

Independent auditor's report on general IT controls in relation to
operating and hosting services from 1 January to 31 December 2019

ISAE 3402 Type II

Sentia Denmark A/S

CVR-nr.: 10 00 81 23

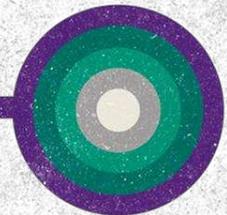
January 2020

Index

	Page	Assessment		Page	Assessment
1. Sentia Denmark’s Letter of Representation	3		• 15. Supplier Relationships	37	●
2. Sentia Denmark’s’ description of general IT’ controls for the operation of hosting activities	6		• 16. Information Security Incident Management	38	●
3. Independent Auditor's Assurance Report on the description of the general IT’ controls, their design and operating effectiveness	20		• 17. Information Security Aspects of Business Continuity Management	39	●
4. Auditor's description of control objectives, security measures, tests and findings	22				
• 4. Risk Assessment and Management	23	●			
• 5. Information Security Policies	24	●			
• 6. Organization of Information Security	25	●			
• 7. Human Resource Security	26	●			
• 8. Asset Management	27	●			
• 9. Access Control	28	●			
• 10. Cryptography	29	●			
• 11. Physical and Environmental Security	30	●			
• 12. Operations Security	31	●			
• 13. Communication Security	36	●			

Symbol

- Our tests have not resulted in any material deviations
- Minor weaknesses have been identified
- Major weaknesses have been identified



1. Sentia Denmark's Letter of Representation

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 from 1st January 2019 to 31st December 2019.

IMPORTANT EVENTS 2019

In 2019 Sentia continued the merger and integration of companies acquired in 2019 and before. At the same time Sentia has proceeded the planned activities for developing and optimizing the services for our customers. These activities include amongst others:

- Development and implementation of new organization;
- Consolidating the locations and datacenters;
- Aligning and optimizing of the ITSM (IT Service Management) processes based on ITIL and adopted to the ServiceNow ITSM application being implemented;
- Implementing improved ISMS (Information Security Management System) based on the ISO 27001 and 27701 standards;
- ISO 27001:2013 re-certification by KPMG for part of the business and preparations for an ISO 27001 certification of the rest of the organization in 2020;
- Continuing the development of the value proposition in Microsoft Azure and Sentia cloud solutions with the re-certification of the role of "Microsoft Azure Expert Managed Service Provider (MSP)" as one of approximately 30 worldwide and the only one in Denmark;
- Aligning the service deliveries across the many different locations, datacenters and public cloud;

- Maintaining procedures to support the regulation and guidelines in the GDPR (EU Regulation 2016/679 General Data Protection Regulation);
- Alignment and improvement of services, SLA (Service Level Agreements) and contractual terms to customer needs, market trends and GDPR.

COMPANY SCOPE OF THE ISAE 3402 TYPE 2 REPORT

The scope of this report is Sentia's delivery of managed services based on private, public or hybrid cloud platforms in datacenters around the world.

Sentia has used Microsoft, Amazon, B4Restore A/S, Front-safe A/S, j2 Global Denmark A/S, Hellosign, InterXion Danmark ApS, Teracom A/S, Cisco Danmark, F-Secure and GlobalConnect A/S as main subcontractors during the period for cloud, backup, mail security, digital signatures, datacenter facilities and physical security. This report includes only controls and control objectives for processes and controls, that are handled by Sentia and, as such, does not contain controls and control objectives that relate to controls and procedures handled by the above listed subcontractors. The compliance of the subcontractors is validated by Sentia through the external auditors reports and certifications i.e. ISAE 3402 type 2, SOC-2, ISAE 3000 or ISO 27001 from each of the subcontractors.

1. Sentia Denmark's Letter of Representation

The accompanying description has been prepared for customers, partners and their auditors, who have used cloud based operating platform offered by Sentia. The description is intended to recipients, who have enough technical and compliance understanding to evaluate the description along with other facts including information on controls, which the customers themselves have used in evaluating the risks of significant misstatements in the customers' financial statements.

Sentia Denmark confirms that:

- a) The accompanying description at pages 6-19 fairly presents a subset of Sentia Denmark's ISO 27002 controls on the the private, hybrid and public cloud based OSE (Operating System Environment) platform throughout the period from 1st January 2019 to 31st December 2019. The criteria used in making this statement 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, by which the general IT controls were operated
 - How the system dealt with significant events and conditions, other than transactions.
 - 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 and communication, control activities and monitoring controls that were relevant for the general IT controls.
- ii. Includes relevant details of changes to the organization's general IT controls and ISMS during the period from 1st January 2019 to 31st December 2019.
- 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 specific circumstances.

1. Sentia Denmark's Letter of Representation

- b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period from 1st January 2019 to 31st December 2019. 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 and;
 - iii. The controls were consistently applied as designed, including that manual controls were applied by individuals, who have the appropriate competence and authority, throughout the period.

Copenhagen, 21st January 2020
Sentia Denmark A/S
Lyskær 3A, 2730 Herlev
CVR-nr.: DK-10 00 81 23

Finn Vagner
Managing Director

2. Sentia's description of general IT controls for the operation of hosting activities

2.1 DESCRIPTION OF GENERAL IT CONTROLS

OVERVIEW AND DESCRIPTION

The following describes the general IT controls in relation to the OSE operated private, public or hybrid cloud platforms offered by Sentia Denmark A/S.

Sentia has three offices in the Copenhagen area, one in Odense and one in Aarhus and owns datacenters in Odense and Glostrup. Apart from the public cloud in Microsoft Azure, Amazon Web Services and Microsoft Office 365, Sentia operates major datacenters housed in locations owned and facility managed by subcontractors such as:

- Cloud services in Skanderborg (Fuzion)
- Cloud services in Taastrup (Two datacenters by GlobalConnect and InterXion);
- Cloud services in Glostrup (Two datacenters by GlobalConnect and InterXion)

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:

- Power and utilities;
- Medical and pharmaceutical;
- Architects and drawing offices;
- Financial institutions;
- Auditors;
- Web agencies;
- Public institutions.

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

To ensure stable operation as well as maintaining system and data 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 according to the ISO 27000 framework 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 27000;
 - Logical access;
 - Physical security;
 - Monitoring;
 - Patch management.
- Backup.
- Change management.

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.

2. Sentia's description of general IT controls for the operation of hosting activities

THE COMPONENTS OF THE INTERNAL CONTROL AT COMPANY LEVEL

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.

CONTROL ENVIRONMENT

This report includes exclusively a subset of Sentia's ISO 27002 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 27002 standard, and includes the overall organization, governance, policies and procedures defining the general attitude in the organization towards internal controls. Parts of Sentia's operation, datacenters and procedures is ISO 27001:2013 certified by KPMG Finland. The principles of ISO 27000 framework will be extended to the entire operation of Sentia in 2020.

Structure of the organization

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

- Infrastructure;
- Technology;
- Operations;
- Public Cloud;
- Projects;
- Service Delivery Management;
- Human Resources;
- Product Management;
- Commercial;
- Finance;
- Business Governance.

2. Sentia's description of general IT controls for the operation of hosting activities

Governance

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

- Managing Director;
- Technology Director;
- Operations Director;
- Commercial Director;
- Financial Director;
- Head of Human Resource;
- Head of Service Delivery;
- Head of Public Cloud;
- 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 authorizations for the individual groups or employees of the organization and determines authorisation hierarchies and rules and procedures for the reporting.

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

HR policies and practice

HR policies and practices relate 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 organizations 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 acknowledges 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.

2. Sentia's description of general IT controls for the operation of hosting activities

RISK ASSESTMENT (ISO 4. Risk Assessment and Management)

Risk assessment is a critical point in Sentia's internal control processes and ISO 27000 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 organizations ability to operate according to the obligations, the company has. Everyone in Sentia's management team is aware of, that risks are to be reported and treated separately, precisely to address and act according to the established framework based on the methodology of OCTAVE Allegro and ISO 27005.

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.

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 is 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.

2. Sentia's description of general IT controls for the operation of hosting activities

2.2 DESCRIPTION OF PROCESSES WITH RESPECTIVE CONTROL OBJECTIVES AND ACTIVITIES

OVERALL MANAGEMENT OF IT SECURITY (ISO 4.6 Organization of Information Security)

Sentia's Information Security Policies as part of the ISMS based on and certified by the ISO 27001:2013 standard 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 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 27000 procedures.

MONITORING OF SUBCONTRACTORS FOR IT OPERATION SERVICES (ISO 4.15 Supplier Relationships)

Sentia uses a range of subcontractors for IT operation services as part of the delivery of the services described in the report. Controls at the subcontractor's locations or procedures are not included in this report.

Sentia has only data located in the company in the two owned datacenters in Glostrup and Odense. Most of the company data is stored in the Microsoft cloud.

Sentia monitors the relevant suppliers through receipt and review of external auditor reports from these suppliers and validates that these include requirements and controls for sufficient assurance regarding physical security, access and backup.

Controls at the subcontractors are not covered by this report.

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 regarding relevant controls, including physical security, access and backup.

2. Sentia's description of general IT controls for the operation of hosting activities

OVERALL MANAGEMENT OF LOGICAL ACCESS (ISO 4.7 Human Resource Security, 4.9 Access Control and 4.13 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.

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.

2. Sentia's description of general IT controls for the operation of hosting activities

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 authorized 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's description of general IT controls for the operation of hosting activities

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 datacenter 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 datacenter 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.

2. Sentia's description of general IT controls for the operation of hosting activities

Assignment of administrator rights

Administrative rights in Sentia are only assigned to technical users, based on work-related needs.

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 work-station 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.
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 work-stations. For wireless MS-CHAP and certificate authentication is used on the devices.
Sentia BOYD	Separate VLANs per location for wireless network for Sentia's employees' own devices and phones with WPA2 encryption.

Sentia's own servers are placed in several secured datacenters on external locations or own two datacenters. Communications between Sentia office locations and the datacenter 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.

2. Sentia's description of general IT controls for the operation of hosting activities

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 accordingly 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.

PATCH MANAGEMENT (ISO 4.12 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 type 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.

2. Sentia's description of general IT controls for the operation of hosting activities

CHANGE MANAGEMENT (ISO 4.12 Operations Security)

Sentia has established a formal change management process. The process ensures 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.

In 2019 Sentia found that for changes with low priority and low impact, it had been possible for the same person to approve and implement the change. When Sentia identified this, an awareness campaign was implemented, in order to secure segregation of duties. This was followed by control of the affected changes. The Service Management system is being changed subsequently.

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.

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.

2. Sentia's description of general IT controls for the operation of hosting activities

BACKUP AND RESTORE (ISO 4.12 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 4.16 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 accordingly 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.

2. Sentia's description of general IT controls for the operation of hosting activities

ASSET MANAGEMENT (ISO 4.8 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 datacenter equipment, Contract Management systems and other relevant IT-operational tasks.
ITSM system	The IT service management (ITSM) systems contains information about SLAs, Configuration Items and CMDB data for day-to-day operation.
SharePoint/MS Teams	<p>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.</p> <p>The internal SharePoint sites (intranet) and Microsoft Teams organized information with all internal documents are only with access for Sentia employees.</p> <p>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.</p>

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 staff members.

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's description of general IT controls for the operation of hosting activities

PHYSICAL SECURITY (4.11 – Physical and Environmental Security)

Sentia has documented processes for maintaining physical security for offices and datacenters 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 unauthorized access in datacenters 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.

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 January 2019 to 31st December 2019, 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 in Chapter 2 and accompanying assertion, 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'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 1 under Letter of Representation. In our opinion,

- a) The description fairly presents the general IT controls of Sentia Denmark A/S for hosting activities, such as they were designed and implemented throughout the period 1st January 2019 to 31st December 2019 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 January 2019 to 31st December 2019; 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 January 2019 to 31st December 2019.

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, 21st January 2020

Grant Thornton

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

Jacob Helly Juell-Hansen
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 effectiveness 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 1st January 2019 to 31st December 2019.

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.

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

Metode	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.

4.2 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.

4. Control Objectives, Security Measures, Tests and Findings

4. Risk Assessment and Management

Risk assessment
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.

	Sentia controls	Auditor's test of controls	Test findings
4.1	The purpose is to identify and classify the risks that may affect the organizations ability to operate according to the obligations, the company has.	We have obtained the current and approved risk assessment. We have verified that frequent risk assessments have been carried out by the compliance team and reported to management. We have verified that Sentia has set a fixed, low level of acceptance of risks.	Our tests have not resulted in any material deviations.
4.2	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.	We have verified that Sentia's exposure is managed based on the risk score, which is calculated from the risk impact and likelihood.	

Penneo dokumentnøgle: PBHKB-GPQDE-0ULTD-ED213-GTHBQ-VDOCW

4. Control Objectives, Security Measures, Tests and Findings

5. Information Security Policies

Management direction for information security

Control objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

Sentia controls	Auditor's test of controls	Test findings
<p>5.1 An IT security policy and ISMS approved by Sentia's management has been prepared and implemented.</p> <p>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.</p>	<p>We have obtained and reviewed Sentia's latest IT security policy.</p> <p>We have verified that maintenance of the IT security policy is conducted on a regular basis. We have checked during our audit that the underlying supporting policies have been implemented.</p> <p>We have checked that the policy is approved and signed by the company's Supervisory and Executive Boards and made available for the employees on Sentia's Intranet.</p>	<p>Our tests have not resulted in any material deviations.</p>

4. Control Objectives, Security Measures, Tests and Findings

6. Organization of Information Security

Internal organization & Mobile devices and teleworking

Control objective: To establish a management framework to initiate and control the implementation and operation of information security within the organisation and ensure the security of teleworking and use of mobile devices.

Sentia controls	Auditor's test of controls	Test findings
6.1 All information security responsibilities should be defined and allocated. Conflicting duties and areas of responsibilities should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	We have verified that the responsibility for Information Security is defined and allocated to qualified employees. We have interviewed key employees and observed that they are aware of their responsibility. We have through our test of controls verified that segregation of duties have been implemented in the controls.	Our tests have not resulted in any material deviations.
6.2 The information security policy includes controls for remote access and security measures are implemented to ensure remote access.	We have inquired about the allocation of information security roles and responsibilities and segregation of duties. We have inquired about the process for contact with authorities and special interest groups. We have inquired about the policy for mobile device management. We have inquired about the implemented security measures for the use of teleworking sites.	

4. Control Objectives, Security Measures, Tests and Findings

7. Human Resource Security

Prior, during and after employment

Control objective: To ensure that employees and contractors are suitable for the role for which they are considered, understand and fulfil their responsibilities and to protect the organisation's interests as part of the process of changing or terminating employment.

	Sentia controls	Auditor's test of controls	Test findings
7.1	Sentia has established formal procedures for hiring new employees.	We have observed that there is a formal procedure for hiring new employees.	Our tests have not resulted in any material deviations.
7.2	Individuals offered a position in Sentia will be the 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 background checks are done on employees prior to employment. We have reviewed contracts and templates that state that the employee is obligated to uphold the contract and non-disclosure agreement. We have inspected that the process for offboarding employees is followed.	
7.3	There is a formal process for offboarding employees.		

4. Control Objectives, Security Measures, Tests and Findings

8. Asset Management

Responsibility for assets, Information classification & Media handling
 Control objective: To identify organisational assets and define appropriate protection responsibilities.

	Sentia controls	Auditor's test of controls	Test findings
8.1	<p>Sentia has registered significant IT assets in a series of systems.</p> <p>Guidelines for accepted use of all information-related assets exist and are available to relevant staff members.</p>	<p>We have observed that assets are registered in systems in Sentia.</p> <p>We have observed that employees are required to update the systems with relevant information.</p> <p>We have inspected that all information-related assets have been identified and that a system owner has been appointed to the asset.</p>	<p>Our tests have not resulted in any material deviations.</p>
8.2	<p>All information-related assets have been identified, that these have been classified, and that a system owner responsible for the assets has been appointed.</p> <p>Controls provide reasonable assurance, that there is appropriate operating documentation.</p>	<p>We have inspected that the documentation of assets is sufficient and correct.</p> <p>We have inquired about guidelines for the classification of data.</p>	
8.3	<p>Controls are implemented to secure the use of portable assets.</p>	<p>We have inquired about guidelines for the handling of assets, including portable assets.</p>	

4. Control Objectives, Security Measures, Tests and Findings

9. Access Control

Access control & management, User responsibilities & System and application access control
 Control objective: To limit access to information and ensure authorised user access and to prevent unauthorised access to systems and services.

	Sentia controls	Auditor's test of controls	Test findings
9.1	There is a policy and procedure for assigning, changing and revoking access rights for employees.	We have inspected the policy and procedure for assigning, changing and revoking access rights at Sentia. We have verified that all assignments, changes and removals are done through the Change Management process.	Our tests have not resulted in any material deviations.
9.2	A formal business procedure exists for granting and revoking user access. Granting and application of extended access rights are limited and monitored. Internal users' access rights are reviewed regularly according to a formalized business procedure.	We have inspected that management periodically validates all employees access rights and only assigns access based on work related needs. We have inspected that the password policy is enforced on all users.	
9.3	Passwords are personal and kept secret.	We have inspected that all access to systems is subject to a pre-defined password policy that is in line with the information security policy, which states the demands for length, duration and reuse of passwords.	
9.4	Access to operating systems and networks are protected by passwords. Quality requirements have been specified for passwords, which must have a minimum length (8 characters), no requirements as to complexity, maximum duration (90 days), and likewise password setup means that passwords cannot be reused (remembers the latest 24 versions). Furthermore, the user will be locked out in the event of repeated unsuccessful attempts to login. Controls have been established, that provide reasonable assurance, that administrator access is limited to individuals with a work-related need for access.	Users are locked out if they repeatedly have unsuccessful login attempts. We have inspected if all privileged user accounts are periodically checked for work-related accesses.	

4. Control Objectives, Security Measures, Tests and Findings

11. Physical and Environmental Security

Secure areas & Equipment

Control objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.

Sentia controls	Auditor's test of controls	Test findings
<p>11.1 All information-related assets are protected from unauthorized access in data centers 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.</p>	<p>We have inspected the two own data centers and verified that access is given based on work-related needs. We have inspected access logs.</p> <p>We have validated that the surveillance is complete and efficient according to Sentia's policies.</p> <p>We have verified that efficient and complete controls are in place to ensure protection against fire, water and heat. We have inspected that fire extinguishers are checked periodically, that sensors for heat and water are functioning properly.</p>	<p>Our tests have not resulted in any material deviations.</p>
<p>11.2 All information-related assets are protected against fire, water and heat.</p> <p>All information-related assets are protected from power-loss by UPS and emergency power systems.</p> <p>Cables for electronical communication and electricity supply are protected against tampering.</p> <p>Data carrying information-related assets are disposed of in a safe manner.</p>	<p>We have inspected that the data centers and information-related assets are protected from power loss with UPS and emergency power from diesel generators. We have inspected reports for tests that show that sufficient power is supplied from the generators.</p> <p>We have inspected that cables are secured and that electricity cables are protected from tampering. Furthermore, that employees in the data centers are protected against harm or damage.</p> <p>We have observed that all data carrying assets are disposed by certified third party.</p>	

4. Control Objectives, Security Measures, Tests and Findings

12. Operations Security

Operational procedures and responsibilities
 Control objective: To ensure correct and secure operations of information processing facilities.

Sentia controls	Auditor's test of controls	Test findings
<p>12.1 The operations procedures for business-critical systems have been documented, and they are available to staff with work-related needs.</p> <p>Segregation of duties is implemented in operational procedures.</p> <p>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.</p>	<p>We have inspected that there are documented operation procedures and that they are available to all employees.</p> <p>We have through our testing validated that the employees are aware of the procedures and that the procedures are performed as expected.</p> <p>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.</p> <p>We have validated that there are automatic controls that ensure segregation of duties on critical procedures.</p> <p>We have inspected that there is a documented procedure for change management.</p> <p>We have verified that a formal system is used, and that the system supports the documented procedures.</p> <p>We have inspected and validated that the controls in the procedure are defined as controls in the systems and that the controls can not be bypassed, and that:</p> <ul style="list-style-type: none"> • change requests are registered and described • all changes are subject to formal approval before implementation 	<p>Segregation of duties has not been implemented fully in ServiceNow. It has been possible for the same person to approve and implement low impact / low complexity changes without peer review.</p> <p>Sentia has stated their opinion on the weakness in section 3, page 16 (Change Management).</p>

Penneo dokumentnøgle: PBHKB-GFQDE-0ULTD-ED2B-GTHBQ-VDOCW

4. Control Objectives, Security Measures, Tests and Findings

12. Operations Security - continued

Protection from malware

Control objective: To ensure that information and information processing facilities are protected against malware.

Sentia 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.	<p>We have inspected that the information security policy states how Sentia should be protected against malware.</p> <p>We have verified that all employees are aware of the threats and precautions against malware.</p> <p>We have verified that information and information processing facilities are sufficiently protected against malware.</p>	Our tests have not resulted in any material deviations.

Backup

Control objective: To protect against loss of data.

Sentia 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).	<p>We have inspected that there are documented procedures for backup and that fixed backup jobs have been made.</p> <p>We have verified that the backup jobs are applied to systems and that the backup jobs are executed according to their schedule.</p> <p>We have inspected that reports are automatically sent to employees and that these reports in timely fashion are handled and incidents are raised if there are failed backup jobs.</p>	Our tests have not resulted in any material deviations.

4. Control Objectives, Security Measures, Tests and Findings

12. Operations Security - continued

Logging and monitoring

Control objective: To record events and generate evidence.

Sentia controls	Auditor's test of controls	Test findings
12.4 Controls have been implemented to provide reasonable assurance, that Sentia has implemented systems for monitoring of server and network operation.	<p>We have inspected that there is implemented a system for gathering and collection of logs and events from servers and network units.</p> <p>We have inspected that events trigger an event in the monitoring system and that employees handle the events according to urgency and effect.</p> <p>We have inspected the applied measures for protection of log information.</p> <p>We have verified that management and compliance team periodically monitor the efficiency of the event monitoring system.</p> <p>We have inspected that synchronization of time has been implemented.</p>	Our tests have not resulted in any material deviations.

4. Control Objectives, Security Measures, Tests and Findings

12. Operations Security - continued

Control of operational software		
Control objective: To ensure the integrity of operational systems.		
Sentia 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).	<p>We have inspected that there is a formal procedure for patching and updating operational systems.</p> <p>We have verified that all attended patches and updates are subject to change management.</p> <p>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.</p> <p>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.</p>	Our tests have not resulted in any material deviations.

4. Control Objectives, Security Measures, Tests and Findings

12. Operations Security - continued

Technical vulnerability management

Control objective: To prevent exploitation of technical vulnerabilities.

Sentia controls	Auditor's test of controls	Test findings
<p>12.6 Critical software applications and updates are monitored through the System Center Operations Manager (SCOM) tool.</p> <p>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.</p>	<p>We have inquired about the management of technical vulnerabilities.</p> <p>We have inquired about restrictions on software installation.</p> <p>We have inspected guidelines and applied controls</p>	<p>Our tests have not resulted in any material deviations.</p>

Information systems audit considerations

Control objective: To minimise the impact of audit activities

Sentia controls	Auditor's test of controls	Test findings
<p>12.7 The employees performing the audit must be independent of the audited area.</p> <p>All audit activities and persons involved must be approved by Compliance.</p>	<p>We have inquired about performed audit activities on suppliers and ISO 27001 certification.</p>	<p>Our tests have not resulted in any material deviations.</p>

4. Control Objectives, Security Measures, Tests and Findings

13. Communication Security

Network security management & Information transfer

Control objective: To ensure the protection of information in networks and in transfer and its supporting information processing facilities.

Sentia controls	Auditor's test of controls	Test findings
13.1 Controls have been established, that provide reasonable assurance, that the network is secured by the use of firewalls.	<p>We have inspected that the network is managed, documented and that documentation is updated upon changes.</p> <p>We have inspected that network services are based upon formal agreements with clients and suppliers.</p> <p>We have inspected that networks are separated and that there are effective controls to ensure that client networks are not accessible to other clients.</p>	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.	<p>We have inspected guidelines for information transfer policies and procedures.</p> <p>We have inspected that changes to the network is based on agreed upon changes.</p> <p>We have inspected that there is sufficient controls in place to secure the transfer of information, including multiple Internet Service Providers.</p> <p>We have inquired about confidentiality or non-disclosure agreements.</p>	

4. Control Objectives, Security Measures, Tests and Findings

15. Supplier Relationships

Information security in supplier relationships & Supplier service delivery management

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

Sentia 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's information security requirements in supplier relationships.	Our tests have not resulted in any material deviations.
15.2 Monitoring of suppliers must be conducted regularly, including supervision of external business partners.	We have verified that Sentia has received and evaluated ISAE 3402 Type II statements from key suppliers and that they have received bridge letters regarding gaps from prior statements that covered 2018, providing indications of 2019 statements that will be in line with the statements that covered 2018.	

4. Control Objectives, Security Measures, Tests and Findings

16. Information security incident management

Management of information security incidents and improvements

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

Sentia controls	Auditor's test of controls	Test findings
16.1 Security Incidents are reported to Management as soon as possible, and they are managed in a consistent and efficient way.	<p>We have inspected the ITSM systems and have observed that all automatic and manually entered security incidents are registered in the systems.</p> <p>We have inspected the procedures for handling security incidents and have verified that management are aware of their roles and that these roles are clearly defined.</p> <p>We have verified that the Security Incident Management plan has been tested.</p>	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

Information security continuity & Redundancies

Control objective: To ensure that information security continuity is embedded in the organisation's business continuity management systems availability of information processing facilities

Sentia 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 that Sentia have a business continuity plan and that it has been reviewed and approved by management. We have verified that the plan has been tested and that the results have been reviewed by management.	Our tests have not resulted in any material deviations.

Penneo dokumentnøgle: PBHKB-GPQDE-0ULTD-ED21B-GTHBQ-VDOCW



© 2020 Grant Thornton International Denmark - All rights reserved.

"Grant Thornton" refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires. GTIL and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms. GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions.

PENNEO

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

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

Jacob Helly Juell-Hansen

Statsautoriseret revisor

Serienummer: CVR:34209936-RID:50904197

IP: 62.243.xxx.xxx

2020-01-21 12:36:27Z

NEM ID 

Anders Grønning Kjærgaard

Revisor

Serienummer: PID:9208-2002-2-822661869402

IP: 2.109.xxx.xxx

2020-01-21 13:12:39Z

NEM ID 

Finn Vagner

Underskriver

Serienummer: PID:9208-2002-2-527151872232

IP: 81.19.xxx.xxx

2020-01-21 18:11:47Z

NEM ID 

Penneo dokumentnøgle: PBHKB-GPQDE-0ULLTD-ED213-GTHBQ-VDOCW

Dette dokument er underskrevet digitalt via **Penneo.com**. Signeringsbeviserne i dokumentet er sikret og valideret ved anvendelse af den matematiske hashværdi af det originale dokument. Dokumentet er låst for ændringer og tidsstemplet med et certifikat fra en betroet tredjepart. Alle kryptografiske signeringsbeviser er indlejret i denne PDF, i tilfælde af de skal anvendes til validering i fremtiden.

Sådan kan du sikre, at dokumentet er originalt

Dette dokument er beskyttet med et Adobe CDS certifikat. Når du åbner dokumentet

i Adobe Reader, kan du se, at dokumentet er certificeret af **Penneo e-signature service** <penneo@penneo.com>. Dette er din garanti for, at indholdet af dokumentet er uændret.

Du har mulighed for at efterprøve de kryptografiske signeringsbeviser indlejret i dokumentet ved at anvende Penneos validator på følgende websted: <https://penneo.com/validate>