Independent service auditors report
ISAE 3402-II

SAC-IT A/S
CVR-no.: 28 89 29 77
February 2024

Aaen & Co. statsautoriserede revisorer p/s - CVR nr.: 33 24 17 63
Kongevejen 3, 3000 Helsingør – Mileparken 22B, 3. sal, 2740 Skovlunde
Telefon 49 21 06 07 - www.aaenco.dk

Content

Section 1: SAC-IT's Management Statement

The following description is available for SAC-ITs customers, who have purchased a hosting service subscription on servers, infrastructure, or hosting, as well as their auditors. The expectation is that the receivers understand the controls sufficiently to assess the information in this document.

SAC-IT A/S uses Fuzion and Digital Realty as subservice suppliers for housing services. This report uses the carve-out method and does not comprise control objectives and related controls that Fuzion and Digital Realty perform for SAC-IT A/S.

SAC-IT A/S uses Veeam, Cove and Avepoint as subservice suppliers for backup services. This report uses the carve-out method and does not comprise control objectives and related controls that Veeam, Cove and Avepoint perform for SAC-IT A/S.

SAC-IT A/S hereby confirms that the following document:

- Contains a valid description of SAC-IT A/S' hosting and cloud services covering the period from 1st of January 2023 to 31st of December 2023. The criteria for this statement were, that the following description contains:
    - A description of the services delivered and how the system is designed and implemented.
    - The processes, both automated and manual, used to initiate, register, process, and, if necessary, correct transactions and transfer them to reports prepared for customers.
    - Relevant control targets and controls designed to achieve these.
    - Other aspects of our control environment, risk assessment process, information system and communication, control activities, and surveillance controls that have been relevant to the processing and reporting of customer transactions.
- Brings relevant information about changes in systems of SAC-IT for the period from 1st of January 2023 to 31st of December 2023
- Do not omit or distort information relevant to the scope of the system described.
- The description has been prepared to meet the general needs of a wide range of customers and their auditors and can therefore not address individual needs.
- The controls associated with the control objectives listed in the accompanying description were appropriately designed and worked efficiently for the period from 1st of January 2023 to 31st of December 2023 . The criteria for this opinion were that:
    - The risks threatening the achievement of the control objectives listed in the description were identified.
    - The identified controls would, if used as described, provide a high level of assurance that the risks involved did not prevent the achievement of the stated control targets.
    - The controls were used consistently as designed, including that manual checks were performed by persons with appropriate competence and competence during the End of 2023.

Vedbæk, 22nd January 2024 - SAC-IT A/S
Jackie Amelung, CEO

Section 2: SAC-IT and the services

About SAC-IT A/S

SAC-IT was formed in 2005 by Steen Amelung. In 2006 the board was extended with Jackie Amelung and Jørgen Jensen. In December 2020 the company changed ownership and is today owned by Jens Morten Hansen, Jakob Arndt, and Jackie Amelung

SAC-IT A/S has offices in Vedbæk and Fredericia and has currently 25 employees.

High-level description

SAC-IT A/S delivers infrastructure and operational services, outsourcing, and cloud solutions in Denmark to small and medium-sized companies within private and public sectors.

SAC-IT has a vision to become a preferred provider of VMware-based infrastructure within the customer segment that SAC-IT operates.

SAC-IT offers the following services to the hosting market:

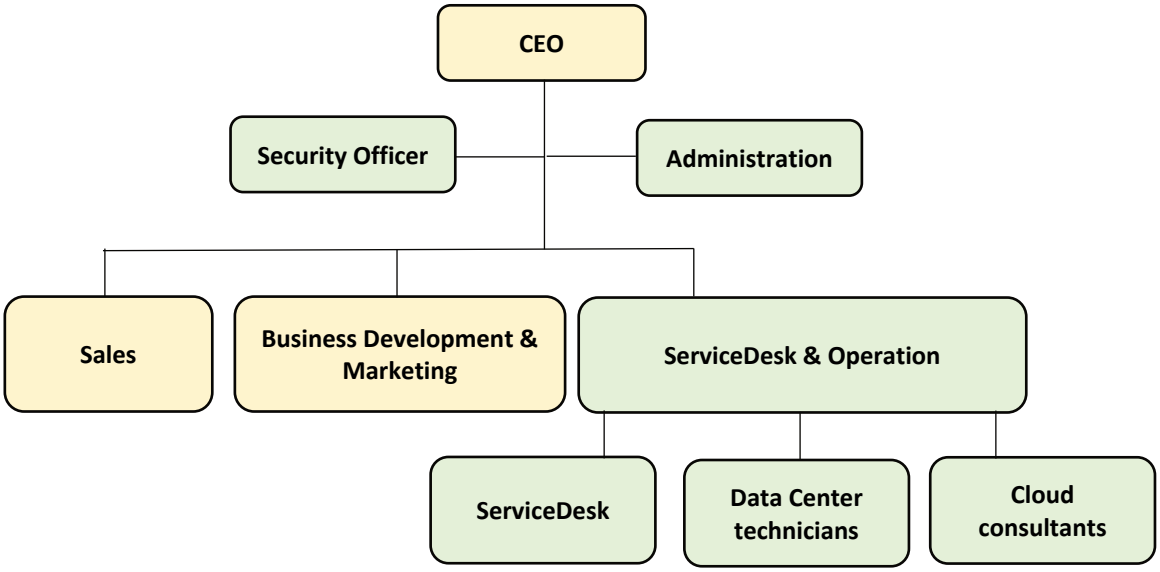
- Hosting and housing
- Remote backup
- Operation
- Hybrid cloud solutions
- Service Desk
- Endpoint Management
- Legal & Compliance
- Compliance & Security

SAC-IT MS Cloud offers the following services:

- Modern Workplace
- Baseline Security Tools
- SIEM
- Reporting/Monitoring
- Whistleblower
- Secure Mail
- Cloud Backup
- Cloud print services
- Awareness

Organization

SAC-IT's organization consists of the following functions and teams:



1) **CEO**
   The CEO handles the daily management of all functions and escalated events around the datacenter.

2) **Sales and Marketing**
   Handles sale-related matters, customer contact, and implementation agreements and contracts and marketing related, home page, and SoMe.

3) **Business Development**
   Handles business development

4) **Security officer**
   The head of security handles the security policy process, GDPR compliance, and ISAE 3402/ISAE 3000-related matters.
   The head of security is at the same time team lead for the MS Cloud Team.

5) **ServiceDesk, Operation, and Cloud**
   Team of data center technicians, cloud consultants, and team lead responsible for:
   a. The day-day manning of the **Service Desk function** handling incoming
      i. Service and implementation requests from customers
      ii. Alarms and incidents

   b. Daily backup and batch jobs setup
   c. Firewall and security setup
   d. New customer implementations and changes
   e. Major change handling and execution
   f. 24-7 Monitoring of all operations in the datacenter
   g. SLA Reporting

The organization is physically located at Frydenlundvej 30 in Vedbæk and Vesterballevej 5 in Fredericia.

Only the green part shown in the organizational diagram above is described further, as this part of the organization is the major caretaker of the data center setup and operation.

The ServiceDesk and Operation

The team consists of 15 people and is responsible for the operation of the data center, located at Digital Realty in Ballerup, and for all changes carried out to this infrastructure. The team includes skilled data center technicians and cloud consulting professionals. The team lead is responsible for service management of the customers and resource management. The team lead ensures that operation is handled 24-7 and that changes are handled safely and securely in the infrastructure of the data center.

The ServiceDesk and Operation team handles support calls during business hours and manages incoming support emails as per service level agreements with clients, which may slightly vary for each customer. Client details are stored securely, accessible only to company personnel. Within business hours, the team gathers for a sprint meeting to ensure all incidents and service requests comply with the Service Level Agreements (SLAs).

Daily incoming support tickets are placed in the Service Management System. This is the administrative repository for service requests, incident handling, and changes management. SAC-IT has implemented ITIL from the day the company was established. This means that service delivery and operation are standardized into roles and processes.

During business hours, at least 4 staff members attend to the support phone and support mail. Outside opening hours, there is always an escalation technician on call. This function acts as a prioritization function if alerted regarding major incident handling and escalating matters upwards to the team lead and the CEO. If technicians need to deal with these outside office hour events, then it is the escalation technician's responsibility to do so. Smaller and non-critical incidents are typically postponed to daytime service desk staff, and urgent incidents are escalated to the right technician(s) and handled best effort depending on the circumstances.

The 24-7 operation is monitored via a set of alarms and job reporting mechanisms. This ensures that security, availability, and batch/backup jobs are continuously handled. The security logs and backup job monitoring are handled outside office hours by a dedicated monitoring team/schedule. During office hours the monitoring is done by the service desk via the monitors in the service desk room.

Any changes to the infrastructure and customer solutions are logged/documented in the Support/Service Management System. Change management is the process followed when assessing change risk and governs how changes are handled. Normal changes are considered low risk, ex. the change of a password, the allocation of disk space, the modification to a backup policy. In changes where there is a risk of a widespread impact or downtime, the major change process caters to the information flow to customers and management. The Major changes are in ex. changes to central firewalls, changes to central storage infrastructure or virtual infrastructure servers, major upgrades to a bulk of customer servers, etc. In the event of a major change, three central questions are typically asked before a major change is planned and executed:

a) How many customers are impacted?

b) Can downtime be avoided or mitigated?
c) Do we need a dialogue with the impacted customers (to assure that downtime is not business critical to the customer), and to ensure service is back?

The last part of part c), is rarely necessary. Most major events are handled without engaging in activities during the major change execution with the customers. But the customers are always warned and given a heads up. Several customers need a minimum heads-up of 14 days before downtime can be accepted. Major changes are often carried out outside normal business hours and followed by extensive system tests and alarm monitoring.

High-Level Datacenter description

Physical security around the data center

The Datacenter is the heart of SAC-ITs operation. It is located at Digital Realty in Ballerup. SAC-IT has its server room, where only SAC-IT-approved personnel can get access. Digital Realty handles all physical access to the premises. The entire data center facility is located behind an electric fence, with few entry points, video monitored and surveilled 24-7. To get access to the SAC-IT server room, only a few SAC-IT technicians can get access, following Digital Realty strict procedures. SAC-IT's server room is video monitored by Digital Realty. Personnel coming into the server room and leaving the server room are weighed, to ensure that nothing is removed without notifying Digital Realty personnel. Access is controlled by fingerprint technology.

Redundancy

The SAC-IT Server room consists of SAC-IT equipment set up in racks. All equipment is built with N+1 redundancy on all critical systems. An example of this is that all power sources are backed up by UPS and diesel generators. Cooling is also redundant.

Logical security in the data center

All networked data paths between the internal servers to the SAC-IT backbone net are going through 3 levels of firewalls. The data paths are handled in a way so that no single point of failure can take down customers' access to their solutions at SAC-IT. The internal storage solutions are created so that multiple redundancies secure the customer's data. Firewalls and all servers in the data center are firmware and patch updated, as soon as our technicians have ensured the stability and impact of the updates.

Everything is closely monitored 24-7 by SAC-IT remotely:

1. Network components such as routers and firewalls
2. Data Traffic patterns
3. Security logs
4. Servers (both SAC-IT and customers)
5. Data storage solutions
6. Capacity
7. Backup jobs

If something is found to deviate from the status quo, incidents are raised and handled.

Service Management

All incidents and changes are logged, prioritized, and handled in the Service Management System. For a more technologically coherent description of each customer solution, each customer has a dedicated document share. This is updated to reflect changes to the customer's infrastructure.

Special care is taken towards so-called major changes. These affect more than one customer and involve the management of SAC-IT and the CEO. They involve the alert of all customers if downtime is expected or at risk and needs to be sent out with a minimum of 2 weeks notice. Major changes are allowed approved by the CEO.

The Control Environment

The Company's controls are reflecting the position that management has taken toward the certification of ISAE3402 type II. Management wants to drive SAC-IT into enterprise-class operation and has the wish to become ISAE 3000, ISO/IEC ISO 27001/2 certified. The controls also reflect the management position taken towards risk assessment, controls, and the importance placed on these controls, politics, processes, procedures, and methods – and the organizational structure is chosen.

The controls have been selected carefully to ensure to the management that SAC-IT is in control of the operation and secure handling of the customer's solutions. The controls are discussed continuously and revised yearly. Management has decided to use the same controls for 2023 as for 2022 to ensure consistency. The controls are estimated to be essential ones for the service delivery of SAC-IT's data center.

The controls are backed up by SAC-IT's security policy. This policy is also revised yearly and handled via the same process as the controls.

The control environment is facilitated by the security officer function in close dialog with management.

Risk Assessment

SAC-IT conducts activities continually to:

- Map and document the server infrastructure in the datacenter.
- Identify threats that have an essential risk of becoming major incident.
- Identify, select, and prioritize the mitigation efforts to match the risk picture.

The probability and consequence of the threats are reevaluated based on the information available. All these together are a measure of the threat level. If the threat level is low there is a smaller demand for mitigation efforts, than if the threat levels are assessed as high. When the threat level is estimated, an evaluation is carried out to determine if the mitigation method is sufficient or not. Management decides if a risk can be accepted, must be mitigated, or needs an insurance deposit. If a risk must be mitigated, a mitigation plan is taken out at the same time. This ensures that if a risk has a high impact x probability value, then mitigation will be carried out to handle the risk so that it no longer presents a threat to the continuous operation of SAC-IT and the risk can be lowered.

A yearly formal revision of the risk assessment is done, by taking input from all functions of SAC-IT, the outcome of the continually based activities, and relevant legal and public authority requirements that need to be handled and catered for. This process is facilitated by the Security officer function. The final reviewed risk assessment is presented to and approved by the CEO and Board of SAC-IT.

Controls

The Company's controls are reflecting the position that management has taken toward the certification of ISAE3402 type II. Management wants to drive SAC-IT into enterprise-class operation and has the wish to become ISO/IEC ISO 27001/2, NIS2 certified. The controls also reflect the management position taken towards risk assessment, controls, and the importance placed on these controls, politics, processes, procedures, and methods – and the organizational structure is chosen.

The controls have been selected carefully to ensure to the management that SAC-IT is in control of the operation and secure handling of the customer's solutions. The controls are discussed continuously and revised yearly. Management has decided to use the same controls for 2023 as for 2022 to ensure consistency.

As part of the journey towards ISO27001 SAC-IT is subject to an annual IT audit which results in an annual audit report prepared in compliance with the ISAE 3402 standard.

The controls are backed up by SAC-IT's security policy. This policy is also revised quarterly and handled via the same process as the controls.

The control environment is facilitated by the security officer function in close dialog with the CEO and management.

With the management we are:

- Monitoring and measuring status of information security.
- Performing internal audits
- Evaluating information security and measures
- Performing Management review with top management.

The following controls are used by SAC-IT:

1. All datacenter and managed services customers have a contract

SAC-IT uses a formal contract template. This ensures that all aspect of the datacenter service delivery is described and agreed with the customer and is aligned with SAC-IT security policy. This is also a quality guarantee that there is a clear agreement of what is delivered as part of operation service. All customer solutions in the datacenter must be mapped to a signed contract following the standard contract template.

2. A security organization is in place.

SAC-IT's management has implemented controls to secure that there is an overall authority in place to govern the information security, and delegated the responsibility and a handling of risks in accordance with requirements from management:

a) Management obligations in connection to the information security
   Management takes an active part in the information security in the organization. The formal responsibility of approving the security policy, lies at the CEO.
b) Coordination of the information security
   Activities to secure that information security is broadly coordinated in SAC-IT is facilitated by the Security Officer, who ensures that all aspects of information security is reviewed by the staff, team leads and management.
c) Information Security overall responsibility.
   The overall day-day responsibility of the security lies at the Security Officer who ensures that policies, procedures, and controls are implemented in the day-day handling of information security.

3. Controls are in place and cover sufficiently.

The IT security policy ensures that SAC-IT is ensuring and safekeeping customers and own assets sufficiently. The controls are the baseline of this. The controls are as a minimum evaluated on a quarterly basis by management. However, many of the controls are a result of day-day operations and requires no extra effort as they are built into the organization and procedures.

4. Risk analysis is performed, and high prioritized risks are mitigated.

Management has chosen the risk analysis method to have a formal way of dealing with threats to the datacenter operation. This results in a priority and grouping of risks, and the mitigation of the selected ones.

5. IT Security Policy is updated

SAC-IT has designed and chosen a process, that leads to changing the IT security policy whenever this is needed. As threat scenarios continuously change, new vulnerabilities emerge and become exposed and existing vulnerabilities needs reevaluation - all this will lead to changes or adjustments to the IT security policy and staff training.
The control checks that such a process is in place and that there is a linkage to the risk assessment that fits purpose.

6. Staff is trained in the security policy and its changes

SAC-IT has established controls to ensure that the staff is familiarized with the IT security policies on a continuous basis, in a way that enables them to safe-keep customers assets. All staff in Service Desk & Operation is cleared to access customer infrastructure.

All employees pledge that they will obey the information security upon signing of their employment contract.

Breaches to the security policy is reported directly to the security officer and to the CEO.

7. Customer solutions are documented

Before a new customer is going into operation, all implementation documents follow the same template are made and placed in the customer document repository. Whenever a change has been made to a customer solution, the customers documentation is updated. The standard document template is created in such a way, that key information as:

a) Server infrastructure
b) Server software
c) Service levels
d) Special procedures
e) Contact information

Is available to both service desk as well as operation technicians.

Not all changes are leading to updates in the documentation on individual customers. But if this is not the case, the major changes are always logged in the Service Management System. Examples of things that are not documented at the level of the individual customers:

a) User password resets which are documented in the service management system if it was a request.
b) Major upgrades and migration of storage system are documented in SAC-IT's system documentation, and in the service management system as a major change.

8. All staff has signed a confidentiality agreement

All new employees of SAC-IT are given the security policy and must sign a confidentiality agreement. The confidentiality is not limited to the contract period but extends to the period after contract has been terminated by either side.

9. Employment contracts contain roles

All employees are designated a role and a description of the role in their employment contracts. This is to ensure that there is a clear segregation of duties between, technicians, datacenter specialists and other. The role description chosen matches the outlines in the security policy and ensures the right training and enhancement of competences, skills and similar access rights. The CEO and Security Office roles are described elsewhere. The roles around the Data Center are:

a) **Role: Other/non-datacenter technician**
   This role can access internal disk drives with documentation, the mail and office suite

b) **Role: Datacenter technician**
   This role has the same access rights as a non-datacenter technician, can access all customer solutions and servers, can be granted access to the datacenter on singular or regular basis, can access the Service Management System, can access the Monitor System, can access the customer backup system.
   Only staff in the Service Desk and Operation team or the CEO can have this role.

c) **Role: Datacenter technician with elevated rights**
This role has the same access rights as the Data Center technician. This role has elevated rights to the administrative superuser settings in the core firewall, the storage system and the core backbone routers and switches, the storage switches, and similar central components in the backbone infrastructure common to all customers. Only 2 persons has these rights at the moment. Only staff in the Service Desk and Operation team can have this role.

d) **Role: Team lead Data Center technicians**

e) Cloud Admin

f) Support/Helpdesk

The Team Lead approves physical access to the datacenter. This can be granted on a regular scheme (all Service Desk & Operation staff) or on a one-time/singular scheme (3rd party specialists who needs physical access to the datacenter, ex.: Cisco, EMC, IBM core component specialists). The 3rd party specialist is always accompanied by SAC-IT staff in the datacenter.

10. Former employees do not have access to any systems

No former employee can access SAC-IT's core systems when the employee becomes a former employee. This means that the employees granted access rights in the VMware datacenter Active Directory and other relevant places are removed, and all SAC-IT owned equipment is returned.

11. All employee PCs are protected by anti-malware

To ensure that malware is not gaining access to the datacenter, all employee PCs and similar, has installed malware protection that is updated on a regular basis.
All endpoints are protected by Realtime scan and firewall

12. Only qualified technicians have access to the infrastructure

SAC-IT's IT security policy states that only qualified technicians are granted access to the datacenter infrastructure. This means that the personnel that operates the datacenter are trained, have the right skills, tools, methods and way of thinking. This also means that no customer is allowed access to the facility. Only a restricted list of SAC-IT's personnel is granted access to the datacenter as mentioned above.

13. Physical access to headquarter is protected

SAC-IT has established measures to ensure that the IT security policy is kept regarding physical access to the head quarter. The headquarter is in this respect protected behind 3 gates, alle requiring and access brick(key) with a pin code. At the same time all computers are locked if personnel step away from the computer. All computers are closed when office premises are closed down/outside office hours.

14. Logical access, vendors

Vendor access is governed by the security policy, to ensure that all vendor access is temporary, approved by SAC-IT and in relevant cases, by a customer.

15. Administrative passwords are renewed on a regular basis

Renewal of passwords on servers and infrastructure is done on a regular basis. Most of the systems are governed by AD policies in this respect. A few systems need manual updated password change.

16. Passwords to password management system

All server and infrastructure administrative passwords are kept in a password management system. This is in accordance with the IT Security Policy, and the password management system is protected by a very strong password, known to a limited list of SAC-IT's personnel.

17. Check datacenter vendor policy quality

Ensure that datacenter is well protected (physical access process). The datacenter access procedures are tested every time access is need to the datacenter premises. Any deviation to previous procedure is reported back and assessed to ensure the quality of the procedures.

18. Check that customer backups can be restored

All customer servers and data drives are backed up via a backup policy. In order to check that backup policy and procedure as well as a capability to restore servers is in place

19. Tickets have been prioritized correctly

All new incidents and service requests are prioritized by a simple scheme based on how many is affected or impacted by the request or incident. This enables SAC-IT to work on the service tickets in the right order, both in alignment with customer needs and urgency, but also in accordance to service agreements.

20. Tickets are processed in the correct way

All ServiceDesk personnel are well trained in handling service requests and incidents. The priority of these is handled and upon creation but is revisited at least twice a day during the work on these. The target is to ensure that lower prioritized tickets from one customer is not stealing away important focus on higher prioritized ticket belonging to other customers. Incidents is also handled before service requests. This ensures that all customer contract related service level agreements are fulfilled.

21. Ensure that all critical systems are operatable by at least two persons

SAC-IT is a small company with dedicated resources to several key components. SAC-IT has chosen to invest in training to avoid the use of key resource dependencies. The starting point is a map of competence of critical systems versus personnel competence. A plan is created and maintained together with the individual (MUS) to ensure that at least two persons are covering critical systems by their know how.

22. Monitors are monitored and reacted upon at frequent intervals during the day

All alarms and monitors are set up in the monitor system. Service Desk personnel can monitor status of the datacenter operation via a monitor placed on the wall in the Service Desk/Operation room. Whenever an alarm goes off, this is clearly signaled by a red color in the display, to ensure that the alarm is reacted upon swiftly.

23. Check that major changes are listed in the Service Management System

Major changes are following a special procedure that caters for the customer involvement and information flow as well as management interaction and approvals. Major Changes are always approved by the CEO. The process is logged in the Service Management System.

24. Ensure that a set of capacity monitors on core infrastructure is in place

Part of the monitors cover key capacity measures, like available diskspace, bandwidth usage on the outgoing network and CPU and RAM resource usage. This ensures that a capacity plan can be formed and approved in good time prior to running out of available infrastructure capacity.

25. All infrastructure and client equipment are protected with suitable malware protection

Same aspects are covered as with control 11 but for infrastructure and client equipment. For some components in the infrastructure, it is firmware updates.

26. Backup/restore process in place and backup is in place on all infrastructure equipment

Backup and restore processes are reviewed at three instances:

a. Whenever the customer solution is put into production, it is assured that all infrastructure components (servers, disks, etc.) are backed up by SAC-IT's backup solution.
b. Whenever changes to a customer or SAC-ITs own solutions are taking place, a check is made to whether or not backup policy needs adjustment or not.
c. During restore tests to evaluate whether changes are needed or not

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

To Management of SAC-IT A/S and their costumers

Scope
We have been engaged to report on SAC-IT A/S' description in section 2 of its general IT controls for operation of user systems to process customers' transactions throughout 1st of January 2023 to 31st of December 2023, and on the design and operation of controls related to the control objectives stated in the description.

SAC-IT A/S' responsibilities
SAC-IT A/S is responsible for: preparing the description (section 2) and accompanying assertion (section 1), including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; stating the control objectives; and designing, implementing and effectively operating controls to achieve the stated control objectives.

Our independence and quality control
We have complied with the independence and other ethical requirements set out in the International Ethics Standards Board for Accountants' international code of ethics for professional accountants (IESBA Code), which incorporates the basic principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior, as well as ethical requirements applicable in Denmark.

Our audit firm applies International Standard on Quality Management 1, ISQM 1, under which we are required to design, implement and operate a quality control system, including policies or procedures for compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Aaen & Co. statsautoriserede revisorer p/s' responsibilities
Our responsibility is to express an opinion on SAC-IT A/S' description, design and operating effectiveness of controls related to the control objectives stated in that description, based on our procedures. We conducted our engagement in accordance with International Standard on Assurance Engagements 3402, "Assurance Reports on Controls at a Service Organization," issued by the International Auditing and Assurance Standards Board. That standard requires that we comply with ethical requirements and plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are suitably designed and operating effectively.

An assurance engagement to report on the description and design of controls at a service organization involves performing procedures to obtain evidence about the disclosures in the service organization's description of its system, the design and operating effectiveness of controls. The procedures selected depend on the service auditor's judgment, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization and described in section 2.

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

Limitation of controls at a service organisation
SAC-IT A/S' 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 its own particular environment. Also, because of their nature, controls at a service organization may not prevent or detect errors or omissions in processing or reporting transactions. Also, the projection of any evaluation of effectiveness to future periods in subject to the risk that controls at a Service Organization may become inadequate or fail.

Opinion
Our opinion has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion are those described in section 2. In our opinion, in all material respects:

a) The description fairly presents the general IT controls as designed and implemented throughout the period from 1st of January to 31st of December 2023; and

b) The controls related to the control objectives stated in the description were suitably designed throughout the period from 1st of January to 31st of December 2023.

c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period from 1st of January to 31st of December 2023.

Intended users and purpose
This report and the description of tests of controls at section 4 are intended only for customers who have used SAC-IT A/S' IT services, and their auditors, who have a sufficient understanding to consider it, along with other information including information about controls operated by customers themselves, when obtaining an understanding of customers' information systems relevant for financial reporting purposes.

Helsingør, 29th of January 2024
Aaen & Co. statsautoriserede revisorer p/s
Kongevejen 3, 3000 Helsingør – CVR 33 24 17 63

Kenn Elmgren
State Authorized Public Accountant
MNE no. 26676

Section 4: Description of targets, control and test of these

The controls and control targets are those described in the previous paragraph. The Tests are those that has been decided as necessary to determine whether or not the targets have been met. The test results and comments to the results, has been described below with notes and comments on their efficiency covering the period from Jan. 1st, 2023 to Dec. 31st, 2023 .

Test of the Controls design and implementation has been executed by **interview**, **inspection**, **observation,** and **repetition/execution**.

Type	Description
Interview	Interview of the relevant staff and roles at SAC-IT has been executed for all relevant control activities. The interviews have been executed to among other things to achieve a knowledge and further information about the implemented policies and procedure, how control activities are executed, and to get a confirmed proof for policies, procedures and controls.
Inspection	Documents and reports, containing evidence for the executed controls, has been read with the purpose to evaluate how the controls has been designed, and how the controls have been monitored, to assess their efficiency and completeness. Similarly, to find out whether the controls are in fact monitored and controlled at regular intervals. Tests of essential configuration of technical platforms, databases, network equipment has been executed to ensure that controls are in fact implemented as stated; further evaluation of logging, backup, patch management, authorization, access controls, data management and inspection of equipment has also been included.
Observation	The execution of specific controls has been observed, and tests has been made to secure that the control has been implemented
Repetition/Execution	Controls has been repeated to find further proof/validation that the control works as expected

1. All datacenter and managed services customers have a contract

Control Target:

- To ensure that all new datacenter and managed services customers have an agreement that follows the latest version of the contract template

Control activity	Test executed by Aaen & Co	Result of test
All signed contracts are following the standard contract used for all customers, aligned with the security policy. No contracts are unsigned, where there are any committing obligations to SAC-IT	We have investigated the preparation of contracts for operation subscription customers, and have selected a random subsample to check whether these were prepared or not.	No significant deviations found

2. A security organization is in place

Control Target:

- To ensure that a security organization is in place, facilitating the revision of information security police and acting as a single point of contact for security breaches

Control activity	Test executed by Aaen & Co	Result of test
The security organization is in place as described. The controls that are the responsibility of the security officer is controlled/supervised by the CEO	We have inquired about guidelines and policies for IT security, and we have inspected documentation for the solution.	No significant deviations found

3. Controls are in place and covers sufficiently

Control Target:

- To ensure that controls are executed, are reviewed on a regular basis and works efficiently

Control activity	Test executed by Aaen & Co	Result of test
The Security officer facilitates the evaluation of the executed controls as part of the yearly review of the security policy. The evaluation is done with data center technicians, and the CEO on a dedicated meeting. New and more covering controls can be suggested if evaluated to be necessary.	We have inquired for preparation and handling of a controls checklist and we have inspected how this has been implemented.	We recommend quarterly documented audits. Apart from this no significant deviations found

4. Risk analysis is performed, and high prioritized risks are mitigated

Control Target:

- To ensure that a yearly risk assessment is performed to mitigate highly prioritized threats lowering the threat

Control activity	Test executed by Aaen & Co	Result of test
Management must be able to demonstrate a risk analysis and the mitigation of the prioritized risks.	We have inquired about a risk analysis and inspected documentation for this.	No significant deviations found

5. IT Security Policy is updated

Control Target:

- To ensure that the IT Security Policy is updated yearly and fit for purpose

Control activity	Test executed by Aaen & Co	Result of test
The Security officer facilitates a yearly process to gather new requirements or improvements to the existing policy. After this the Security Officer updates and publishes the updated security policy. Part of the input to changes are the Control evaluation and the risk assessment, to ensure that controls and risk mitigation is supported by the security policy If the security policy is changed, this leads to training/information being released to the organization	We have investigated the management of the IT security policy and we have inspected the procedures around this.	We have been informed that the IT Security Policy has been reviewed and updated. It is our recommendation that the yearly review is documented e.g. by ensuring proper version no. and date is applied. Apart from this, no significant deviations found.

6. Staff is trained in the security policy and its changes

Control Target:

- To ensure that the staff is informed about the security policy whenever it is changed

Control activity	Test executed by Aaen & Co	Result of test
The staff must be familiar with the IT security policy in a way that enables them to safe-keep customers assets; checked by: 1) Documenting the information/training effort 2) Asking staff control questions	We have inquired about the procedures and management of the information distribution and training in the IT security policy and we have inspected how this is handled.	We have noted, that all employees have received the company's security policy when hired and when major changes to the policy has occurred. However, it is our recommendation, that the policy is sent out on a regular basis going forward, to keep staff well informed. Apart from this, no significant deviations found.

7. Customer solutions are documented

Control Target:

- To ensure that information regarding individual customer solutions is created and updated when it has been changed

Control activity	Test executed by Aaen & Co	Result of test
The team leaders of the Service Desk and Operation checks and approves the customer documentation whenever it has been created and when new customers are being implemented. There are two values in this control: 1) New customers must be documented following a standard 2) If major changes have been done to a customer infra-structure it must be documented	We have made inquiries regarding customer solutions and we have inspected a sample of customers and their documentation. We have also made inquiries on the change management of customers and how this is documented.	No significant deviations found

8. All staff has signed a confidentiality agreement		
Control Target: • To ensure that customer and SAC-IT information is kept confidential.		
Control activity	**Test executed by Aaen & Co**	**Result of test**
The CEO updates the repository of confidentiality agreements whenever a new employee has signed a new agreement. If the CEO updates the template – all personnel must sign the new agreement again. A list of the employees of SAC-IT must match the list of signed confidentiality agreements.	We have made inquiries on proce-dures around staff confidentiality agreements, and we have checked a sample of these. Further to this, there has been no updates to the confidentiality agreement this year.	No significant deviations found

9. Employment contracts contains roles		
Control Target: • To ensure that customer and SAC-IT information is kept confidential, roles must be implemented in a way that ensures that roles are granted the right access to the datacenter		
Control activity	**Test executed by Aaen & Co**	**Result of test**
The CEO updates the repository of employment contracts whenever a new employee has signed a new agreement. All contracts must contain a role description matching the outlines in the security policy in order to ensure competences and access rights. Roles: a) Data center technician or similar Danish wording b) Data center technician with elevated rights – or similar Danish wording c) Team lead (for data center technicians) d) Non-data center technician e) Cloud Admin f) Cloud Helpdesk g) Support/Helpdesk	We have made inquiries regarding employment contracts and controlled a sample of these, to check the role descriptions	We found that roles described in contracts in some cases deviates from the roles described in access procedures.

10. Former employees do not have access to any systems		
Control Target: • To ensure that access to SAC-IT's customer information is accessible to only qualified staff.		
Control activity	**Test executed by Aaen & Co**	**Result of test**
It is checked that no former employee can access SAC-IT's core systems. This control is performed by ensuring that former employees are blocked from access and password is change in the VMWare datacenter Active Directory	We have made inquiries around the procedures and the management of former employee accesses, and we have inspected the working solution of this.	No significant deviations found

11. All employee PCs are protected by anti-malware

Control Target:

- To ensure that devices used to access customer infrastructure and data is safe guarded with updated anti malware protection

Control activity	Test executed by Aaen & Co	Result of test
The control is performed by selecting a couple of laptops belonging to employees.	We have made inquiries regarding how the employee's computers and mobile units are protected against malware and inspected how this has been implemented.	No significant deviations found

12. Only qualified technicians have access to the infrastructure

Control Target:

- To ensure that only qualified technicians operate the datacenter, and to ensure they are trained, have the right skills, tools and methods

Control activity	Test executed by Aaen & Co	Result of test
the access list to the datacenter is checked to ensure that only team members of the Service Desk & Operation team have access.	We have controlled the guidelines and procedures for granting system and data access for technicians and checked the documentation of this. Furthermore, we have made inquiries regarding a checklist for access rights and selected a sample to check for the correct access rights.	No significant deviations found

13. Physical access to the headquarter is protected

Control Target:

- Ensure that no one can enter the premises nor access an in logged laptop when no one is present at the office.

Control activity	Test executed by Aaen & Co	Result of test
Check that pause screens are activated and password protected after max 5 min of inactivity at all laptop equipment. Check that no one can enter the office unnoted. Check that doors are always locked when personnel are away	We have made inquiries regarding procedures for shutting off operation premises in Vedbæk. The procedures have been inspected and access to operational facility has been checked at a randomly selected sample.	No significant deviations found

14. Logical access, vendors

Control Target:

- Ensure that all vendor access is temporary and approved by SAC-IT and by the customer (in some cases)

Control activity	Test executed by Aaen & Co	Result of test
Check the VMWare Datacenter AD to ensure that non datacenter technician accesses are disabled	We have made inquiries on the system access policy, controlling access to systems and how it is implemented.	No significant deviations found

15. Administrative passwords are renewed on a regular basis

Control Target:

- To ensure that administrative passwords are strong and renewed on a regular basis

Control activity	Test executed by Aaen & Co	Result of test
Check that the administrative passwords are renewed as a minimum once a year and are strong, by the definition in the security policy	We have made inquiries to guidelines for management of administrative passwords and controlled the way it has been implemented.	No significant deviations found

16. Passwords to password management system

Control Target:

- To ensure that passwords to the password management system are extraordinary strong

Control activity	Test executed by Aaen & Co	Result of test
The Security Officer checks that the administrative password to the password management system is extraordinary strong by the definition of the security policy	We have made inquiries to guidelines for management of passwords to password management systems and controlled the way it has been implemented.	No significant deviations found

17. Check datacenter vendor policy quality

Control Target:

- To ensure that physical security in InterXion is sufficiently high

Control activity	Test executed by Aaen & Co	Result of test
Check that there is no deviation to procedures in InterXion and Fuzion by interviewing staff	We have made inquiries to the management regarding control of the physical access to the datacenter, and we have checked the way this is implemented, controlled and documented.	No significant deviations found

18. Check that customer backups can be restored

Control Target:

- The main purpose of backup is to be able to restore data. This must be checked on a regular basis

Control activity	Test executed by Aaen & Co	Result of test
Check a random selection of customers and their backup configuration to ensure that it is correct. Repeat a backup and a restore on a randomly picked customer server to ensure that a file can be backed up as well as restored.	We have made inquiries on the backup configuration of customer backups and based on randomly selected samples checked the documentation. We have checked the test of restore of backup files and the documentation of this.	No significant deviations found

19. Tickets have been prioritized correctly

Control Target:

- Ensure that tickets are prioritized correct.

Control activity	Test executed by Aaen & Co	Result of test
Check at a random day the list of tickets. Ensure that a random sample of tickets have been prioritized correctly	We have made inquiries into the procedure for prioritizing service tickets and checked the documen-tation on the implementation.	We recommend that procedures for handling tickets should be accessible both physical and digital. Apart from this no significant deviations found.

20. Tickets are processed in the correct way

Control Target:

- To ensure that highest prioritized tickets are worked at before lower prioritized ones

Control activity	Test executed by Aaen & Co	Result of test
Check by sample that service desk personnel are working on the correctly prioritized tickets	We have made inquiries regarding the guidelines and processing of service tickets, and we have observed the execution	We recommend that procedures for handling tickets should be accessible both physical and digital. Apart from this no significant deviations found.

21. Ensure that all critical systems are operatable by at least two persons

Control Target:

- Ensure to avoid key resource dependencies

Control activity	Test executed by Aaen & Co	Result of test
This is controlled by mapping the key competence areas and eliminate areas where there is only a single competent staff.	We have made inquiries on policy and guidelines on how to avoid key resource dependencies and how this is managed.	No significant deviations found

22. Monitors are monitored and reacted upon at frequent intervals during the day

Control Target:

- Ensure that alarms are reacted on swiftly to avoid down time

Control activity	Test executed by Aaen & Co	Result of test
Make sure that no servers are running out of capacity and monitor that services that should run is running	We have checked the procedures on daily monitoring and reaction on alarms from the system monitors and their implementation.	No significant deviations found

23. Check that major changes are listed in the Service Management System

Control Target:

- Major changes must follow a specific procedure to ensure customer downtime is avoided and to ensure the customers are in control and satisfied

Control activity	Test executed by Aaen & Co	Result of test
Ensure that procedure is followed. Major changes need to be logged and approved in the Service Management System	We have made inquiries to the policy and procedures for major change management on the customers solution. We have – based on samples - inspected the implementation, how it performs and the way it is documented.	No significant deviations found

24. Ensure that a set of capacity monitors on core infrastructure is in place

Control Target:

- To ensure that SAC-IT do not run out of capacity that takes long time to establish

Control activity	Test executed by Aaen & Co	Result of test
Make sure that there is enough physical capacity in the datacenter by establishing capacity monitors for the data storage, the VMWare CPU and RAM available resources and network bandwidth	We have made inquiries to the set of capacity monitors on core infrastructure set up to ensure sufficient capacity management is in place. We have inspected the Implementation of this and the performance.	No significant deviations found

25. All infrastructure and client equipment are protected with suitable malware protection

Control Target:

- To ensure that malware is not infecting infrastructure or client equipment

Control activity	Test executed by Aaen & Co	Result of test
Check that a sample of customer servers is having updated anti malware installed and running	We have checked the procedures and technical implementation of malware protection. We have made randomly selected samples to control the implementation and the documentation	No significant deviations found

26. Backup/restore process is in place and backup is in place on all infrastructure equipment		
Control Target: • To ensure that neither customers nor SAC-IT loose data by mishaps, breakdowns, malware attacks or data breaches		
Control activity	**Test executed by Aaen & Co**	**Result of test**
Ensure that backup jobs have been set up on a sample customer solution, and that the backup job is running. Ensure that a backed-up file can be restored.	We have made inquiries to procedures for backup/restores and inspected documentation for this.	No significant deviations found

Dette dokument er underskrevet af nedenstående parter, der med deres underskrift har bekræftet dokumentets indhold samt alle datoer i dokumentet.

This document is signed by the following parties with their signatures confirming the documents content and all dates in the document.

Jackie Amelung

Navnet returneret af dansk MitID var:
Jackie Nyberg Amelung
Direktør
ID: f221ba78-ae56-4e40-ae35-0b6f34082295
Tidspunkt for underskrift: 23-02-2024 kl.: 09:57:34
Underskrevet med MitID

Kenn Elmgren

Navnet returneret af dansk MitID var:
Kenn Erik Elmgren
Revisor
ID: b36c00e6-db47-42fb-9f50-3c12e11a6d68
Tidspunkt for underskrift: 23-02-2024 kl.: 10:02:06
Underskrevet med MitID