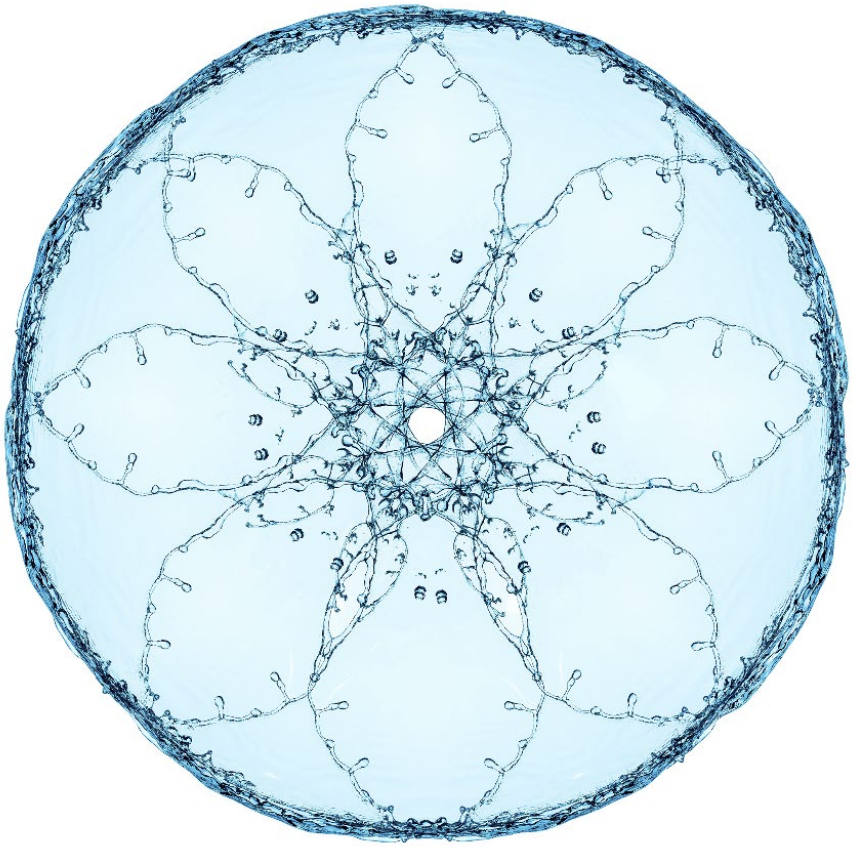
Deloitte
Statsautoriseret
Revisionspartnerselskab
CVR no. 33 96 35 56
Weidekampsgade 6
PO Box 1600
DK-0900 Copenhagen C

Phone: +45 36102030
Fax: +45 36102040
www.deloitte.dk



A/S ScanNet

ISAE 3402 type 2 Service Auditor's Report on general IT controls related to hosting services

Throughout the period from 01.01.2020 to 31.12.2020

Table of Contents

1 Independent Service Auditor's Report

Independent Service Auditor's Assurance Report on the Description of Controls, their Design, and Operating Effectiveness

To: the management at A/S ScanNet, A/S ScanNet's customers and their auditors

Scope

We have been engaged to report on A/S ScanNet's (hereinafter "ScanNet") description in section 3 "ScanNet's Description" of selected general IT controls related to the supplied hosting services throughout the period from 01.01.2020 to 31.12.2020 (the description), and on the design and operation of controls related to the control objectives stated in the description.

This auditor's report covers selected common general IT controls that are performed by ScanNet in the delivery of the agreed upon hosting services. Any specific agreements between clients and ScanNet that exceed the standard services delivered are not covered in this auditor's report.

ScanNet's system description does not include control objectives and associated controls at the subservice organisations. ScanNet uses the following sub-suppliers to deliver physical and environmental security of production environments and storage of backup.

- Fuzion A/S:
  - Housing
  - Physical and environmental security of production environment
- GlobalConnect A/S:
  - Housing
  - Physical and environmental security of production environment
- Cibicom A/S:
  - Housing
  - Physical and environmental security of production environment
  - Storage of backup.

Additionally, ScanNet uses the subservice provider, SentinelOne, for cloud storage and reporting logic for a subset of logging and monitoring on critical platforms.

This report is prepared using the carve-out method, and our testing does not include controls that are carried out by the subservice organisation.

Some of the control objectives noted in ScanNet's description of its system can only be achieved if the complementary controls at the user organisations are suitably designed and operating effectively together with the controls at ScanNet. The opinion does not include the suitability of the design and operating effectiveness of these complementary controls.

ScanNet's Responsibilities
ScanNet is responsible for: preparing the description and accompanying assertion in section 2, "Service Organisation's assertion", 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.

Service Auditor's Independence and Quality Control

We have complied with the requirements for independence and other ethical requirements in the IESBA's Code of Ethics for Professional Accountants, which is based on the fundamental principles of integrity, objectivity, professional competence and due care, confidentiality, and professional conduct.

Deloitte uses ISQC 1 and therefore maintains a comprehensive system for quality management, including documented policies and procedures for compliance with the Code of Ethics for Professional Accountants, professional standards, and applicable requirements according to the law and other regulations.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on ScanNet'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 International Standard on Assurance Engagements 3402, "*Assurance Reports on Controls at a Service Organisation*," 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, design, and operating effectiveness of controls at a service organisation involves performing procedures to obtain evidence about the disclosures in the service organisation's description of its system, and the design and operating effectiveness of controls. The procedures selected depend on the service auditor's 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 objectives stated therein, and the suitability of the criteria specified by the service organisation and described in section 2, "Service Organisation's assertion".

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

Limitations of Controls at a Service Organisation

ScanNet'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 organisation may not prevent or detect all errors or omissions in processing or reporting transactions. Also, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at a service organisation 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 selected general IT controls related to the hosting services provided by ScanNet as designed and implemented throughout the period from 01.01.2020 to 31.12.2020;
(b) The controls related to the control objectives stated in the description were suitably designed throughout the period from 01.01.2020 to 31.12.2020; and
(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 01.01.2020 to 31.12.2020.

Description of Tests of Controls

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

Intended Users and Purpose

This report and the description of tests of controls in section 4 are intended only for customers who have used ScanNet's standard hosting 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 assessing the risks of material misstatements of customers' financial statements.

Copenhagen, 26 February 2021

Deloitte
Statsautoriseret Revisionspartnerselskab
CVR-nr. 33 96 35 56

Thomas Kühn
Partner, state-authorised public accountant

Michael Bagger
Director, CISA

2 Service Organisation's Assertion

The accompanying description has been prepared for customers who have used the hosting services provided by ScanNet and their auditors, who have a sufficient understanding to consider the description along with other information, including information about controls operated by the customers themselves, when assessing the risks of material misstatements of customers' financial statements.
ScanNet confirms that:

a) The accompanying description in section 3 fairly presents the selected general IT controls related to the supplied hosting services provided by ScanNet throughout the period from 01.01.2020 to 31.12.2020. The criteria used in making this assertion were that the accompanying description:

i. Presents how the system was designed and implemented, including:

- The types of services provided, including, as appropriate, classes of transactions processed.
- The procedures, within both information technology and manual systems, by which those transactions were initiated, recorded, processed, corrected as necessary, and transferred to the reports prepared for customers.
- The related accounting records, supporting information and specific accounts that were used to initiate, record, process, and report transactions; this includes the correction of incorrect information and how information was transferred to the reports prepared for customers.
- How the system dealt with significant events and conditions, other than transactions.
- The process used to prepare reports for customers.
- Relevant control objectives and controls designed to achieve those objectives.
- Controls that we assumed, in the design of the system, would be implemented by user entities, and which, if necessary to achieve the control objectives stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved by ourselves alone.
- Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities, and monitoring controls that were relevant to processing and reporting customers' transactions.

ii. Includes relevant details of changes to the service organisation's system during the period from 01.01.2020 to 31.12.2020.

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 its own particular environment.

b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period from 01.01.2020 to 31.12.2020. The criteria used in making this assertion 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 from 01.01.2020 to 31.12.2020.

Skanderborg, 26 February 2021

ScanNet

Stefan Rosenlund
CEO

3 ScanNet's Description

3.1 Service provider system description

Introduction
This description is designed to provide information for the use of ScanNet clients and their auditors and to meet the requirements of audit standard ISAE 3402, "*Assurance Reports on Controls at a Service Organisation*".

The description is also prepared with the aim of providing information on the controls used in relation to the provision of hosting services and IT operating services provided by ScanNet.

Description of ScanNet's services
ScanNet develops, manages and delivers a range of professional hosting and cloud solutions for a wide range of companies and organisations in Denmark.

The scope of this audit statement covers the following services:
- Hosted Navision
- Hosted Desktop (Citrix)
- Hosted Exchange
- Mailhotel
- Webhotel
- Hosted Webshop
- Hosted CMS
- OnPay
- DNS Hotel and DNS servers' hosting domains
- Hosted Spam filter
- TSM Backup
- Veeam Backup.

Services not specifically mentioned above are not covered, but the infrastructure components (network, storage, management, operating systems) supporting the services are covered.

For the following products, only the infrastructure components (network, storage, management, hypervisor) are covered:

- Cloud Resource Pool (CRP)
- Virtual Data Centre (VDC)
- Cloud Server
- VPS Hosting

Microsoft Office 365 and Azure services are also not covered.

3.2 ScanNet's organisation and security

ScanNet operates an ISO 27001-certified Information Management System. Information Security is governed by the Security Board which sets the overall objectives of the ISMS. The Security Board consists of the following members:

- COO, Lotte Brandstrup
- CTO, Ole P. Jensen
- Chief Legal Officer, Bo Brandt Cramer
- CISO, Jakob Flink Schwartz.

The Head of Security (CISO) refers to the CEO.

The group meets quarterly and on an ad hoc basis to set and follow up on IT security objectives and risks.

Risk management at ScanNet
Risk management is implemented in ScanNet as an integral part of ScanNet's processes. A risk register is continuously maintained throughout the year, containing the most significant risks to ScanNet's operation of services. Risk treatment plans are defined and tracked for risks that fall outside our risk acceptance criteria. The risk register is reviewed at least annually and approved by the Security Board.

3.3 Control framework, control structure and control implementation criteria

ScanNet's IT security policy, established processes and controls include all systems and services offered to customers. The continued work on adapting and improving ScanNet's security measures is ongoing in cooperation with highly qualified specialists.

The criteria and scope of the control implementation at ScanNet were established in 2020 on the basis of the ISO 27001 and ISO 27002 standards. Based on this control framework, relevant control areas and control activities are implemented on the services provided by ScanNet.

The following essential control areas shall be included in the overall control environment:

- Information Security Policies (A.5.1)
- User Access Management (A.9.2)
- System and application access control (A.9.4)
- Operational procedures and responsibilities (A.12.1)
- Backup (A.12.3)
- Logging and monitoring (A.12.4)
- Technical vulnerability management (A.12.6)
- Supplier service delivery management (A.15.2)
- Information security aspects of business continuity management (A.17.1)

3.4 Established control environment

Each area is described in detail in the following sections.

Information security (A.5.1)

Objective
A management-approved information security policy is based on an IT risk analysis and is communicated to relevant employees in the company.

Procedures and controls used
ScanNet identifies relevant IT risks on established services to customers. This is done through an ongoing risk assessment at ScanNet. The risk assessment is approved annually by the Security Board.

Information security policy is available for all employees and communicated to all employees at least annually. Other material changes are communicated on an ad hoc basis.

Timing of the control
The IT risk analysis and IT security policy are reviewed at least annually. Information security policy is communicated annually.

Who performs the control?
The risk assessment and the annual review of policies are approved by the Security Board.

Control documentation

Information Security policy and risk assessment are versioned, and Security Board has approved. Minutes of Security Board meetings are kept.

User Access Management (A.9.2)

Objective
To ensure authorised user access and to prevent unauthorised access to systems and services.

Procedures and controls used
A formal process ensures new users are provisioned based on managers approval. Access rights are based on access profiles related to their job function.

A formal process ensures that users access rights are revoked, and users are disabled or de-registered on termination of employment or contract.

Privileged access rights are given on a need-to-use basis based on their functional roles.

A quarterly review of users ensures that any inactive users or users without work-related need for the privileges are removed.

Timing of the control
The user creation check occurs whenever ScanNet has a new employee. User de-registration is done when an employee is leaving ScanNet. Checks on inactive users and users with administrative rights are carried out quarterly.

Who performs the control?
The operations department of ScanNet is responsible for compliance with the access procedures.

Control documentation
Documentation on registration, de-registration and reviews of users are kept in ScanNet's internal ticketing system.

System and application access control (A.9.4)

Objective
To prevent unauthorised access to systems and applications.

Procedures and controls used
Access to ScanNet's assets happens through a secure logon process. Users are stored in a central user database. Password requirements and lock-out procedures are handled by internal Windows Active Directory. Password and lock-out settings are based on ScanNet's risk assessment.

All access from external or untrusted networks require MFA.

Timing of the control
User verification happens at logon.

Who performs the control?
ScanNet's internal Windows Active Directory.

Control documentation
Logins are logged. Group policies and MFA system configuration.

Operational procedures and responsibilities (A.12.1)

Objective
To ensure correct and secure operations of information processing facilities by: Ensuring that changes to systems are consistent and controlled.

Procedures and controls used
Changes to ScanNet's Operations Management System are controlled and documented through:

- Version control
- Code review
- Static code analysis.

Change management to systems follows a standardised process. Changes are documented in the internal ticketing system and communicated to customers. Changes must contain a description of impact for the customers, timeframe, and a description of affected services.

Timing of the control
When changes are planned or executed.

Who performs the control?
The person planning or executing the change.

Control documentation
Changes to Operations Management System is registered in Git and supporting systems.
Changes to systems are registered and communicated to customers via the internal change announcement system.

Configuration baseline (A.12.1)

Objective
To ensure correct and secure operations of information processing facilities by: Ensuring that customers' servers are deployed according to our security baseline.

Procedures and controls used
Customers' servers are deployed based on our configuration baseline. This includes requirements for automatic patching, firewall settings and password policy.

Configuration baselines is reviewed at least annually.

Timing of the control
When customers' servers are deployed. Review of baseline is performed annually.

Who performs the control?
Deployment is automated by the deployment system. Review is done via peer review.

Control documentation
Deployment is logged in the deployment system, and the peer review is documented in an internal ticket.

Capacity management (A.12.1)

Objective
To ensure correct and secure operations of information processing facilities by: Ensuring availability of systems and services.

Procedures and controls used
Servers are monitored for availability on predefined services based on the categorisation and the type of the server. Alerts are raised when service checks fails and handled by Operations staff. Repetitive alerts are escalated for further root cause analysis.

Timing of the control
Services are checked every five minutes. Summary of repetitive alerts is generated daily.

Who performs the control?
Monitoring system checks services. Repetitive alerts are checked by Operations staff.

Control documentation
Alerts are logged in Operations Management System.

Backup (A.12.3)

Objective
To protect against loss of data for systems within ScanNet's responsibility.

Scope
The scope of the report covers public systems providing services to customers where backup is included, i.e. Hosted Exchange, Webhotel, Hosted Desktop, Hosted Navision, VPS Server.

Internal systems providing services internally, i.e. corp. email, CMDB, Intranet, management systems

Out of scope:

- Services without backup included:
  - Virtual servers: Cloud Server, Cloud Resource Pool (CRP), Virtual Data Centre (VDC)
  - Backup services provided where the customer manages the backup jobs and monitors backup jobs
  - Restore testing – We guarantee the integrity of our backup systems, but only the customer can test if their backup is valid.

Procedures and controls used
For "public systems providing services to customers", we guarantee backup of data with 14 days retention and recovery point objective of 24 hours, if there is no disruption to the backup job.

For "Internal systems providing services internally", we guarantee backup so they can be recovered again.

Backups are always stored in a different data centre than where production data is stored. Backup data is replicated to another data centre site daily.

Integrity of backup systems is continuously insured by restore jobs internally and by customers.

We continuously test our restore capabilities by restoring internal systems and customer systems. Customers can ad-hoc order restore tests of their specific systems.

There is an automated procedure for daily follow-ups on failed backup jobs. If a backup job fails consecutively two days in a row, a ticket is raised. If a backup job fails three times over a period of 14 days, a ticket is raised.

Timing of the control
Automatic backup has been established and restore tests are carried out at least once a year.

Who performs the control?
The operations department is responsible for the day-to-day control of backup logs.

Control documentation
Backup log is stored in ScanNet's asset management system.

Logging (A.12.4)

Objective
To record events and generate evidence.

Procedures and controls used
Events from critical systems are logged to central log management platform.

Extended Detection and Response (XDR) platform logs and ships events off site for protection. XDR platform monitors for malicious behaviour. Alerts are raised to Operations staff for investigation.

Timing of the control
Continuously.

Who performs the control?
Operations team investigates events raised.

Control documentation
Logs stored in log management platform and events are stored in the XDR platform.

Technical vulnerability management (A.12.6)

Objective
To prevent exploitation of technical vulnerabilities through patch management.

Procedures and controls used
For operating systems Windows and Linux servers, security patches are installed continuously throughout the year, and exceptions are documented.

For hypervisors, security patches are evaluated by system owner and installed appropriately.

For hardware devices, security patches are evaluated by system owner and installed appropriately.

Timing of the control
The update check is automated through the respective patch platforms.

Who performs the control?
The operations department is responsible for carrying out updates and checking them.

Control documentation
Documented in the patch management platform. On each server, a list of patches installed is available. Evaluated patches are documented in tickets.

Supplier services delivery management (A.15.2)

Objective
To maintain an agreed level of information security and service delivery in line with supplier agreements.

Procedures and controls used
Conduct review of independent auditor's reports, if available, and assess issues identified.
Conduct physical inspection of supplier services in data centres.

Timing of the control
The review of the supplier's audit reports and the review of supplier's services are performed annually.

Who performs the control?
CISO and Infrastructure

Control documentation
Documented review of supplier audit reports is stored in the internal documentation system.
Documented review of supplier services is stored in the internal ticketing system.

Business continuity planning and testing (A.17.1)

Objective
Planning for resuming business and services after any type of major incident.

Procedures and controls used
ScanNet has established a contingency plan, which generally sets out guidelines on how to deal with any type of emergency situation. The contingency plan is approved annually by ScanNet's management.

The contingency plan shall be reviewed on an ongoing basis and at least once a year.

Timing of the control
The contingency plan shall be reviewed and approved annually.

Who performs the control?
The Information Security department is to review, and management is to approve.

Control documentation
The contingency plan is versioned. There is evidence of actions taken in connection with the 'dry run' of the contingency plan.

3.5 Additional information on the established control environment and conditions to be observed by client auditors (complementary controls)

Service delivery
The controls described in ScanNet's system description is based on ScanNet's standard terms. As a result, customer agreements which differ from ScanNet's standard terms are not covered by the scope of this auditor's report. Customers and their auditors should assess whether the control scope in this auditor's report can be used in assessing the general IT controls at ScanNet in relation to operations and hosting services provided from ScanNet to the customer. Customers and their auditors should also themselves identify any other material risks related to their environment.

User Management
ScanNet provides access and assigns access privileges in accordance with customer instructions as they are registered through the Service Desk or Control Panels. ScanNet is not responsible for the accuracy of information about users, and it is therefore the responsibility of customers to ensure that accesses and rights to systems and applications are allocated in accordance with the customers' own expectations for

appropriate user management, including segregation of duties and periodic reassessment in the system environments hosted and operated by ScanNet. If desired, the customer can create users on the individual servers themselves – controls related to this process are the responsibilities of the customers'.

Logical security configuration
ScanNet has configured logical security on its own infrastructure for providing operating and hosting services to its customers. Establishing and configuring logical security in customers' own environments are the responsibilities of the customers, and it is the responsibility of the customers to verify that these security configurations are consistent with the desired level of security.

Logging
Logging inside the customers' environments is the responsibility of the customers. Thus, each customer should ensure appropriate controls for configuration and monitoring of logs.

Backup
It is the customer's own responsibility to ensure that backup is set up according to the customer's own needs. Recovery of customer data from backup systems is only tested when a specific agreement has been reached with the customer or if ScanNet receives a request from the customer with a specific request. According to ScanNet's procedures, it is subsequently the customer's responsibility to ensure that completed restore can be used as intended in the respective environments.

Contingency planning
ScanNet has set up general contingency planning that includes ScanNet's own infrastructure. Customers should therefore independently assess whether additional procedures or contingency plans need to be implemented, including verification thereof.

Compliance with relevant legislation
ScanNet is not responsible for applications that are run on the hosted equipment. It is therefore the responsibility of customers to establish reassuring controls in the applications, including that they support compliance with the Danish Accounting Act, the Personal Data Act, the Financial Business Act and/or other relevant legislation.

4 ScanNet's Control Objectives and Related Controls, and Deloitte's Tests of Controls and Results of Tests

4.1 Introduction

This report is intended to provide ScanNet's customers with information about the controls at ScanNet that may affect the processing of user organisations' transactions and also to provide ScanNet's customers with information about the operating effectiveness of the controls that were tested.

This report, when combined with an understanding and assessment of the controls at user organisations, is intended to assist user auditors in (1) planning the audit of user organisations' financial statements and in (2) assessing control risk for assertions in user organisations' financial statements that may be affected by controls at ScanNet.

Our testing of ScanNet's controls was restricted to the control objectives and related controls listed in the matrices in this section of the report and was not extended to controls described in the system description but not included in the aforementioned matrices, or to controls that may be in effect at user organisations. It is each user auditor's responsibility to evaluate this information in relation to the controls in place at each user organisation. If certain complementary controls are not in place at user organisations, ScanNet's controls may not compensate for such weaknesses.

ScanNet's system description does not include control objectives and associated controls at the subservice organisation. ScanNet uses the following sub-suppliers to deliver physical and environmental security of production environments and storage of backup.

- Fuzion A/S:
  - Housing
  - Physical and environmental security of production environment
- GlobalConnect A/S:
  - Housing
  - Physical and environmental security of production environment
- Cibicom A/S:
  - Housing
  - Physical and environmental security of production environment
  - Storage of backup.

Additionally, ScanNet uses the subservice provider, SentinelOne, for cloud storage and reporting logic for a subset of logging and monitoring on critical platforms.

The customers' own auditors should gain assurance through inspection of auditor's reports from the subservice organisations to collectively assess whether all relevant controls have been covered considering their clients' control environments as a whole.

4.2 Test of Controls

The test of controls performed consists of one or more of the following methods:

Method	Description
Inquiry	Interview, i.e., inquiry with selected personnel at ScanNet.
Observation	Observation of the execution of control
Inspection	Review and evaluation of policies, procedures, and documentation concerning the performance of the control. This includes reading and evaluating reports and other documentation to assess whether specific controls are designed and implemented. Furthermore, it is assessed whether controls are monitored and supervised adequately and at appropriate intervals.

Re-performance of control	Repetition of the relevant control to verify that the control functions as intended

4.3 Test of Operating Effectiveness

Our test of the operating effectiveness of controls includes such tests as we consider necessary to evaluate whether those controls performed, and the extent of compliance with them, were sufficient to provide reasonable, but not absolute, assurance that the specific control objectives were achieved throughout the period from 01.01.2020 to 31.12.2020.

Our test of the operating effectiveness of controls was designed to cover a representative number of transactions throughout the period from 01.01.2020 to 31.12.2020 for each of the controls listed in this section, which are designed to achieve the specific control objectives.

4.4 Control Objectives, Controls and Test Results

4.4.1 Information Security Policies (A.5.1)

Objective: A management-approved information security policy is based on an IT risk analysis and is communicated to relevant employees in the company.

ID	Control specified by ScanNet	Control performed by Deloitte	Conclusion
A.5.1.1 *Policies for information security*	Information security policies are documented and communicated to employees.	Deloitte inspected that the information security policy and selected sub-policies are documented, and available on Confluence. Deloitte inspected that the updated employee information security policy, has been communicated to employees via the intranet.	No deviations noted.
A.5.1.2 *Review of the policies for information security*	Information security policies are reviewed and approved at least annually.	Deloitte inspected that the information security policy was reviewed and approved in November 2020.	No deviations noted.
A.5.2.1 *IT Risk Analysis*	Information security risk assessment of critical risks to ScanNet operations of infrastructure is documented, reviewed at least annually, and approved.	Deloitte inspected the IT risk analysis and verified that it was updated in the audit period. Deloitte verified that the IT risk analysis had been approved by the security board.	No deviations noted.

4.4.2 User Access Management (A.9.2)

Objective: To ensure authorised user access and to prevent unauthorised access to systems and services.

ID	Control specified by ScanNet	Control performed by Deloitte	Conclusion
A.9.2.2 *User-access provisioning*	Internal users at ScanNet is created according to formal creation procedures based on request from manager. All internal users are created in the Windows domain with a personal user account.	Deloitte inspected that an Access Management Policy is covering requirements for user access creation and has been reviewed in 2020. Deloitte inspected, on a sample basis, that user creations are based on a ticket, and that the creation is requested and approved by a manager.	We noted, for one sample, that no formal ticket was in place for the creation of the users admin profile. Vi have been informed that user's manager confirms that access is approved. No further deviations noted.
A.9.2.3 *Management of privileged access rights*	Privileged access rights are limited to employees at ScanNet with a work-related need.	Deloitte inspected the list of users with privileged access on the two internal Windows domains, and per inquiry with key personnel verified that only users with a work-related need have access.	No deviations noted.
A.9.2.5 *Review of user access rights*	Periodic review of users with privileged access rights is performed, and inactive users as well as users without a work-related need for the access are removed.	Deloitte inspected, on a sample basis, that users with privileged access rights in the two Windows domains are reviewed in the audit period, and users without a work-related need for the access are removed.	We noted that the available documentation for the performed review does not clearly denote the conclusion of the review. Via review of the user lists. We have confirmed with management that access is approved and work-related. No further deviations noted.
A.9.2.6 *Removal or adjustment of access rights*	Internal users are disabled prior to or on the termination date of the employees. Furthermore, ScanNet performs an assessment of whether relevant passwords should be changed. This is documented via the ticketing system.	Deloitte inspected, on a sample basis, that terminated users accounts are disabled according to the procedure.	No deviations noted.

4.4.3 System and application access control (A.9.4)

Objective: To prevent unauthorised access to systems and applications.

ID	Control specified by ScanNet	Control performed by Deloitte	Conclusion
A.9.4.2 *Secure logon procedures*	Access to ScanNet's network goes through secure logon in Windows Active Directory, where password is configured according to the formalised password policy. MFA is required for access from external networks.	Deloitte inspected the configuration of the password policy on the two internal Windows domains and verified whether it corresponded to the management-approved password policy. Deloitte observed, on a sample basis, employees being validated through MFA.	No deviations noted.

4.4.4 Operational procedures and responsibilities (A.12.1)

Objective: To ensure correct and secure operations of information processing facilities by: Ensuring that changes to systems are consistent and controlled; ensuring that customers' servers are deployed according to our security baseline; and ensuring availability of systems and services.

ID	Control specified by ScanNet	Control performed by Deloitte	Conclusion
A.12.1.2a *Change Management*	Changes to ScanNet's Operations Management System is controlled and documented through: • Version control • Code review • Static code analysis	Deloitte inspected the change management procedure and verified with key personnel that the process was valid in the audit period. Deloitte verified, for one sample, that the system functionality supports version control as a standard. Deloitte inspected, for selected change samples, that Code review and Static code analysis are performed according to ScanNet's requirements.	We have noted, for 4 out of 25 samples for changes, that no documentation for double approval on code changes is available. We were informed that the process was changed in august 2020, and following this change, the double approval is mandated by the system. No further deviations noted.
A.12.1.2b *Planned changes*	Planned changes are documented according to a standardised process that ensures that maintenance announcements are made with the required information. All maintenance announcements are processed and approved by the CTO.	Deloitte inquired on the process for changes, and verified that the process is system-supported, to ensure that required information for maintenance announcements is specified. Deloitte inspected, for selected samples, that all required information is noted on the maintenance announcement and that they are processed and approved by the CTO.	No deviations noted.
A.12.1.2c *Configuration baseline – Review*	A yearly review of the configuration baseline is performed, and the review is approved by the line manager.	Deloitte inspected documentation for the performed review of the configuration baseline, and verified that the review was performed, peer reviewed and approved by the line manager.	No deviations noted.
A.12.1.2d *Configuration baseline – Control*	New Windows servers that are created are configured in compliance with actual baselines that have been defined in a number of scripts. This baseline contains specific requirements for password and patching	Deloitte inquired with key personnel on the procedure for creating a new VPS server with a Windows operating system. Deloitte observed whether a newly created Windows server is in compliance with the baseline.	No deviations noted.

ID	Control specified by ScanNet	Control performed by Deloitte	Conclusion
A.12.1.3 *Capacity management*	All servers are automatically monitored for availability via the central monitoring tool. Alerts are pushed to the monitoring screens placed in the operations department.	Deloitte inspected, for a sample of servers, that availability monitoring is configured, and verified whether deviations in availability are registered, and any outages are handled. Deloitte observed that monitoring screens are placed in the operations department and verified with key personnel that alerts are monitored.	No deviations noted.

4.4.5 Backup (A.12.3)

Objective: To protect against loss of data for systems within ScanNet's responsibility.

ID	Control specified by ScanNet	Control performed by Deloitte	Conclusion
A.12.3.1a *Information backup – configuration*	All ScanNet services with backup included are stored for at least 14 days. Backup runs daily and reoccurring errors result in a ticket for Operations staff.	Deloitte inspected, for selected server samples, that backup retention is set to at least 14 days. Deloitte inspected, for selected server samples, that backup is performed on a daily basis, and for backup errors inspected that errors are resulting in a ticket that is handled according to the procedure.	We have noted that tickets for handling backup errors are generated after three consecutive failed backups. Thus, not within the timeframe of two consecutive failed backup as per specification in the backup procedure. We have been informed that this has been resolved. Furthermore, we have noted for 2 out of 24 sampled servers that backup, for the one server, was missed three days in May and for the other server, backup was missed two days in June. No further deviations noted.
A.12.3.1c *Information backup – locations*	Backup is stored off site away from any production system.	Deloitte inspected for selected server samples that back-ups are stored on different sites than production servers.	No deviations noted.

4.4.6 Logging and monitoring (A.12.4)

Objective: To record events and generate evidence.

ID	Control specified by ScanNet	Control performed by Deloitte	Conclusion
A.12.4.1 *Event logging*	Event logging is configured for ScanNet's critical, central systems.	Deloitte inspected, on a sample basis, that event logging is configured on two internal Windows domain controllers. Deloitte inspected whether the same two internal Windows domain controllers were also covered by SentinelOne logging.	No deviations noted.
A.12.4.2 *Protection of log information*	ScanNet's central critical logs are stored at external party and cannot be altered.	Deloitte inspected, on a sample basis, that logs from two internal Windows domain controllers were transferred to the log management tool. Deloitte inquired with key personnel whether logs from server samples, Windows Domain Controllers and Operations Management System are protected from deletion and manipulation.	We have been informed that a limited group of server administrators have access to delete logs on servers and in the log management tool. We have been informed that some log events are stored in the SentinelOne log tool, where logs are protected from deletion. No further deviations noted.
A.12.4.3 *Administrator and operator logs*	System administrator and system operator activities shall be logged in the Operations Management System.	Deloitte inspected that a password access log from the Operations Management System to document the use of the shared administrator-users is available. Deloitte inspected, on a sample basis, whether user access logs are stored on local servers for a limited time period.	No deviations noted.

4.4.7 Technical vulnerability management (A.12.6)

Objective: To prevent exploitation of technical vulnerabilities through patch management.

ID	Control specified by ScanNet	Control performed by Deloitte	Conclusion
A.12.6.1 *Management of technical vulnerabilities*	For operating systems, security patches for Windows and Linux servers are installed continuously throughout the year, and exceptions are documented. For hypervisors, security patches are evaluated by system owner and installed appropriately.	Deloitte verified, on a sample basis, that Linux and Windows servers had been updated throughout the audit period. Deloitte verified, on a sample basis, the ESXi patch level and verified via inquiry with key personnel that the patch level is in accordance with the patch policy.	We noted that five sampled Windows servers had not been patched consistently throughout 2020. For three of these servers, the missing patches are caused by the Operating system End Of Life. We have been informed by ScanNet that migration projects are initiated. No further deviations noted.

4.4.8 Supplier service delivery management (A.15.2)

Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.

ID	Control specified by ScanNet	Control performed by Deloitte	Conclusion
A.15.2.1 *Monitoring and review of supplier services*	ScanNet performs an annual review of independent auditor's reports for critical sub-suppliers, if available, and assess issues identified. ScanNet performs an annual physical inspection of supplier services in data centres, and the results are document in the ticketing tool.	Deloitte inspected documentation showing that review of independent auditor's reports for critical sub-suppliers is performed and the results are documented on confluence. Deloitte inspected, on a sample basis, that annual physical inspection of supplier services in data centres was performed and documented in the ticketing tool.	No deviation noted.

4.4.9 Information security aspects of business continuity management (A.17.1)

Objective: Planning for resuming business and services after any type of major incident.

ID	Control specified by ScanNet	Control performed by Deloitte	Conclusion
A.17.1.2 *Implementing information security continuity*	A business continuity plan is documented, reviewed, and annually approved by management.	Deloitte inspected that a business continuity plan is documented, and that it consist of an overall business continuity plan and a backup policy. Deloitte inspected that the business continuity plan has been reviewed and approved annually by the management in 2020.	No deviations noted.
A.17.1.3 *Verify, review and evaluate information security continuity*	Business continuity tests are conducted at least annually. There is evidence of actions taken in connection with the 'dry run' of the contingency plan.	Deloitte inspected playbook and meeting notes from the latest business continuity test, and that the test has been approved by the Security Board.	No deviations noted.