Grant Thornton

Independent Auditor's ISAE 3402 Assurance Report

On the design and operating effectiveness of general IT controls in relation to operating and hosting services from the 1st of January 2021 to 31st of December 2021.

Sentia Denmark A/S

CVR Nr.: 10 00 81 23

Table of Contents

		Page	Assessment
1.	Management Statement	3	
2.	Description of General IT Controls	5	
3.	Independent Auditor's Assurance Report	18	
4.	Control Objectives, Security Measures, Tests and Findings	20	
	• Risk Assessment and Management	21	●
	• Information Security Policies	22	●
	• Organization of Information Security	23	●
	• Human Resource Security	24	●
	• Asset Management	26	●
	• Access Control	28	●
	• Physical and Environmental Security	30	●
	• Operations Security	32	●
	• Communication Security	37	●
	• Supplier Relationships	38	●
	• Information Security Incident Management	40	●
	• Information Security Aspects of Business Continuity Management	41	●
	• Compliance	42	●

Symbol

- ● Our tests have not resulted in any material deviations.
- ● Some weaknesses have been identified in the controls.
- ● Critical weaknesses or deficiencies have been identified.

1. Management Statement

SCOPE OF THE ISAE 3402 TYPE 2 REPORT

This ISAE 3402 Type 2 Report includes Sentia Denmark A/S CVR: 10 00 81 23 (hereinafter "Sentia") for the period 1st January 2021 to 31st December 2021.

IMPORTANT ACTIVITIES IN 2021

In 2021 Sentia continued consolidation and integration of business activities. At the same time Sentia has proceeded the planned activities for developing and optimizing the service portfolio. These activities include amongst others:

- Development and implementation of new organization
- Consolidating data centers
- Aligning and optimizing of the ITSM (IT Service Management) processes based on ITIL and adoption to the ServiceNow ITSM application
- Extended scope of ISO 27001:2013 certification by KPMG Finland to cover all of Sentia Denmark
- Continuing the development of the value proposition in Microsoft Azure and Sentia cloud solutions with the Microsoft Azure Expert Managed Service Provider (MSP) re-certification
- Maintain Google Resell Partner & Service Partner status
- Alignment and improvement of services, SLA (Service Level Agreements) and contractual terms
- Divestment of data center Smedeland

The accompanying description has been prepared for customers who have used Sentia Denmark A/S' operating and hosting services and their auditors who have a sufficient understanding to consider the description, along with other information including information about controls operated by customers themselves, when assessing the risks of material misstatements of customers' financial statements.

Sentia Denmark A/S confirms that:

a) The accompanying description in section 2 fairly presents Sentia Denmark A/S' operating and hosting services throughout the period 1st of January 2021 to 31st of December 2021 The criteria used in making this assertion were that the accompanying description:

i. presents how the system was designed and implemented, including:
   - the types of services provided.
   - the procedures, within both information technology and manual systems, to ensure the confidentiality, integrity and accessibility of systems and data.
   - 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 control objectives stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved by ourselves alone.
   - other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that were relevant to processing.

ii. provides relevant details of changes to the service organization's system throughout the period from 1st of January 2021 to 31st of December 2021.

iii. does not omit or distort information relevant to the scope of the described system, 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 to their own particular environment.

1. Management Statement

b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period 1st of January 2021 to 31st of December 2021. 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 persons who have the appropriate competence and authority, throughout the period 1st of January 2021 to 31st of December 2021.

Herlev, 18th of January 2022

Lyskær 3A, 2730

Jakob Høholdt

Managing Director

2. Sentia Denmark A/S' System Description

DESCRIPTION OF GENERAL IT CONTROLS

OVERVIEW AND DESCRIPTION OF INCLUDED SERVICES

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

Sentia has offices in:

- Glostrup
- Herlev
- Odense
- Aarhus

Sentia operates data centers in:

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

Sentia provides public cloud in:

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

Sentia delivers managed services such as:

- Colocation, 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 also supports a broad range of technologies to cover most customer needs in an effective, secure, and appropriate manner.

To ensure stable operation 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.

2. Sentia Denmark A/S' System Description

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 organization relating to the delivery of IT operation services. As a result, Sentia's internal software development activities are not covered by this statement.

THE COMPONENTS OF THE INTERNAL CONTROL

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

Control environment

The control environment framework includes the overall organization, governance, policies, and procedures and defines the general attitude in the organization 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 and embedded in the organization.

Information and communication

The component includes formal, informal, and automated systems that ensure identification, capturing and exchange of information which, in terms of form and time, allows the organization'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, that may affect the organization's objectives and activities and forms the basis for how they address and manage these risks.

2. Sentia Denmark A/S' System Description

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, that may have a pervasive and permanent effect on the organization as a whole or on processes, applications, interactions, and transaction patterns. Certain control components will relate to the organization, 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 organization, governance, policies, and procedures defining the general attitude in the organization towards internal controls. Sentia's operation, data centers and procedures is ISO 27001:2013 certified by KPMG Finland.

Structure of the organization

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

- Global Infrastructure
- Operations
- Public Cloud
- Human Resources
- Commercial
- Finance
- Business Governance

Governance (ISO 18. Compliance)

Sentia is managed by a Top Management board consisting of the directors and managers from the different organizational units:

- Managing Director
- Operations Director
- 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 organization, 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 organization, 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 organization, including authorisation hierarchies, rules and procedures for the reporting.

The Managing Director reports to the Sentia Group Management in the Netherlands.

2. Sentia Denmark A/S' System Description

HR policies and practice (ISO 7. 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 organization'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 other 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 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 ASSESTMENT (ISO 4. 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 the risks. The purpose is to identify and classify the risks, that may affect the organization'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 in 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.

2. Sentia Denmark A/S' System Description

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 5. Information Security Policies, 6. Organization of Information Security and 18. Compliance)

The Management in Sentia governs information security to meet regulatory requirements and practice, that 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 organization 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.

2. Sentia Denmark A/S' System Description

MONITORING OF SUBCONTRACTORS FOR IT OPERATION SERVICES (ISO 15. 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.

OVERALL MANAGEMENT OF LOGICAL ACCESS (ISO 7. Human resource security, 9. Access control and 13. 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 organization 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 offered a position in Sentia will be the subject of a background check in accordance with applicable laws and regulations prior to starting employment. Background inspections may include, e.g., proof from educational institutions, ID information, former employment and criminal records as well as other documentation, which may be of relevance for the employment.

Under the introduction process, the new employee receives relevant information, which includes an overview of Sentia's human resources policies and procedures. This information packet includes the following:

- Employment contract including non-disclosure agreement
- Review of the employee handbook and Security policies

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.

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.

2. Sentia Denmark A/S' System Description

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:

- Gathering and verification of criminal record
- 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 the 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 a 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 conduct at least once 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 launches established change processes, which involve deactivation of the user on the customer's systems. Also reviewed are all users of all customer systems – limited, however, to the systems that are subject to Sentia's Supply agreement with the customer – with fixed and agreed intervals, following which the customer has an opportunity to validate, that it is only the right users, who have access and are active.

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

2. Sentia Denmark A/S' System Description

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 accordingly 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 center 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 center 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 authorised 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 are 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 perform as well as the tools.

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 by the restrictive rules of the company (ISMS).
Local admin	Administrator rights have been granted, so the user has full control over the workstation. Complying to the ISMS is still mandatory but managed by the user.

2. Sentia Denmark A/S' System Description

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, that 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 by way of physical firewall appliances, which are intended to protect the network against unauthorised 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 centers on external locations or own two data centers. Communications between Sentia office locations and the data centers 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 accordingly to the generally applicable change management process.

Related control objectives

Controls have been established, that provide reasonable assurance, that the network is secured by the use of 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.

2. Sentia Denmark A/S' System Description

PATCH MANAGEMENT (ISO 12. 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 12. 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, 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 organization 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 separation 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 needed the test responsible and method are recorded on the change in the ITSM systems.

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.

2. Sentia Denmark A/S' System Description

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 authorised, 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 12. Operations security)

As part of the work to ensure consistent accessibility, integrity, and confidentiality regarding information-related assets, Sentia has implemented backup 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. Formalised 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.

OPERATION MONITORING AND ALARMS (ISO 16. 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 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 organization registers the incident in ITSM system and classifies the inquiry according to the applicable SLA and the nature of the problem.

2. Sentia Denmark A/S' System Description

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 8. Asset Management)

Sentia has registered significant 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 center 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 is 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 organized information with all internal documents are only with access for Sentia employees.
(continued)	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.

2. Sentia Denmark A/S' System Description

PHYSICAL SECURITY (ISO 11. Physical and Environmental Security)

Sentia has documented processes for maintaining physical security for offices and data centers with focus on access based on work-related needs and mitigation of risks. The risk areas are identified as i.e. 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 unauthorised access in data centers 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 is 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.

COMPLEMENTARY CONTROLS AT USER ORGANIZATIONS

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

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

3. Independent Auditor's Assurance Report on the description of the general IT controls, their design and operating effectiveness

For the customers of Sentia Denmark A/S and their auditors

Scope

We have been engaged to report on Sentia Denmark A/S' description in Chapter 2, which is a description of general IT controls conducted in connection with the operation of Sentia Denmark A/S Hosting activities for processing customers' transactions during the period from 1st of January 2021 to 31st of December 2021, and on the design and operating effectiveness of controls related to the control objectives mentioned in the description.

We express our opinion with reasonable assurance.

The report is based on a holistic approach, which means this report also includes the IT security controls and control objectives related to use of external business partners. The scope of our report does not cover customer-specific conditions, and the report does not include the complementary controls and control activities conducted by the user company; see the description of the company in Chapter 2 under the section: Complementary controls.

Sentia Denmark A/S' responsibility

Sentia Denmark A/S is responsible for the preparation of the description and accompanying assertion in Chapter 2, including the completeness, accuracy and method of presentation of the description and assertion; for providing the hosting activities covered by the description; for stating the control objectives; and for designing, implementing and effectively operating controls to achieve the stated control objectives.

Grant Thornton's independence and quality management

We have complied with the requirements of independence and other ethical requirements laid down in FSR's Ethical Rules based on fundamental principles of integrity, objectivity, professional competence and requisite care, confidentiality and professional conduct. We apply ISQC 1 and thus sustain a comprehensive system of quality management, including documented policies and procedures for compliance with ethical rules, professional standards as well as requirements in force under existing laws and additional regulation.

Auditor's responsibility

Our responsibility is to express an opinion on Sentia Denmark A/S' description and on the design and operation of 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 Organization, issued by the IAASB. The standard requires that we comply with ethical requirements and that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and whether the controls are appropriately designed and operate effectively in all material respects. An assurance engagement to report on the description, design and operating effectiveness of controls at a service organization involves performing procedures to obtain evidence about the disclosures in the service organization's description of its system, and the design and operating effectiveness of controls. The procedures selected depend on the judgement of the service organization's auditor, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed or not 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.

3. Independent Auditor's Assurance Report on the description of the general IT controls, their design and operating effectiveness

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 and described in Chapter 2 by Sentia Denmark A/S.

Grant Thornton believes that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Limitations of controls at Sentia Denmark A/S

Sentia Denmark A/S' description is prepared to meet the common needs of a broad range of customers and their auditors and thus may not include every aspect of the system that each individual customer may consider important in its own particular environment. In addition, because of their nature, controls at Sentia Denmark A/S may not prevent or detect all errors or omissions in processing or reporting transactions. The projection of any evaluation of effectiveness to future periods is subject to the risk that controls at the service organizations may become inadequate or fail.

Opinion

Our opinion is based on the matters outlined in this report. The criteria on which our opinion is based are those described in Chapter 2 under Sentia Denmark A/S' system description. In our opinion,

a) The description fairly presents the general IT controls of Sentia Denmark A/S for cloud based operating platform services, such as they were designed and implemented throughout the period 1st of January 2021 to 31st of December 2021 in all material respects; and

b) The controls related to the control objectives stated in the description were in all material respects suitably designed throughout the period 1st of January 2021 to 31st of December 2021; and

c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved in all material respects, operated effectively throughout the period 1st of January 2021 to 31st of December 2021.

Description of tests of controls

The specific controls tested and the nature, timing and findings of those tests are listed in Chapter 4.

Intended users and purpose

This report and the description of the test of controls in Chapter 4 are intended only for Sentia Denmark A/S' customers and their auditors, who have sufficient understanding to consider them, along with other information, including information about controls operated by customers themselves, when assessing the risks of material misstatement in their financial statements.

Copenhagen, 18th of January 2022

Grant Thornton
State authorized public accountants
CVR-nr: 34 20 99 36

Martin Bomholtz
State authorized public accountant

Anders Grønning-Kjærgaard
Head of IT Audit & Advisory

4. Control Objectives, Security Measures, Tests and Findings

4.1 Purpose and scope

The following overview is provided to facilitate an understanding of the controls implemented by Sentia Denmark A/S. Our testing of functionality comprised the controls that we considered necessary to provide reasonable assurance that the control objectives stated in the description were achieved during the period from the 1st of January 2021 to 31st of December 2021.

Thus, we have not necessarily tested all the controls mentioned by Sentia Denmark A/S in the description in chapter 2. Moreover, our statement does not apply to any controls performed at Sentia Denmark A/S' customers, as the customers' own auditors should perform this review and assessment.

4.2 Test activities performed

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 from the described controls, we have specified this.

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

Method	General Description
Inquiries	Inquiry of appropriate personnel. Inquiries have included how the controls are performed.
Observation	We have observed the execution of the control.
Inspection	Reading of documents and reports containing specifications regarding the execution of the control. This includes reading and consideration of reports and other documentation in order to assess whether specific controls are designed so they may be expected to become effective, if implemented. Furthermore, it is assessed whether controls are being monitored and checked sufficiently and at appropriate intervals.
Repetition of the control	Repeat the relevant control. We have repeated the execution of the control to verify that the control functions as assumed.

4. Control Objectives, Security Measures, Tests and Findings

4. Risk Assessment and Management

Control objective: **The risk assessment must identify and prioritize the risks based on the operation of hosting activities. The findings are to contribute to the identification and prioritization of management interventions and precautionary measures necessary to address relevant risks.**			
Nr.	***Sentia Denmark A/S controls***	***Auditor's test of controls***	***Test findings***
4	Controls have been established, that provide reasonable assurance, that processes for risk assessment is implemented and a risk assessment is conducted at least once per 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.	We have obtained the current and approved risk assessment. We have verified that frequent risk assessments have been carried out by the Business Governance team and reported to management. We have verified that Sentia has set a fixed, low level of acceptance of risk. We have verified that Sentia's exposure is managed based on the risk score, which is calculated from the risk impact and likelihood	Our tests have not resulted in any material deviations.

4. Control Objectives, Security Measures, Tests and Findings

5. Information Security Policies

Control objective: **To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.**			
Nr.	***Sentia Denmark A/S controls***	***Auditor's test of controls***	***Test findings***
5.	An IT security policy and ISMS approved by Sentia's management has been prepared and implemented. Sentia ensures this by communicating revisions and updates throughout the organization via awareness training programs, e-mails as well as at the departmental and staff meetings.	We have obtained and reviewed Sentia's latest IT security policy and ISMS. We have verified that maintenance of the IT security policy and ISMS is conducted on a regular basis. We have checked during our audit that the underlying, supporting policies have been implemented. We have checked that the policy is approved and signed by the Head of Business Governance and Managing Director and made available to employees on Sentia's Intranet and awareness training.	Our tests have not resulted in any material deviations.

4. Control Objectives, Security Measures, Tests and Findings

6. Organization of Information Security

Control objective: To establish a management framework to initiate and control the implementation and operation of information security within the organisation.			
Nr.	***Sentia Denmark A/S controls***	***Auditor's test of controls***	***Test findings***
6.1	All information security responsibilities are defined and allocated. Business Governance assists in the implementation of practice and performs audits and additional controls. Approving and executing parties are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets. Roles and process for contact with authorities and interest groups have been defined. Risk assessment is conducted, when major changes, new applications/services or subcontractors are implemented	We have inspected documentation for the allocation of information security roles and responsibilities. We have inquired about segregation of duties and inspected assigned roles in the change management system. We have inspected documentation on the process for contact with authorities and special interest groups. We have inquired about evaluation of risk when new systems/services or subcontractors are implemented.	Our tests have not resulted in any material deviations.

Control objective: To ensure the security of teleworking and use of mobile devices.			
Nr.	***Sentia Denmark A/S controls***	***Auditor's test of controls***	***Test findings***
6.2	The information security policy includes controls for remote access and security measures are implemented to ensure remote access.	We have inspected the policies and controls for mobile device management. We have inspected the selected security measures for the use of teleworking sites. We have verified that accesses to customers' environment handled through the change management process. We have inspected that access requests has to be approved by appropriate personnel.	Our tests have not resulted in any material deviations.

4. Control Objectives, Security Measures, Tests and Findings

7. Human Resource Security

Control Objective:
To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

Nr.	*Sentia Denmark A/S controls*	*Auditor's test of controls*	*Test findings*
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 the procedure for hiring new employees and verified that it includes a screening. We have in spot checks inspected that the procedure for hiring new employees has been followed. We have inquired about the formalisation of terms and conditions of employment for employees. We have inspected that the standard employee contract entails obligations of confidentiality.	Our tests have not resulted in any material deviations.

Control Objective:
To ensure that employees and contractors are aware of and fulfil their information security responsibilities.

Nr.	*Sentia Denmark A/S controls*	*Auditor's test of controls*	*Test findings*
7.2	Sentia Management acknowledge their responsibility for promoting the 'Code of Conduct' and creating the desired culture. Employees are obligated to read the Employee Handbook including the 'Code of Conduct' as well as the Information Security Policies. Sentia conducts awareness training programs, e-mails as well as at the departmental and staff meetings to ensure employees are familiar with the ISMS.	We have inquired about management's responsibility for the dissemination of policies and procedures. We have inspected documentation that employees have received education and training in information security and the organization's policies. We have inspected that employees are trained and certified in relevant technologies. We have inquired about sanctioning guidelines and we have inspected the guidelines.	Our tests have not resulted in any material deviations.

4. Control Objectives, Security Measures, Tests and Findings

7. Human Resource Security - continued

Control Objective: To protect the organisation's interests as part of the process of changing or terminating employment.			
Nr.	***Sentia Denmark A/S controls***	***Auditor's test of controls***	***Test findings***
7.3	There is a formal process for offboarding employees.	We have inspected the process for offboarding employees. For a sample of terminations, we have verified that the process has been followed.	Our tests have not resulted in any material deviations.

4. Control Objectives, Security Measures, Tests and Findings

8. Asset Management

Control Objective: To identify organisational assets and define appropriate protection responsibilities.			
Nr.	***Sentia Denmark A/S controls***	***Auditor's test of controls***	***Test findings***
8.1	Sentia has registered significant IT assets in a series of systems and defined ownership of categories of assets. All changes to customer assets have to be registered and approved according to change management process. Guidelines for accepted use of assets exist and are available to relevant staff members.	We have observed that assets are registered in systems, including CMDB, in Sentia. We have inspected that categories of assets have been identified and that owners have been appointed to the assets. We have verified that changes are to customers' assets follow changes management processes. We have inspected that guidelines for use of assets are defined in policies and procedures, which employees are informed about.	Our tests have not resulted in any material deviations.
Control Objective: **To ensure that the information receives an appropriate level of protection in accordance with its importance to the organisation.**			
8.2	Assets have classified and labeling have been applied for relevant aspects. Controls provide reasonable assurance, that there is appropriate operating documentation.	We have inquired about and inspected the classification and labelling of assets, data and customers. We have inquired about guidelines for the handling of assets and inspected how assets handled according to contracts and SLAs.	Our tests have not resulted in any material deviations.

4. Control Objectives, Security Measures, Tests and Findings

8. Asset Management - continued

Control Objective: To prevent unauthorised disclosure, modification, removal or destruction of information stored on media.			
Nr.	***Sentia Denmark A/S controls***	***Auditor's test of controls***	***Test findings***
8.3	Controls are implemented to secure the use of portable assets.	We have inquired about the management of removable media. We have inquired about guidelines for disposal of media and physical media transfer. We have inspected that removeable media have been securely destroyed.	Our tests have not resulted in any material deviations.

4. Control Objectives, Security Measures, Tests and Findings

9. Access Control

Nr.	Sentia Denmark A/S controls	Auditor's test of controls	Test findings
Control Objective: To limit access to information and information processing facilities.			
9.1	There is a policy and procedure for assigning, changing and revoking access rights for employees.	We have inspected the policies for assigning, changing and revoking access rights. We have inquired about policies for access to networks and network services. We have inspected the implemented policies.	Our tests have not resulted in any material deviations.
Control Objective: To ensure authorised user access and to prevent unauthorised access to systems and services.			
9.2	A formal business procedure exists for granting and revoking user access. Granting and application of extended access/privileged rights are limited and monitored. Internal users' access rights are reviewed regularly according to a formalised business procedure.	We have inquired about and inspected the user registration and de-registration procedure. We have in spot checks inspected user registrations and de-registrations on the infrastructure and in the applications during the audit period. We have inquired about the management and implemented controls of privileged access rights. We have inquired about procedures for the provision of secret authentication information. We have inspected controls for periodic review of user access rights and inspected documentation of the performed controls. We have inspected the applied controls.	Our tests have not resulted in any material deviations.

4. Control Objectives, Security Measures, Tests and Findings

9. Access Control - continued

Control Objective: To make users accountable for safeguarding their authentication information.			
Nr.	***Sentia Denmark A/S controls***	***Auditor's test of controls***	***Test findings***
9.3	Passwords are personal and kept secret.	We have inquired about users' use of secret authentication information and inspected guidelines. We have inspected documentation of a yearly control of the password policy.	Our tests have not resulted in any material deviations.
9.4	Access to operating systems and networks are protected by passwords. Sentia has established and implemented policies for access passwords, including their complexity, length, and periodic changes thereof. The user will be locked out in the event of repeated unsuccessful attempts to login.	We have inquired about guidelines for information access restriction and secure log-on procedures. We have inquired about the password management system and the use of privileged utility programs. We have inspected the password management system and the implemented requirements to ensure the quality of passwords giving access to relevant systems and applications. We have verified log-on possibilities to relevant systems and applications. We have inspected the applied controls.	Our tests have not resulted in any material deviations.

4. Control Objectives, Security Measures, Tests and Findings

11. Physical and Environmental Security

Control Objective:
To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities and to prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.

Nr.	*Sentia Denmark A/S controls*	*Auditor's test of controls*	*Test findings*
11.1	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 according to business and work-related needs.	We have inspected the physical security perimeters for Sentia's location. We have inquired about the procedure for allocation of access rights to the server room at Sentia Denmark A/S. We have inquired about securing of offices, rooms and facilities, and protection against external and environmental threats. We have inspected service auditor's assurance report for the outsourced operation and maintenance of physical housing for the audit period.	Our tests have not resulted in any material deviations.

4. Control Objectives, Security Measures, Tests and Findings

11. Physical and Environmental Security - continued

Control Objective:
To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities and to prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.

Nr.	*Sentia Denmark A/S controls*	*Auditor's test of controls*	*Test findings*
11.2	All information-related assets are protected against fire, water and heat. All information-related assets are protected from power-loss by UPS and emergency power systems. Cables for electronical communication and electricity supply are protected against tampering. Employees are required to ensure that clear desk and screen lock are enforced on laptops. Data carrying information-related assets are disposed of in a safe manner.	We have inspected the protection of operational facilities and maintenance of equipment at Sentia's data centres. We have inspected supporting utilities and the maintenance of supporting utilities including that security measures are in place to prevent and detect fire, water, and heat. We have inspected that UPS and power loss systems are in place and that cables are protected from tampering. We have inspected documentation for secure disposal of equipment. We have inspected guidelines for clear desk and unattended user equipment, including screen locks on laptops. We have inspected service auditor's assurance report for outsourced operation and maintenance of data centres.	Our tests have not resulted in any material deviations.

4. Control Objectives, Security Measures, Tests and Findings

12. Operations Security

Control Objective:
To ensure correct and secure operations of information processing facilities.

Nr.	*Sentia Denmark A/S controls*	*Auditor's test of controls*	*Test findings*
12.1	The operations procedures for business-critical systems have been documented, and they are available to staff with work-related needs. Segregation of duties is implemented in operational procedures. 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.	We have inspected that there are documented operation procedures and that they are available to all employees. We have validated that the employees are aware of the procedures and that the procedures are performed as expected. We have validated and tested controls in systems supporting the operational procedures to ensure that automatic controls are in place to ensure completeness and efficiency of the operational procedures. We have validated that there are automatic controls that ensure segregation of duties for critical procedures. We have inspected that there is a documented procedure for change management. We have verified that a formal system is used, and that the system supports the documented procedures. We have inspected and validated that the controls cannot be bypassed, and that: • change requests are registered and described • all changes are subject to formal approval before implementation	Our tests have not resulted in any material deviations.

4. Control Objectives, Security Measures, Tests and Findings

12. Operations Security - continued

Control Objective: To ensure that information and information processing facilities are protected against malware.			
Nr.	***Sentia Denmark A/S controls***	***Auditor's test of controls***	***Test findings***
12.2	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 patches.	We have inspected that the information security policy states how Sentia should be protected against malware. We have verified that information and information processing facilities are sufficiently protected against malware. We have noted that anti-virus software has been installed on selected servers and user equipment and that this software is updated.	Our tests have not resulted in any material deviations.

Control Objective: To protect against loss of data.			
Nr.	***Sentia Denmark A/S controls***	***Auditor's test of controls***	***Test findings***
12.3	Controls have been established, that 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 (SLA).	We have inspected that there are documented procedures for backup and that fixed backup jobs have been made. We have verified that the backup jobs are applied to systems and that the backup jobs are executed according to their schedule. We have inspected that reports are sent to employees and that these reports in timely fashion are handled and incidents are raised if there are failed backup jobs.	Our tests have not resulted in any material deviations.

4. Control Objectives, Security Measures, Tests and Findings

12. Operations Security - continued

Control Objective: To record events and generate evidence			
Nr.	***Sentia Denmark A/S controls***	***Auditor's test of controls***	***Test findings***
12.4	Controls have been implemented to provide reasonable assurance, that Sentia has implemented systems for the monitoring of server and network operations.	We have inspected that there is implemented a system for gathering and collection of logs and events from servers and network units. We have inspected that events trigger an event in the monitoring system and that employees handle the events according to urgency and effect. We have inspected the applied measures for protection of log information. We have verified that the management and Business Governance team periodically monitor the relevant log information. We have inspected that synchronisation of time has been implemented.	Our tests have not resulted in any material deviations.

4. Control Objectives, Security Measures, Tests and Findings

12. Operations Security - continued

Control Objective: To ensure the integrity of operational systems.			
Nr.	***Sentia Denmark A/S controls***	***Auditor's test of controls***	***Test findings***
12.5	Controls have been established, that provide reasonable assurance, that the operating platform is patched according to internal guidelines and the Supply agreements with customers (SLA).	We have inspected that there is a formal procedure for patching and updating operational systems. We have verified that all attended patches and updates are subject to change management. We have verified that there is a formal procedure for assessing if a patch or update is cleared for unattended release and that unattended patches and updates only are released based on client agreements. We have validated that failed or missing patches and updates are logged and reported. We have inspected that status on the integrity of the operating system is logged in the system.	Our tests have not resulted in any material deviations.

4. Control Objectives, Security Measures, Tests and Findings

12. Operations Security - continued

Control Objective: To prevent exploitation of technical vulnerabilities.			
Nr.	***Sentia Denmark A/S controls***	***Auditor's test of controls***	***Test findings***
12.6	Sentia performs continually vulnerability scanning of critical infrastructure based on updated knowledge of known vulnerabilities and best practices in network security. There are no technical limitations, either internally or for the customers. It is the responsibility of Sentia's customers and Sentia to comply with all licensing rights, for any installed software.	We have inquired about the management of technical vulnerabilities. We have inspected documentation showing that vulnerability scans are performed on a regular basis. We have inquired about restrictions on software installation.	Our tests have not resulted in any material deviations.

Control Objective: To minimise the impact of audit activities			
Nr.	***Sentia Denmark A/S controls***	***Auditor's test of controls***	***Test findings***
12.7	The employees performing the audit must be independent of the audited area. All audit activities and persons involved must be approved by Business Governance.	We have inspected documentation that internal audit is performed. We have inquired about performed audit activities on suppliers and ISO 27001 certification.	Our tests have not resulted in any material deviations.

4. Control Objectives, Security Measures, Tests and Findings

13. Communication Security

Control Objective: To ensure the protection of information in networks and its supporting information processing facilities and to maintain the security of information transferred within an organization and with any external entity.			
Nr.	***Sentia Denmark A/S controls***	***Auditor's test of controls***	***Test findings***
13.1	Controls have been established, that provide reasonable assurance that the network is secured using firewalls.	We have inspected that the network is documented and updated upon changes. We have verified that there are appropriate procedures in place to manage the network equipment. We have inspected that networks are separated, and connections are shielded through dark fiber. We have verified that the production environment is secured using firewalls.	Our tests have not resulted in any material deviations.
13.2	Controls have been established, that provide reasonable assurance, that the transfer of information is protected.	We have inspected information transfer policies and procedures. We have inquired about confidentiality and non-disclosure agreements.	Our tests have not resulted in any material deviations.

4. Control Objectives, Security Measures, Tests and Findings

15. Supplier Relationships

Control Objective:
To ensure protection of the organisation's assets that are accessible by suppliers and to maintain an agreed upon level of information security and service delivery in line with supplier agreements.

Nr.	*Sentia Denmark A/S controls*	*Auditor's test of controls*	*Test findings*
15.1	Risks related to external business partners are identified, and security in third-party agreements and security in relation to customers are managed.	We have inquired about and inspected the process of maintaining Sentia Denmark A/S' information security requirements in supplier relationships. We have inquired about the addressing of security within supplier agreements.	Some suppliers have ISAE 3402 assurance reports that do not cover the full audit period. Where this is the case the data processer has received Bridge Letters or Management statements from the supplier covering the relevant periods to cover the full period. Our tests have not resulted in any material deviations.

4. Control Objectives, Security Measures, Tests and Findings

15. Supplier Relationships - continued

Control Objective: To ensure protection of the organisation's assets that are accessible by suppliers and to maintain an agreed upon level of information security and service delivery in line with supplier agreements.			
Nr.	***Sentia Denmark A/S controls***	***Auditor's test of controls***	***Test findings***
15.2	Monitoring of suppliers must be conducted regularly, including supervision of external business partners.	We have inquired about controls for the monitoring of supplier services and changes in these. We have verified that Sentia has received and evaluated statements from key suppliers and that they have received bridge letters regarding gaps from prior statements that covered 2020, providing indications of 2021 statements that will be in line with the statements that covered 2020.	Some suppliers have ISAE 3402 assurance reports that do not cover the full audit period. Where this is the case the data processer has received Bridge Letters or Management statements from the supplier covering the relevant periods to cover the full period. Our tests have not resulted in any material deviations.

4. Control Objectives, Security Measures, Tests and Findings

16. Information security incident management

Control Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.			
Nr.	***Sentia Denmark A/S controls***	***Auditor's test of controls***	***Test findings***
16.1	Security incidents are reported to the management as soon as possible, and they are managed in a consistent and efficient way.	We have inspected the procedures for incident management, including reporting of security events. We have inspected that incidents are reported, and roles and responsibilities are defined. We have in spot check controlled that incidents have been registered and handled according to the process.	Our tests have not resulted in any material deviations.

4. Control Objectives, Security Measures, Tests and Findings

17. Information Security Aspects of Business Continuity Management

Control Objective: Information security continuity should be embedded in the organisation's business continuity management systems.			
Nr.	***Sentia Denmark A/S controls***	***Auditor's test of controls***	***Test findings***
17.1	A consistent framework has been established for the company's contingency plans to ensure that all the plans are coherent and meet all security requirements, and to determine the prioritization of tests and maintenance.	We have inspected the procedure for handling incidents. We have inspected that incidents are reported, and that roles and responsibilities are defined. We have in spot checks controlled that incidents have been registered and handled according to procedures. We have inspected that Sentia has performed a test of the Continuity Plan.	Our tests have not resulted in any material deviations.
Control objective: **To ensure availability of information processing facilities.**			
17.2	Controls have been established to ensure availability of information processing facilities.	We have inquired about the availability of information processing facilities. We have inspected service auditor's assurance report for outsourced operations.	Our tests have not resulted in any material deviations.

4. Control Objectives, Security Measures, Tests and Findings

18. Compliance

Nr.	Sentia Denmark A/S controls	Auditor's test of controls	Test findings
Control Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements			
18.1	Sentia has established procedures and controls to avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements. Controls have been established to ensure privacy and protection of personally identifiable information as required in relevant legislation and regulation where applicable.	We have inquired about controls to identify legal and contractual requirements. We have inspected the implemented controls regarding privacy and protection of personally identifiable information. We have inspected the implemented controls of cryptography.	Our tests have not resulted in any material deviations.
Control objective: To ensure that information security is implemented and operated in accordance with the organisational policies and procedures.			
18.2	Sentia has established controls to ensure that information security is implemented and operated in accordance with the organisational policies and procedures.	We have inspected implemented controls to ensure compliance with corporate policies and standards. We have inquired about implemented controls to ensure technical compliance review.	Our tests have not resulted in any material deviations.

PENNEO

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registereret, og informationerne er listet herunder.

"Med min underskrift bekræfter jeg indholdet og alle datoer i dette dokument."

Jakob Høholdt
Underskriver 1
Serienummer: PID:9208-2002-2-086945606573
IP: 81.7.xxx.xxx
2022-01-18 08:58:14 UTC
NEM ID

Anders Grønning Kjærgaard
Underskriver 2
Serienummer: PID:9208-2002-2-822661869402
IP: 82.192.xxx.xxx
2022-01-18 09:24:06 UTC
NEM ID

Martin Bomholtz
Underskriver 3
Serienummer: PID:9208-2002-2-013768766685
IP: 62.243.xxx.xxx
2022-01-18 09:27:07 UTC
NEM ID