Assurance report

Sentia Denmark A/S

ISAE 3402 type 2 assurance report on the OSE (Operating System Environment) operated private and public cloud platforms, as well as for co-location, offered by Sentia, and related IT-general controls during the period 1 January 2023 to 31 December 2023

January 2024

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

Table of contents

Section 1: Sentia Denmark A/S' statement

The accompanying description has been prepared for customers who have used Sentia Denmark A/S' services, 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.

This assurance report is prepared in accordance with the carve-out method and Sentia Denmark A/S' description does not include control objectives and controls within relevant subservice organisations. Customers who have used Sentia Denmark A/S' services should refer to their specific supply agreement for detailed information.

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

Sentia Denmark A/S confirms that:

(a) The accompanying description in Section 3 fairly presents the IT general controls related to Sentia Denmark A/S' OSE (Operating System Environment) operated private and public cloud platforms, as well as for co-location, processing of customer transactions throughout the period 1 January 2023 to 31 December 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 January 2023 to 31 December 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 operationally effective during the period 1 January 2023 to 31 December 2023 if relevant controls with the sub-supplier were operationally effective and the customers have performed the complementary controls, assumed in the design of Sentia Denmark A/S' controls during the entire period from 1 January 2023 to 31 December 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 January 2023 to 31 December 2023

Herlev, 19 January 2024
Sentia Denmark A/S

Kim Madsen
Chairman of the Board

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

To Sentia Denmark A/S, their customers and their auditors.

Scope

We have been engaged to report on Sentia Denmark A/S' description in Section 3 of its system for delivery of Sentia Denmark A/S' services throughout the period 1 January 2023 to 31 December 2023 (the description) and on the design and operation of controls related to the control objectives stated in the description.

This assurance report is prepared in accordance with the carve-out method and Sentia Denmark A/S' description does not include control objectives and controls within relevant subservice organisations. Customers who have used Sentia Denmark A/S' services should refer to their specific supply agreement for detailed information.

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

Sentia Denmark A/S' responsibility

Sentia Denmark A/S is responsible for preparing the description in Section 3 and accompanying statement in Section 1 including the completeness, accuracy, and method of presentation of the description and statement. Additionally, Sentia Denmark 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 the International Standard on Quality Management 1, ISQM 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 Sentia Denmark A/S' description in 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.

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 1.

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

Sentia Denmark 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 Sentia Denmark A/S' statement in Section 1 and based on this, it is our opinion that:

(a) The description of the IT general controls, as they were designed and implemented throughout the period 1 January 2023 to 31 December 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 January 2023 to 31 December 2023 in all material respects, if controls with sup-suppliers were operationally effective and if the customers have designed and implemented the complementary controls assumed in the design of Sentia Denmark A/S' controls during the period 1 January 2023 to 31 December 2023.
(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 January 2023 to 31 December 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 4 including control objectives, test, and test results.

Intended users and purpose

This assurance report is intended only for customers who have used Sentia Denmark A/S 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, 19 January 2024

Grant Thornton
Godkendt Revisionspartnerselskab

Jacob Helly Juell-Hansen
State Authorised Public Accountant

Andreas Moos
Director, CISA, CISM

Section 3: Description of Sentia Denmark A/S' services in connection with the OSE (Operating System Environment) operated private and public cloud platforms, as well as for co-location, offered by Sentia, and related IT-general controls

Introduction

The following system description describes the general IT controls in relation to the OSE (Operating System Environment) operated private and public cloud platforms, as well as for co-location, offered by Sentia.

Overview and description of included services

Sentia has offices in:

- Herlev
- Odense
- Aarhus

Sentia deliver services from the following data centres:

- Ballerup
- Copenhagen
- Glostrup
- Kolding
- Skanderborg
- Taastrup
- Valby

Sentia provides public cloud in:

- Microsoft Azure & Office 365
- Amazon Web Services
- Google Cloud

Sentia delivers managed services such as:

- Co-location, Data Connectivity, Software License Rental, Break-Fix Support, Technical Support, End-user Support, Cloud, Backup and Web
- Operations management for Cloud, OSE, Data Connectivity, Firewall,

Network and other relevant areas

- IT advisory, transition, and consultancy services

The customers are within a broad range of industries including, but not limited to:

- Publishing, Media & Digital Agencies
- Software & Technology Vendors
- Retail & Logistics
- Fintech & Finance
- Manufacturing & Utilities
- Health & Pharmaceuticals
- Public Sector & Non-profit

Sentia offers an IT operating platform that supports a broad range of technologies to cover most customer needs in an effective, secure, and appropriate manner.

To ensure stable operations as well as maintaining systems' and data's confidentiality, integrity and accessibility with operating procedures based on the principles of ITIL (Information Technology Infrastructure Library) and best practices, Sentia has also implemented processes and controls that correspond to the assessed business needs and risks accordingly to the ISO 27001 standard and GDPR.

This report includes the IT platform offered by Sentia and related services, including:

- Operations monitoring
- Incident and Problem management
- Security management, including:
    - A subset of Sentia's security controls and procedures accordingly to ISO 27001 Annex A controls
    - Logical access
    - Physical security
    - Monitoring
    - Patch management
- Backup
- Change management

The respective areas are further described in the following.

In addition to this, the statement is restricted to the controls and control objectives in Sentia's organisation relating to the delivery of IT operation services.

The components of the internal control

This section describes the five components, which together make up the framework for the internal controls at Sentia.

Control environment
The control environment framework includes the overall organisation, governance, policies, and procedures and defines the general attitude in the organisation towards internal controls.

Control activities
The activities include the policies and procedures intended to ensure that decisions and measures adopted by the management will be implemented in the organisation.

Information and communication
The component include formal, informal, and automated systems that ensure identification, capturing and exchange of information which, in terms of form and time, allows the organisation's employees to carry out their work in a satisfactory manner.

Monitoring
Monitoring includes processes to ensure that the quality of the controls is maintained and complies with the quality objectives over time.

Risk assessment
The method identifies and analyses the risks, which may affect the organisation's objectives and activities and forms the basis for how they address and manage these risks.

Control environment

This report includes exclusively a subset of Sentia's ISO 27001 Annex A controls and the components of Sentia's internal verification including controls, which may have a pervasive and permanent effect on the organisation as a whole or on processes, applications, interactions, and transaction patterns. Certain control components will relate to the organisation, where others will be related to specific processes or applications.

The total control environment is aligned with the ISO 27001 standard, and includes the overall organisation, governance, policies, and procedures defining the general attitude in the organisation towards internal controls.

Sentia's operation and procedures are ISO 27001:2013 certified by KPMG Finland.

Structure of the organisation
The structure of the organisation in Sentia Denmark is divided into the major business activities with the supporting functions:

- Delivery & Managed Services
- Infrastructure
- Public Cloud Solutions & Consulting
- Digital Experience Monitoring Consulting
- Technology
- Transformation & Integration
- Human Resources
- Sales & Marketing
- Legal
- Financial Management
- Procurement
- Business Governance

GOVERNANCE
(ISO A18. Compliance)
Sentia is managed by a Top Management board consisting of the directors and managers from the different organisational units:

- Managing Director
- Director of Delivery and Managed Services
- Commercial Director
- Financial Director
- Human Resources Director
- Head of Business Governance

The Top Management board is responsible for the preparation of policies and ensures, that they are implemented in the organisation, supported by the necessary procedures and controls, and that employees understand, accept, and comply with the policies as well as the underlying procedures and controls. The practical tasks in relation to implementing and supporting may be delegated to the management team or others in the organisation, but the overall responsibility remains that of the Top Management board.

The Top Management board determines responsibility and authorisations for the individual groups and employees of the organisation, including authorisation hierarchies, rules, and procedures for the reporting.

HR POLICIES AND PRACTICE
(ISO A7. Human resources)
HR policies and practices related to recruitment, information, training, evaluation, advisory services, promotion, and compensation of staff. The staff's qualifications and integrity are key elements for Sentia's control environment. The organisation's ability to recruit and retain sufficiently competent and responsible employees is highly dependent on the HR policies and practices.

Sentia focuses on the continuous development of the competencies of the company's employees and, thus, has a formal training program for the employees, whereby Sentia offers relevant technology and process certifications. The managers identify training plans for the departments and technology areas.

A list of employee qualifications and educational background is maintained for each individual employee with attention to formal certifications by educational institutions, partners, or others on behalf of technology vendors.

Code of Conduct
The correct attitude among management and employees is essential to ensure that processes and controls are operating effectively and as intended. To support promotion and the maintenance of the desired culture, values, and attitudes, Sentia has prepared a formal "Code of Conduct', which, among other things, deals with the importance of the individual employee maintaining a high degree of integrity and acting in accordance with Sentia values and the current legislation at all times.

Sentia's Top Management and the management team acknowledge their responsibility for promoting these values and creating the desired culture.

In addition, upon hiring, each employee is obligated to read the Employee Handbook including the "Code of Conduct" as well as the Information Security Policies.

RISK ASSESMENT
(ISO A6. Risk assessment and management)
Risk assessment is a critical point in Sentia's internal control processes and ISO 27001 ISMS (Information Security Management System) to deal with and regularly assess risks. The purpose is to identify and classify the risks, which may affect the organisation's ability to operate according to the obligations, the company has. Everyone in Sentia's management team is aware, that risks are to be reported and treated separately, precisely to address and act accordingly to the established framework based on the methodology from Digitaliseringsstyrelsen.

Therefore, a regular assessment and control of the challenges facing the business are made, and these are treated by the management team, where the management assess, whether new risks have arisen and, thus, require additional analysis and handling. If a given risk is identified and considered significant, it is escalated to the management team and Top Management board and if needed separate tracks are initiated to update the relevant documents, procedures and ensure mitigation in relation to the business.

Assessment of the risks in relation to IT security is an integral part of the overall risk assessment in the ISMS.

Related control objectives
Controls have been established, that provide reasonable assurance, that processes for risk assessment is implemented and a risk assessment is conducted at least once a year.
Controls have been established, that provide reasonable assurance, that a risk assessment is conducted, when major changes, new applications/services or subcontractors are implemented.

MONITORING
Sentia regularly assesses whether the set of controls sufficiently covers any requirements made by external stakeholders including statutory requirements to Sentia or the customers.

INFORMATION AND COMMUNICATION
Information and communication are an integral part of Sentia's internal control system. The component covers the processes that deal with identification, collection, and exchange of information in a form and time horizon that is necessary to manage and review the company's operations.

At Sentia, information is identified, processed, and reported by various information systems and through conversations with customers, suppliers, employees, and other external stakeholders.

DESCRIPTION OF PROCESSES WITH RESPECTIVE CONTROL OBJECTIVES AND ACTIVITIES

OVERALL MANAGEMENT OF IT SECURITY
(ISO A5. Information security policies, A6. Organization of information security and A18. Compliance)

The Management in Sentia governs information security to meet regulatory requirements and practice, which meets the complexity and risk of Sentia's business. The scope of Sentia's ISMS includes implementation of practice and follow up on effectiveness, based on reporting, reviews and audits.

Sentia's Business Governance department has the responsibility to assist in implementation of practice and performs internal audit and additional controls.

Sentia's information security policies are part of the ISMS. These are implemented and certified according to the ISO 27001:2013 standard.

The information security policy describes how to obtain access to and use Sentia's systems and data. It defines the roles and obligations relating to the secure use of IT in Sentia.

As employee of Sentia, the individuals are personally responsible for always being familiar with the content of the ISMS. Sentia ensures this by communicating revisions and updates throughout the organisation via awareness training programs, e-mails as well as at the departmental and staff meetings. It is also part of the introduction of new employees to ensure awareness and knowledge, where the ISMS are available on Sentia's SharePoint, wiki's, and other applications, and that it is always the employee's responsibility to be familiar with the contents of the ISMS.

Sentia performs continually vulnerability scanning of critical infrastructure to reduce risk of compromising, based on updated knowledge of known vulnerabilities and best practice in network security.

Sentia has established and documented processes that describe how employees and their assigned access rights are handled.

Related control objectives
For overall management of information security, controls have been established, which provide a reasonable level of certainty, that a defined and approved level of IT security has been established, and that the IT security is adapted to the existing threats.
An IT security policy and ISMS approved by Sentia's management has been prepared and implemented.
Sentia is maintaining a Continual Improvement Plan for the ISMS and ISO 27001 procedures.

MONITORING OF SUBCONTRACTORS FOR IT OPERATION SERVICES
(ISO A15. Supplier relationships)

Sentia uses a range of subcontractors for IT operation services as part of the delivery of the services described in the report. Sentia performs controls of subcontractors by obtaining:

- Auditor statement or
- Service documentation

Related control objectives
Controls provide reasonable assurance, that IT operation services provided by external suppliers are monitored in relationship to the establishment of sufficient and documented security.
At least once a year, auditors' reports are obtained from important subcontractors and reviewed regarding relevant controls, including physical security, access, and backup, or Sentia performs controls on relevant documentation for services implemented at the subcontractor.

Information security in supplier relationships
Sentia has established procedures for assessment of information security in supplier relationships by formal approval of new supplier. Control of suppliers is performed to ensure that they can document an appropriate level of information security, based on audit reports or company certifications.

Related control objectives
Controls have been established to ensure systematic collection of documentation from suppliers.

OVERALL MANAGEMENT OF LOGICAL ACCESS
(ISO A7. Human resource security, A9. Access control and A13. Communication security)

Recruitment process
Sentia has established formal procedures for hiring new employees.

The procedures describe, among other things, how the manager within each of the respective functional groups in the organisation reveals the need for additional resources and presents formal requests for job notices to the Management board for acceptance.

After completed interviews, the relevant manager presents a proposal to the Finance and HR departments regarding acceptance of employment of the selected candidate.

Individuals considered to a position in Sentia will be the subject to a background check in accordance with applicable laws and regulations prior to being offered an employment. Background inspections may include, e.g., proof from educational institutions, ID validation, former employment, and criminal records as well as other documentation, which may be of relevance to the employment.

Individuals who accept a position in Sentia must sign an employee contract including non-disclosure agreement. The employees confirm by signature on their employment contract, that they are under an obligation to be familiar and comply with the contents of the contract and the non-disclosure agreement.

During the introduction process, the new employee receives relevant information, which includes an overview of documentation in Sentia e.g., Employee Handbook, Information Security Polies and Sentias Quality Management System.

Performance and skills management
Sentia has a formal performance assessment process. Managers will be asked to discuss output, expectations, and objectives with each individual employee at least once a year. Managers are also strongly urged to have regular, informal interviews with the employees on their performance during the year.

Assignment of access and rights to employees
On hiring a new employee, the manager of the relevant department launches the process for new employees by contacting the HR Department.

Using a template, a control form is created that includes all the activities to be performed before the employment can be regarded as final. For each activity, an individual is designated to be responsible, and this information is added to the form. On the completion of each activity, it is marked as completed. Examples of activities can include:

- Issuing of ID card
- Issuing of keys/access card, etc.
- Ordering of equipment
- Introduction plan

When all activities are completed, the control form is archived in the employee's personnel file by HR.

Once the new employee process has been started, the Operations department receives a change notification with instructions regarding the access rights for the new employee. For example, a new employee in Operations is given access to CRM/ITSM systems, various mailboxes relevant to the job function, documentations sites for customers as well as departments, etc. All assigned access rights are linked to the employee's Active Directory account.

When the Change Approver receives a change notification regarding the creation of a new employee with instructions on the assignment of access rights, the Change Approver ensures, that the source of the change notification is a manager or employee with the correct authorisations to request such a change. There is segregation of duties, so the approving and executing parties are different people.

In the event of an employee resigning his position or is dismissed, a corresponding operation is launched with the relevant control forms to ensure, that assigned access rights is revoked as well as equipment issued and other Sentia effects are returned by the employee.

For access to systems at the subcontractors, Sentia asks the external suppliers to assign access for relevant employees and advises the suppliers on withdrawal of access in the event of resignation or changes in duties, that no longer require access.

Related control objectives
Controls have been established, that provide reasonable assurance that access to information and infrastructure is limited to properly authorised individuals and applications.

Periodic review of users
Sentia monitors changes to AD daily and conducts at least twice a year a control review of its own users in Active Directory to ensure, that all access rights and users still should be active.

When the customer notifies Sentia that an employee has resigned from his position, Sentia implement a change, which involves deactivation of the user on the relevant systems. In the scope of relevant systems that are subject to Sentia's Supply agreement with the customer, the customer will at agreed intervals receive information about users to validate these. Feedback about changes will be implemented.

Related control objectives
Controls have been established, that provide reasonable assurance, that resigned users are deactivated in the systems.
Periodical controls have been established to ensure, that access is granted based on work related needs and upon changes to access rights

Password and audit policies
Sentia has internally implemented password policies, collection of logs and audit control to ensure that users' use of privileged access and granted rights to the systems takes place in accordance with prescribed procedures and security policies. Logging level is defined in the ISMS. The policies and logging are adapted to the role of the different active directories in Sentia e.g., Administrative AD (Normal users), System Management AD (Technical users with Remote Desktop and different monitoring tools) and Customer specific AD for handling access rights for customer shared platforms.

Sentia aims to ensure that customers' IT systems are sufficiently protected. Therefore, Sentia always advises the customer (if applicable according to the supply agreement) about the use of password policies and configuration thereof, including applicable "best practices" for the use of strong passwords.

Related control objectives
Controls have been established, that provide reasonable assurance, that Sentia has established and implemented policies for access passwords, including their complexity, length, and periodic changes thereof.

Assignment of remote access
Employees in Sentia can be given remote access to Sentia's data centre systems, so the employees can perform work from an external location. To obtain remote access a two-factor authentication access solution is used to ensure that employee has been approved to gain remote access. The remote access to the data centre systems will extend to customer systems for appropriate technical employees through the hypervisor layer.

Related control objectives
Controls have been established, that provide reasonable assurance, that remote access to information and infrastructure is limited to properly authorized individuals and applications.
Controls have been established, that provide reasonable assurance, that to obtain remote access to costumers' environment, a change request in the ITSM tool must be approved by appropriate personnel.

Assignment of administrator rights
Sentia employees have assigned administrator rights (local admin) for their own workstation. The administrator rights are assigned due to the nature of the work, that technical users (technicians and consultants) in Sentia performs.

Administrator rights to the Active Directory domains (domain admin) are granted only to a few selected employees.

In continuation of the above:

Administrative user	An administrative normal IT user with limited access rights to the assigned workstation. Software deployment and security software are managed centrally. Technical users can also select this role for their workstation by complying with the restrictive rules of the company (ISMS).
Local admin	Administrator rights have been granted, so the user has full control over the workstation. Complying with the ISMS is still mandatory but managed by the user.
Domain admin	Administrator rights have been granted, so that the user has full control of all machinery in the domain, including servers. Domain admin has rights and privileges, which are limited to the (sub)-domain(s), they are granted for.

Related control objectives
Controls have been established, that provide reasonable assurance, that administrator access is limited to individuals with a work-related need for access.

Security and monitoring of the network
Sentia has secured the internal network using physical firewall appliances, which are intended to protect the network against unauthorized access and other elements such as Internet viruses and "worms".

Sentia uses various networks for different objectives:

Guest network	Separate VLANs per location, which guests can use at Sentia offices during their visit.
Sentia corp. networks	Separate VLANs per location and for respectively wired and wireless network for employees Sentia workstations. For wireless MS-CHAP and certificate authentication is used on the devices.

Sentia's own servers are placed in several secured data centres on external locations. Communications between Sentia office locations and the data centres are via encrypted network tunnels.

Sentia has implemented a centrally managed information protection software solution. The software is installed on all Windows-based entities, communication platforms or on the hypervisor layer of the host in the network, where the employees have administrative privileges, and where the customer has not opted out of implementation in consideration to the customer's systems. Baselines have been established from the administration server, which determine definition update and scanning intervals as well as capturing of logs from clients on the network.

To accommodate software-based vulnerabilities on systems, Sentia has established processes for updating servers, so that operating system (OSE) and applications are updated on a continuing basis at regular intervals and according to a controlled method. This ensures that no irregularities arise, e.g., in the form of compatibility problems because of an update.

All changes to the configuration of the network or security measures must be tested, approved, and documented according to the generally applicable change management process.

Related control objectives
Controls have been established, that provide reasonable assurance, that the network is secured using firewalls.
Controls have been established, that provide reasonable assurance, that IT assets are protected against viruses and the like and are updated regularly with critical security fixes.

Information transfer
Sentia has secured information transfer by secure communication lines, equipment from approved partners, and use of encryption.

Related control objectives
Controls have been established, that provide reasonable assurance, that information transfer is protected.
Controls have been established, that provide reasonable assurance, that to obtain remote access to costumers' environment, a change request in the ITSM tool must be approved by appropriate personnel.

PATCH MANAGEMENT
(ISO A12. Operations security)

As part of the operating platform offered by Sentia, servers and services are subject to the established processes and controls regarding planned updates of OSE and third-party applications. Servers are reviewed monthly for updates to both OSE and third-party applications (tools) or accordingly to specific agreement with the customer. Third party applications (tools) include, but are not limited to: Adobe Flash Player, Adobe Reader, and Java JRE. Major application correction packs (Service Packs) are subject to change management procedures as well as testing and final acceptance by the customer before they are installed. The patch management procedures are divided into two types of processes: unattended (in scope of this control) and attended (handled by change management processes).

Related control objectives
Controls have been established, that provide reasonable assurance, that the operating platform is patched accordingly to internal guidelines and the Supply agreements with customers.

CHANGE MANAGEMENT
(ISO A12. Operations security)

Sentia has established a formal change management process. The process will ensure transparency and traceability in relation to changes made on the operating platform and those of Sentia's customers' systems for which Sentia is responsible for ensuring reliable operation. With regards to this report, the changes primarily comprise changes to configuration of servers, maintenance tasks related to operations of the solutions, but no software development is in scope.

A general description of this process is presented below.

Generally, there are two sources of Requests for Change (RFC):

1. RFCs are established by Sentia's consultants because of work relating to support or error correction of customers' systems or operating platform, including notifications (events) from Sentia's monitoring tools.
2. Authorised individuals in the customer organisation issue an RFC for the amendment of functionality or configuration of the customer's systems, where the stable operation is Sentia's responsibility.

The process dictates that the beneficiary, approving and executing individual shall be different persons, so that the requirements for segregation of duties have been complied with.

When the RFC has been approved, the implementing party receives notification and begins the work.

When the work is completed, a test of the change is performed. The scope of the test is scaled according to the type and complexity of the change. When a completed test of the change produces positive results in relation to test requirements, it may be approved by changing the state to 'implemented.' If the test failed, an incident, problem or new change with appropriate actions is created. When required, the test responsible and method is recorded in the change documented in the ITSM system.

When the work is completed with a positive test result, and satisfactory documentation has been prepared, the RFC is closed for invoicing and administrative processing.

Changes in the operating environment are documented in relevant systems. Changes in logical rights are recorded in the service management systems (ITSM). Configuration changes are documented in the Configuration Management Database (CMDB). The Change Management process thereby ensures, that all operating documentation always is updated.

Related control objectives
Controls provide reasonable assurance that changes of both existing and new solutions have been properly authorized, documented, tested, and approved.
Controls have been established, that provide reasonable assurance, that Sentia has established a formal change management process, which ensures testing and approval of relevant changes.
Controls have been established, that provide reasonable assurance, that Sentia has established test environments, where agreed with the customer.

BACKUP AND RESTORE
(ISO A12. Operations security)

As part of the work to ensure consistent accessibility, integrity, and confidentiality regarding information assets, Sentia has implemented processes for handling the backup of data.

Sentia uses software designed for the virtualization and cloud platforms that Sentia operate, to create backup of servers and the data related to these. If transmission of backup data is needed, the backup software transmits data via encrypted lines to an external location for encrypted storage. Formalized and documented processes have been established for configuration and implementation of the software. Daily verification of the results and success of the backup jobs is conducted. Procedures for initiation of processes in the event of error on backup jobs are established.

To ensure valid data in backup, periodic restore tests for validity of selected backups are performed by Sentia. Restore tests are in accordance with customers' supply agreement.

Related control objectives
Controls provide reasonable assurance, that the processes regarding backup and recovery of data are satisfactory and in accordance with customers' Supply agreement and Sentia's contractual obligations in that connection.

TECHNICAL VULNERABILITY MANAGEMENT
(ISO A12 OPERATIONS SECURITY)

Sentia continually performs evaluation of vulnerabilities in the infrastructure to prevent exploitation of technical vulnerabilities. Sentia evaluates suppliers of software updates and has implemented processes to monitor software applications and updates. Based on identifying risks of vulnerabilities and malware, implementation is planned for regular updates (patches) and security releases.

Additionally, Sentia performs vulnerability scans of critical infrastructure to identify exposure and respond appropriately to handle those exposures.

Only approved software is used.

Related control objectives
Controls provide reasonable assurance, that vulnerabilities are mitigated through systematic updating and control through vulnerability scanning.

OPERATION MONITORING AND ALARMS
(ISO A16. Information security incident management)

As part of the operating platform Sentia provides, Sentia offers monitoring of the availability of the servers, network and other IT-services, with different appropriate monitoring software i.e., Microsoft SCOM, which helps to ensure that unavailability, errors and interruptions on both servers and IT-services are detected in a timely manner, providing the best opportunity to respond and rectify errors quickly and flexibly.

Related control objectives
Controls provide reasonable assurance, that Sentia has implemented systems for monitoring of server and network operation.

Incident management and problem management
To ensure that all incidents are processed in accordance with the Service Level Agreement (SLA) and the related obligations of Sentia, Sentia has established formalised procedures for incident management.

Incidents will be received either by phone, Sentia Customer Portals, or e-mail. Service Desk and other parts of the organisation registers the incident in ITSM system and classifies the inquiry according to the applicable SLA and the nature of the problem.

Related control objectives
The controls provide reasonable assurance, that problems occurring in the operating environment are recorded, classified, investigated, monitored, and resolved.
The controls provide reasonable assurance, that incidents are reported and monitored according to the seriousness of the incident.

ASSET MANAGEMENT
(ISO A8. Asset management)

Sentia has registered IT assets in a series of systems:

Contract Management systems	Sentia uses different applications for registration of Supply agreements.
CMDB	Sentia has developed and implemented CMDB systems with incorporated features for automatically updating from data centre equipment, Contract Management systems and other relevant IT-operational tasks.
ITSM systems	The IT service management (ITSM) systems contains information about SLAs, Configuration Items and CMDB data for day-to-day operation.
SharePoint/MS Teams	The SharePoint and MS Teams online platforms at Sentia are divided into two major separate components for internally use and for external sharing with customers and partners. The internal SharePoint sites (intranet) and Microsoft Teams organised information with all internal documents are only with access for Sentia employees. The external customer and partner SharePoint and MS Teams sites are used for meeting minutes, documentation, monthly KPI/SLA reports, and other relevant documents shared with external parties. Only relevant users are granted access to these sites and within the limitations of the connected customer or partner.
Wiki	Sentia has implemented multiple wiki sites for internal and external use. The sites contain documentation, operational procedures etc.
Equipment and asset register	Additional IT assets and any rights, etc. are registered in Sentia's ERP systems in the balance sheet and inventory module, respectively.

Guidelines for accepted use of all information-related assets exist and are available to relevant employees.

Related control objectives
The controls provide reasonable assurance that all information-related assets have been identified that these have been classified, and that a system owner responsible for the assets has been appointed. Controls also provide reasonable assurance that guidelines for accepted use of all information-related assets exist and are available to relevant staff members.
The controls provide reasonable assurance, that there is appropriate operating documentation in Sentia's CMDB and other applications of operating systems, patch levels, RAM, etc. for the assets.

PHYSICAL SECURITY
(ISO A11. Physical and environmental security)

Sentia has documented processes for maintaining physical security for offices and data centres with focus on access based on work-related needs and mitigation of risks. The risk areas are identified as unauthorized access, theft, environment impact, power supply failure, fire, and local area-imposed risks.

Related control objectives
The controls provide reasonable assurance that all information-related assets are protected from unauthorized access in data centres and offices with access systems, monitoring, and alarms. Controls also provide reasonable assurance, that the access are monitored, granted accordingly to business and work-related needs.
The controls provide reasonable assurance that all information-related assets are protected against fire, water, and heat. Controls also provide reasonable assurance, that the conditions are monitored, and the fire systems are tested by a vendor.
The controls provide reasonable assurance that all information-related assets are protected from power-loss by UPS and emergency power systems.
The controls provide reasonable assurance, that data carrying information-related assets are disposed of in a safe manner.

INFORMATION SECURITY CONTINUITY
(ISO A17. Information security aspects of business continuity management)

Information security continuity is embedded in Sentia's systems.

To ensure appropriate handling in case of critical incidents, Sentia has implemented an IT Contingency Plan with roles, responsibilities, and activities to be completed, to restore services.

Testing of the plan validates activities in the plan is carried out.

Related control objectives
The controls provide reasonable assurance that the plan is reviewed and formally tested at least annually.

Ensure availability of information processing facilities
To ensure availability of information processing facilities Sentia has implemented redundancy for business-critical systems.

Related control objectives
The controls provide reasonable assurance that the plan is reviewed and formally tested at least annually.

COMPLEMENTARY CONTROLS AT USER ORGANISATIONS

To achieve the control objectives specified in this report, controls must be established and handled correctly by the user organisations cf. the terms and conditions in the Supply Agreement with Sentia Denmark A/S.

The controls at user organisations are not covered by this report.

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.

This statement is issued according to the carve-out method and therefore does not include controls of Sentia Denmark A/S' subservice organisations.

Controls, which are specific to the individual customer solutions, or are performed by Sentia Denmark A/S' customers, are not included in this report.

Tests performed

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

Method	General description
Inquiries	Interview with appropriate personnel at Sentia Denmark 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 Sentia Denmark A/S.

A.5 Information security policies

A.5.1 Management direction for information security
Control objective: To ensure that a defined and approved level of IT security has been established, and that the IT security is adapted to the existing threats.

No.	*Sentia Denmark A/S' control*	*Grant Thornton's test*	*Test results*
5.1	An IT security policy and ISMS approved by Sentia's management has been prepared and implemented. Sentia ensure that the IT security policy and content of the ISMS is communicated to employees via awareness training programs, e-mails as well as at the departmental and staff meetings.	We have inspected that an IT security policy has been defined and approved by Sentia's management. We have inspected that the IT security policy is updated. We have inspected that the IT security policy and content of the ISMS is communicated to employees via Sentia's Intranet and awareness training.	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.	*Sentia Denmark A/S' control*	*Grant Thornton's test*	*Test results*
6.1	Processes for risk assessment is implemented and a risk assessment is conducted at least once per year. A risk assessment is conducted, when major changes, new applications/services or subcontractors are implemented.	We have inspected the established risk assessment procedure. We have inspected that the risk assessment is updated and approved. We have inspected that a risk assessment is performed, when major changes, new applications/services or subcontractors are being implemented.	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.	*Sentia Denmark A/S' control*	*Grant Thornton's test*	*Test results*
7.1	Sentia has established formal procedures for hiring new employees. Individuals offered a position in Sentia will be subject to a background check in accordance with applicable laws and regulations prior to starting employment. The employees confirm by way of signature on their employment contract, that they are under an obligation to be familiar with the contents of the contract and the non-disclosure agreement.	We have inspected that formal procedures for hiring new employees are in place. We have, by sample test, inspected that employees are screened as part of the employment process including: • Test conducted and feedback obtained • Reference checks performed • CV obtained • Criminal record obtained We have, by sample test, inspected that new hires have signed a confidentiality agreement.	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.	*Sentia Denmark A/S' control*	*Grant Thornton's test*	*Test results*
7.2	Sentia has prepared a formal "Code of Conduct' which includes area of the importance of the individual employee maintaining a high degree of integrity and acting in accordance with Sentia values. Upon hiring, each employee is obligated to read the Employee Handbook including the "Code of Conduct" as well as the Information Security Policies. Sentia conducts awareness training programs to ensure employees are familiar with the ISMS.	We have inspected that a "Code of Conduct" is in place. We have, by sample test, inspected that employees appointed during the assurance period have been introduced to: • Information security policy • Employee Handbook including the "Code of Conduct" We have inspected that awareness training covering the ISMS is provided to employees.	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.	***Sentia Denmark A/S' control***	***Grant Thornton's test***	***Test results***
7.3	In the event of an employee resigning his position or is dismissed, a corresponding operation is launched with the relevant control forms to ensure, that assigned access rights is revoked as well as equipment issued and other Sentia effects are returned by the employee.	We have inspected procedures ensuring that resigned or dismissed employees' rights are deactivated or terminated upon resignation or dismissal and that assets such as access cards, computers, mobile phones, etc. are returned. We have, by sample test, inspected that access rights have been deactivated or terminated and that assets have been returned for employees resigned or dismissed during the assurance period.	No deviations noted.

A.8 Asset management

A.8.1 Acceptable use of assets Control objective: To ensure that rules for the acceptable use of information and of assets associated with information and information processing facilities are made aware to employees.			
No.	***Sentia Denmark A/S' control***	***Grant Thornton's test***	***Test results***
8.1	Guidelines for accepted use of all information-related assets exist and are available to relevant staff members.	We have inspected that guidelines for acceptable use of assets are in place and made available to employees.	No deviations noted.

A.8.2 Classification and registration of information Control objective: To ensure an appropriate protection of information considering the value of the information to the organisation.			
No.	***Sentia Denmark A/S' control***	***Grant Thornton's test***	***Test results***
8.2	IT assets are registered and updated in CMDB systems. Information-related assets have been classified. A system owner responsible for the assets has been appointed.	We have inspected that assets are registered in systems, including CMDB, in Sentia. We have inspected that assets have been classified and labelled. We have inspected that categories of assets have been identified and that owners have been appointed to the assets.	No deviations noted.

A.8.3 Media handling Control objective: To prevent unauthorised disclosure, modification, removal, or destruction of information stored on media			
No.	***Sentia Denmark A/S' control***	***Grant Thornton's test***	***Test results***
8.3	Data carrying information-related assets are disposed of in a safe manner.	We have inquired about the management of removable media. We have inspected the guidelines for disposal of media and physical media transfer. We have inspected that removeable media have been securely destroyed.	No deviations noted.

A.9 Access control

A.9.1 Assignment of access and rights to employees
Control objective: To ensure that access to information and infrastructure is limited to properly authorised individuals and applications.

No.	*Sentia Denmark A/S' control*	*Grant Thornton's test*	*Test results*
9.1	Policy and procedures have been established describing how employees and their assigned access rights are handled. For assignment of new access rights, access request tickets are sent to a change approver in the Operations department who will review the request and ensure that the source of the change notification is a manager or employee with the correct authorizations to request such a change. Segregation of duties is established between change requester and change approver.	We have inspected that formalised procedures are in place for restricting users' access to a work-related need. We have, by sample test, inspected that user accesses granted have been authorised and that a work-related need exists for employees' access to systems and databases. We have inspected that segregation of duties is established between change requester and change approver.	No deviations noted.

A.9.2 Periodic review of users
Control objective: To ensure that access is granted based on work related needs and upon changes to access rights

No.	*Sentia Denmark A/S' control*	*Grant Thornton's test*	*Test results*
9.2	Internal users' access rights are reviewed regularly according to formalised business procedures.	We have inspected that formalised procedures are in place for following up on users' access to personal data being consistent with their work-related need. We have inspected that documentation exists of granted user accesses are evaluated on an annual basis.	No deviations noted.

A.9.3 Termination of user access rights Control objective: To ensure that resigned users are deactivated in the systems.			
No.	***Sentia Denmark A/S' control***	***Grant Thornton's test***	***Test results***
9.3	The access rights of employees and external contractors are removed upon termination of their employment, contract, or agreement, or adjusted upon change.	We have inspected that formalised procedures exist for removing users' access to systems and databases upon termination of their employment, contract, or agreement. We have, by sample test, inspected resigned or dismissed employees to establish whether their access to systems and databases was deactivated or removed on a timely basis.	No deviations noted.

A.9.4 Password policies Control objective: To limit the risk of unauthorized access to systems or data			
No.	***Sentia Denmark A/S' control***	***Grant Thornton's test***	***Test results***
9.4	Sentia has established and implemented a password policy, including defined criteria for complexity, length, periodic changes etc.	We have inspected that a password policy is in place. We have inspected the password management system and that implemented password configuration settings are following the password policy.	No deviations noted.

A.9.5 Assignment of administrator rights Control objective: To ensure that administrator access is limited to individuals with a work-related need for access.			
No.	***Sentia Denmark A/S' control***	***Grant Thornton's test***	***Test results***
9.5	The allocation and use of privileged access rights are limited to individuals with a work-related need for the access.	We have inspected that an access control policy also including the allocation and use of privileged access rights is in place. We have inspected that the allocation and use of privileged access rights are limited to individuals with a work-related need for the access.	No deviations noted.

A.9.6 Assignment of remote access Control objective: To ensure that remote access to information and infrastructure is limited to properly authorised individuals and applications.			
No.	***Sentia Denmark A/S' control***	***Grant Thornton's test***	***Test results***
9.6	Two-factor authentication access is used to ensure, that employee has been approved to gain remote access.	We have inspected that procedures exist to ensure that two-factor authentication is used to ensure, that employees have been approved to gain remote access. We have inspected documentation that users are prompted with two-factor authentication when signing in.	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.	***Sentia Denmark A/S' control***	***Grant Thornton's test***	***Test results***
11.1	All information-related assets are protected from unauthorized access to offices with access systems, monitoring, and alarms. Physical security for offices has been designed and applied.	We have inspected that procedures exist to ensure that only authorised persons can gain physical access to offices. We have observed that access points are established at office entry points. We have inspected that access to offices and data centres are monitored and granted according to business and work-related needs. We have observed that offices have camera surveillance installed. We have inspected that tests are performed on a regular basis to prevent fire hazards.	No deviations noted.

A.12 Operations security

A.12.1 Change Management
Control objective: To ensure correct and secure operation of information processing facilities

No.	*Sentia Denmark A/S' control*	*Grant Thornton's test*	*Test results*
12.1	A formal change management process has been established. Changes of both existing and new solutions have been properly authorised, documented, tested, and approved. Test environments are established, where agreed with the customer.	We have inspected that a formal change management process is in place. We have, by sample test, inspected that changes have been authorised, documented, tested, and approved before implementation. We have inspected that test environments are established, where agreed with the customer.	No deviations noted.

A 12.2 Patch Management
Control objective: To ensure that the operating platform is patched accordingly to internal guidelines and the Supply agreements with customers.

No.	*Sentia Denmark A/S' control*	*Grant Thornton's test*	*Test results*
12.2	IT assets are updated and patched regularly with critical security fixes according to internal guidelines and the Supply agreements with customers (SLA).	We have inspected that a formal patch management process is in place. We have, by sample test, inspected that IT assets are updated and patched according to internal guidelines and SLA. We have, by sample test, inspected that antivirus software has been installed on systems and databases. We have inspected that antivirus software is up to date.	No deviations noted.

A.12.3 Backup and restore Control objective: To ensure that the processes regarding backup and recovery of data are satisfactory and in accordance with customers' Supply agreement and contractual obligations in that connection.			
No.	***Sentia Denmark A/S' control***	***Grant Thornton's test***	***Test results***
12.3	Formalised and documented processes have been established for backup of data. Daily verification of the results and success of the backup jobs is conducted. Procedures for initiation of processes in the event of error on backup jobs are established. Periodic restore tests for validity of selected backups are performed in accordance with customers' Supply agreement.	We have inspected that a formal backup process is in place. We have inspected that daily follow-up of the results and success of the backup jobs is performed. We have inspected that procedures for initiation of processes, in the event of error, on backup jobs are established. We have inspected that restore test of backup data are performed on a periodic basis.	No deviations noted.

A.12.4 Logging and monitoring Control objective: To record events and generate evidence			
No.	***Sentia Denmark A/S' control***	***Grant Thornton's test***	***Test results***
12.4	Sentia has implemented systems for monitoring of server and network operation.	We have inspected the procedure for logging and monitoring, including the logging strategy We have, by sample test, inspected that an alarm feature is installed on systems and databases connected to the network. We have, by sample test, inspected that alarms were followed up on.	No deviations noted.

A.12.5 Technical vulnerability management Control objective: To prevent exploitation of technical vulnerabilities			
No.	***Sentia Denmark A/S' control***	***Grant Thornton's test***	***Test results***
12.5	Continually vulnerability scanning of critical infrastructure are performed to reduce risk of compromising, based on updated knowledge of known vulnerabilities and best practice in network security.	We have inspected that formalised procedures exist for regularly testing of technical measures, including performing vulnerability scans and penetration tests. We have inspected that regular testing of vulnerabilities and that supporting technical measures are established. We have inspected that any deviations or weaknesses in the technical measures have been responded to in a timely and satisfactory manner.	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.	***Sentia Denmark A/S' control***	***Grant Thornton's test***	***Test results***
13.1	The internal network is secured by way of physical firewall appliances. Communications between Sentia office locations and the data centres are via encrypted network tunnels. Baselines have been established from the administration server, which determine definition update and scanning intervals as well as capturing of logs from clients on the network. All changes to the configuration of the network or security measures must be tested, approved, and documented accordingly to the generally applicable change management process.	We have inspected that the internal network is secured by firewall appliances. We have inspected that communication between Sentia office locations, and the data centres are performed via VPN encrypted network tunnels. We have inspected that baselines have been established from the administration server. We have, by sample test, inspected that changes to the configuration of the network or security measures follow the change management process.	No deviations noted.

A.15 Supplier relationships

15.1 Assessment of supplier relationships

Control objective: To ensure that suppliers can document an appropriate level of information security, based on audit reports or company certifications

No.	*Sentia Denmark A/S' control*	*Grant Thornton's test*	*Test results*
15.1	Sentia has established procedures for assessment of information security in supplier relationships by formal approval of new supplier.	We have inspected that procedures for assessment of information security in supplier relationships is in place.	No deviations noted.

A15.2 Monitoring of subcontractors for IT operation services

Control objective: To ensure that IT operation services provided by external suppliers are monitored in relationship to the establishment of sufficient and documented security

No.	*Sentia Denmark A/S' control*	*Grant Thornton's test*	*Test results*
15.2	Sentia regularly monitor, review and audit supplier service delivery. The monitor and review activities include areas for physical security associated with information-related assets in data centres.	We have inspected that the procedure for managing suppliers and supplier agreements contains requirements for regularly monitor, review, and audit supplier service delivery. We have inspected, that review and assessment of relevant audit reports on significant sub-suppliers have been performed. We have inspected that the monitoring and review control activities include areas for physical security associated with information-related assets in data centres.	No deviations noted.

A.16 Incident and problem management

A.16.1 Incident and problem management
Control objective: To ensure a consistent and effective approach to the management of incidents, including communication on security events and weaknesses

No.	*Sentia Denmark A/S' control*	*Grant Thornton's test*	*Test results*
16.1	Sentia has established formalised procedures for incident management. Incident and problems are registered in the ITSM system and classified according to the applicable SLA and the nature of the problem. Incidents are reported and monitored according to the seriousness of the incident.	We have inspected that a formalised incident management procedure is in place. We have, by sample test, inspected that incident and problems are registered and reported via the ITSM system and including relevant classification for reporting.	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.	*Sentia Denmark A/S' control*	*Grant Thornton's test*	*Test results*
17.1	An IT Contingency Plan has been implemented including the allocation of roles, responsibilities, and activities to be completed, to restore services. The IT Contingency Plan is reviewed and formally tested at least annually.	We have inspected that an IT contingency plan has been implemented including the allocation of roles, responsibilities, and activities to be completed. We have inspected the procedure for management of the IT contingency plan. We have inspected that the IT contingency plan is available for relevant employees. We have inspected the IT contingency plan have been tested and reviewed annually.	No deviations noted.

A.17.2 Redundancies Control objective: To ensure availability of information processing facilities			
No.	***Sentia Denmark A/S' control***	***Grant Thornton's test***	***Test results***
17.2	Information processing facilities are implemented with redundancy sufficient to meet availability requirements.	We have inspected that redundant infrastructure with individual backup has been established.	No deviations noted.

A.18 Compliance

18.1 Compliance with legal and contractual requirements Control objective: To avoid breaches of legal, statutory, regulatory, or contractual obligations related to information security and of any security requirements.			
No.	***Sentia Denmark A/S' control***	***Grant Thornton's test***	***Test results***
18.1	The Management in Sentia governs information security to meet regulatory requirements and practice, which meets the complexity and risk of Sentia's business.	We have inspected that a management approved, and updated security policy that include sections for compliance of regulatory requirements and practice, is in place.	No deviations noted.

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.	***Sentia Denmark A/S' control***	***Grant Thornton's test***	***Test results***
18.2	Sentia is maintaining a continual improvement plan for the ISMS and ISO 27001 procedures. An internal IT audit has been established and an annual wheel is in place to ensure that internal audit activities associated with information security are performed in a timely manner.	We have inspected that an internal IT audit has been established. We have inspected that an annual wheel is in place to ensure that internal audit activities associated with information security are performed in a timely manner. We have inspected that identified control deficiencies are registered, assigned to an owner and followed-up on.	No deviations noted.