March 2024 to 28 February 2025 we have undergone the following significant changes:

- Digitalising advanced threat protection and vulnerability reporting in Azure,
- Unifying Teams telephony across the group,
- Closing unsecure MFA Authentication methods (Mobile text/call),
- Implementing Evaluation Module in PM – for clients to have the opportunity to rate the services and quality provided by emagine and our consultants.
- Changing of finance & invoicing reporting system, from Navision to Business Central,
- Moving all files from Fileshares into SharePoint,
- Upgrading all devices to Windows 11.

Complementary user entity controls

In support of emagine 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 (consultants) in the client's domain
- Authorisation of the users' (consultants') access
- Monitoring of users (consultants) starting or ending their employment with the client
- Information of and training in the clients' specific security controls if any
- Revocation of authorisation

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

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

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' customers, are not included in this report.

Tests performed

We performed our test of controls at emagine Consulting A/S, by taking the following actions:

Method	General description
Inquiries	Interview with appropriate personnel at emagine Consulting A/S regarding controls. Inquiries have included questions on how controls are being performed.
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. The effectiveness of the controls during the audit period, is assessed by sample testing.
Re-performance	Re-performance of controls in order to verify that the control is working as assumed.

Test results

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

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 Consulting A/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 inspected that the information security policy contains relevant information. We have inspected that the risk assessment has identified risks relevant for the service and for the physical security in Poland. We have inspected that the information security policy is available for employees.	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 during the period. We have inspected documentation that management has approved the risk assessment.	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 Consulting A/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 that roles and responsibility for managing information security have been identified and that employees are required to follow them.	No deviations noted.

A.7 Human resource 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 Consulting A/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 inspected the procedure for screening of new employees. We have, by sample test, inspected documentation that screening documentation is being obtained on new employees during the audit period.	We have been informed that one (1) out of seven (7) samples of new employees for Poland, have not been tested with MPA and ACE in accordance with the Group policy. 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 in 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 Consulting A/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 inspected policies procedure concerning establishing requirements for employees and partners.	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 inspected documentation on activities developing and maintaining security awareness with employees during the period.	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 that sanctioning guidelines are communicated to the employees. We have by sample test inspected a selection of contracts with employees and consultants in order to determine whether these contains a provision of sanctions, in case employees fail to keep the organisation's policies and procedures.	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 Consulting A/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, inspected that confidentiality agreements are enforced.	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 Consulting A/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 that records of assets contain relevant assets in accordance with internal policy.	No deviations noted.
8.1.2	*Ownership of assets* Assets maintained in the inventory are being owned.	We have inspected that the record of asset ownership has an identified owner.	No deviations noted.

No.	emagine Consulting A/S' control	Grant Thornton's test	Test results
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 inspected that there are guidelines for acceptable use of assets and that the guidelines are available to employees.	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 inspected the procedure for securing the return of delivered assets. We have, by sample test, inspected the return of assets during the period.	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 Consulting A/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 and policies for transportable media.	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 destroyed equipment during the period.	We have been informed that no equipment has been destroyed. 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 Consulting A/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 inspected that the policy of managing access control 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 authorised to use.	We have inspected that the procedure for access management describes how to gain access to the network. We have, by sample test, inspected that users are identifiable in accordance with the procedure for accesses management.	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 Consulting A/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 user registration and de-registration We have, by sample test, inspected that granting and removal of access rights has followed the procedure. We have, by sample test, inspected withdrawal of physical access for terminated employees. We have, by sample test, inspected registration of physical access for new employees.	No deviations noted.

No.	emagine Consulting A/S' control	Grant Thornton's test	Test results
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 and de-registration of users 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 inspected procedures for allocation of user rights, use and limitation of privileged access rights. We have inspected list of administrators for selected systems for physical access control.	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 inspected two examples of the process for handing out passwords. We have inspected the password policy.	No deviations noted.
9.2.5	*Review of user access rights.* Asset owners are reviewing user's access rights at regular intervals	We have inspected the control for access review for physical security.	No deviations noted.
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 inspected procedures for discontinuation and adjustment of access rights. We have, by sample test, inspected that terminated employees have had their access rights removed and their access cards revoked.	No deviations noted.

A.9.3 User responsibilities Control objective: To make users accountable for safeguarding their authentication information			
No.	***emagine Consulting A/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 inspected that the password policy 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 Consulting A/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, by sample test, inspected documentation physical security for office facilities in Poland.	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 points to establish, whether personal access cards are used to gain access to the office. We have inspected that alarms have been installed for physical access control.	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 access to selected facilities in Poland offices. We have inspected that offices, facilities and rooms are secured with physical access control.	No deviations noted.

No.	emagine Consulting A/S' control	Grant Thornton's test	Test results
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 service reports concerning maintenance of selected equipment, in order to determine whether relevant equipment has been maintained. We have, by sample test, inspected that selected equipment is protected from potential natural disasters.	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 Consulting A/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 the location of 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 procedures for protection of equipment. We have inspected documentation for a test of UPS within the audit 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 that power- and telecommunications cabling are protected against interception and damage.	No deviations noted.
11.2.4	*Equipment maintenance.* Equipment is being correctly maintained to ensure its continued availability and integrity.	We have inspected the policy for maintenance of equipment. We have inquired whether equipment has been maintained within the audit period.	We have been informed that no equipment has been maintained during the period, as it has not been necessary. No deviations noted.

No.	emagine Consulting A/S' control	Grant Thornton's test	Test results
11.2.5	*Removal of assets* Equipment information or software is not taken off-site without prior authorization.	We have inquired into guidelines for removal of equipment, information, and software from the company.	We have been informed that no assets have been removed during the audit period. 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 that handling of equipment is addressed in the policy for acceptable use. We have inspected that controls are implemented to secure assets off-premises.	No deviations noted.
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, by sample test, inspected handling of recycled assets during the period. We have inquired whether any equipment related to Poland has been destroyed within the audit period.	We have been informed that no equipment related to Poland operations has been destroyed within the audit period. 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 inspected the policy of tidy desk and clear screen. We have inspected documentation for enforced 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 Consulting A/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 in the system.	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 inspected a selection of logging configurations for physical security to establish whether login information is protected against manipulation and unauthorised access.	No deviations noted.
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, to establish whether the actions of administrators are logged.	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 Consulting A/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. We have inspected documentation for network design.	No deviations noted.

No.	emagine Consulting A/S' control	Grant Thornton's test	Test results
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, by sample test, inspected documentation that the internal network is protected by a firewall. We have inspected service agreements regarding network security	No deviations noted.
13.1.3	*Segregation of networks* Groups of information services users and information systems are segregated on networks.	We have inspected network charts, showing segregation of networks. We have inspected technical documentation that system environments are being segregated.	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 Consulting A/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 inspected that the procedure for handling incidents has distribution of responsibilities. We have inspected that the procedure has been maintained.	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 inspected that the procedure for handling incidents and events describes reporting of security events. We have, by sample test, inspected that the log have the required information.	No deviations noted.

No.	emagine Consulting A/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 that the procedure for handling incidents describes reporting of vulnerabilities. We have inspected the log of incidents. We have inquired about information security weaknesses during the period.	We have been informed that no security weaknesses have been reported. 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 inspected the log of incidents and events We have inspected how the incidents in the audit period have been handled and categorised.	We have inspected that one (1) out of two (2) relevant events do not have Severity Level indicated. We have been informed that there have been no information security breaches related to physical security in Poland. No further 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 breaches for physical security in Poland.	We have been informed that there have been no information security breaches related to Polands physical security. 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 Consulting A/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 inspected that the contingency plan to ensure the continuation of operations contains relevant systems and plans. We have inspected that the plan has been approved by management.	No deviations noted.
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 inspected that all relevant systems are included in the contingency plan. 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 inspected documentation that the plan has been tested during 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 Consulting A/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 inspected 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 inspected that internal compliance has been tested during the period.	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 Fredrik Gratte
Underskriver 1
Serial number: f37555ae-8ab8-4fb9-bfb4-4a1612b5332c
IP: 87.49.xxx.xxx
2025-05-14 14:21:11 UTC

Mit ID

Martin Brogaard Borup Nielsen
Grant Thornton, Godkendt Revisionspartnerselskab CVR: 34209936
Underskriver 2
Serial number: 658bcd61-1988-4367-b3eb-215cfbbb49b0
IP: 62.243.xxx.xxx
2025-05-14 14:23:41 UTC

Mit ID

Kristian Randløv Lydolph
Grant Thornton, Godkendt Revisionspartnerselskab CVR: 34209936
Underskriver 3
Serial number: 84758c07-82ce-4650-a48d-5224b246b5c4
IP: 62.243.xxx.xxx
2025-05-14 15:53:01 UTC

Mit ID