

Nianet A/S

ISAE 3402 Type 2 Report

Report on general IT controls and the effectiveness thereof for the service co- location/housing for the period from 16 June 2017 to 7 June 2018

Table of contents

1	Independent auditor's report	2
2	Statement by Nianet	4
3	Systems description by Nianet	5
3.1	Introduction	5
3.2	Control environment, risk assessment and monitoring	6
3.2.1	Responsibility, Nianet's Board of Directors and Executive Board	6
3.3	Risk management	6
3.4	Emergency preparedness	7
3.5	Security	8
3.6	User control – consideration for customers	9
4	Information distributed by Deloitte	10
4.1	Introduction	10
4.2	Testing of effectiveness	10
4.3	Security, control objectives and control activities	11
4.3.1	A.5.1. Information security policies (ISO 27001)	11
4.3.2	A.6.1. Internal organisation (ISO 27001)	12
4.3.3	A.7.1. Before hiring (ISO 27001)	15
4.3.4	A.7.2. During the employment period (ISO 27001)	15
4.3.5	A.9.1 Business related requirements of access management (ISO 27001)	16
4.3.6	A.9.2 Administration of user access rights (ISO 27001)	17
4.3.7	A.11.1 Physical security (ISO 27001)	20
4.3.8	A.16.1 Management of information security incidents and improvements (ISO 27001)	23
4.3.9	A.17.1 Information security continuity (ISO 27001)	24
5	Supplementary information provided by Nianet	25

1 Independent auditor's report

To the management of Nianet A/S

Scope

We have been asked to report on Nianet A/S' (hereinafter "Nianet") description in section 3 of the handling of the general IT controls for the service co-location/housing, including the design, implementation and effectiveness of controls as regards the control objectives referred to in the description.

The description and, accordingly, our report only deal with shared processes, controls involved in those processes and the security baselines generally applicable to Nianet's customers. This report does not cover customers with specific process- and security requirements.

Information presented in section 5 *Supplementary information provided by Nianet*, has not been subjected to the procedures applied in the examination of the description and of the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description of the system and, accordingly, we express no opinion on it.

Nianet's responsibility

Nianet is responsible for the preparation of the description and the appertaining statement by Management as provided in section 2, including the completeness and accuracy of those documents as well as the method under which the description and the statement are presented, the provision of the services included in the description includes, for stating the control objectives and for the design, implementation and effectively operating controls to achieve the stated control objectives.

Auditor's responsibility

Based on our procedures, our responsibility is to express an opinion on Nianet's description as well as on the design, implementation and effectiveness of controls related to the control objectives stated in this description. We have conducted our work in accordance with the Danish version of the International Standard on Assurance Engagements (ISAE) 3402 issued by FSR – Danish Auditors. This Standard requires that we plan and perform our procedures to obtain reasonable assurance that the description gives a fair presentation in all material respects and that the controls have been appropriately designed and operate effectively.

We have complied with the independence and other ethical requirements of the Code of Ethics issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

Deloitte applies the International Standard on Quality Control (ISQC) 1 and, accordingly, maintains a comprehensive quality control system, including documented policies and procedures for ensuring compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

An assurance engagement to report on the description, design and effectiveness of controls at Nianet involves performing procedures to obtain evidence about the disclosures in Nianet's description of its system, and the design and effectiveness of controls. The procedures selected depend on the auditor's judgment, including the assessment of the risks that the description is not fairly presented, and that the controls are not suitably designed or operating effectively. Our procedures involved testing the effectiveness of controls we consider necessary to provide reasonable assurance that the control objectives stated in the description had been achieved. An assurance engagement of this type also involves evaluating the overall presentation of the description, the suitability of the objectives stated therein, and the suitability of the criteria specified by Nianet in sections 2 and 3.

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

Due to their nature, controls at a service organisation do not prevent or detect all errors or omissions in the processing or reporting of transactions. Also, the projection of the systems description and the opinion 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,

- 1) the description of Nianet's services and control environment as designed and implemented during the period from 16 June 2017 to 7 June 2018 is adequate, in all material respects;
- 2) the controls related to the control objectives stated in the description had been appropriately designed during the period from 16 June 2017 to 7 June 2018;
- 3) the controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved in all material respects, operated effectively throughout the entire period from 16 June 2017 to 7 June 2018.

The opinion above does not cover customer-specific process and security requirements as specified in the customised service level agreement, nor does it cover compliance with specific requirements of the European General Data Protection Regulation (GDPR). Should Nianet's customers request a report on customer-specific matters, this would require the conclusion of an agreement with Nianet for the issuing of customer-specific reports.

Description of the testing of controls

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

Intended users and purpose

This report and the description of the test of controls in section 4 are intended solely for Nianet and its customers and their auditors, who have a sufficient understanding thereof to consider the contents of the report in addition to other information, including information about controls operated by the customers themselves, when assessing the risk of material misstatement of financial statements.

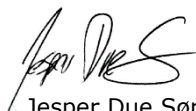
Copenhagen, 27 June 2018

Deloitte

Statsautoriseret Revisionspartnerselskab
CVR No. 33 96 35 56



Thomas Kühn
State-Authorised Public Accountant



Jesper Due Sørensen
Partner, CISA

2 Statement by Nianet

The description provided in section 3 is intended for those of Nianet's customers who have used Nianet as their co-location/housing services provider and their auditors, who have sufficient knowledge to consider the description in addition to other information, including information about controls performed by the customers themselves when assessing the risks of material misstatement of their financial statements.

Nianet confirms that:


- (a) The description provided in section 3 is an adequate description of Nianet's operating services as provided to the customers during the period from 16 June 2017 to 7 June 2018. The criteria for this statement were that the accompanying description:
- (I) explains how the system has been designed and implemented, and specifies:
 - the types of services provided.
 - procedures governing the use of IT, including procedures intended to ensure the confidentiality, integrity and accessibility of systems and data;
 - procedure applied for preparing reports and other information for customers;
 - relevant control objectives and controls designed to achieve those objectives;
 - controls that we, with reference to the system's design, have assumed would have been implemented by the customers of Nianet and which, if necessary to achieve the control objectives stated in the description, are identified in the description along with the specific control objectives;
 - 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 the processing and reporting of operating services provided to Nianet's customers;
 - (II) contains relevant information about changes in Nianet's system made in the period from 16 June 2017 to 7 June 2018;
 - (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 particular environment;
- (b) the controls related to the control objectives listed in the accompanying description were appropriately designed and operated effectively throughout the period from 16 June 2017 to 7 June 2018. The criteria for this statement were that:
- (I) the risks that threaten achievement of the control objectives stated in the description had been identified;
 - (II) the controls identified would, if operated as described, provide reasonable assurance that those risks do not prevent the stated control objectives from being achieved;
 - (III) the controls were consistently applied as designed, and manual controls were applied by individuals who have the appropriate competence and authority throughout the period from 16 June 2017 to 7 June 2018.

Glostrup, 27 June 2017

Nianet A/S



Christian Holm Christensen
CEO



Per Skovgaard Rosen
CTO

3 Systems description by Nianet

3.1 Introduction

This description has been prepared for the purpose of providing information to be used by Nianet's customers and their auditors and meeting the requirements of ISAE 3402 assurance reports on controls at a service organisation. Also, the description was drawn up for the purpose of providing information about the controls applied in Nianet's provision of co-location/housing services.

Scope

The description provides information about the controls applied in relation to the physical security of services provided by Nianet. The description includes physical security provided by Nianet and focuses on control objectives relevant to the internal controls that relate to financial reporting by Nianet's customers. The description covers the business processes, which Nianet deems important to their customers from an accounting point of view as well as supporting general IT controls. Nianet's Management is responsible for identifying control objectives and for the manual and automated controls implemented with a view to achieving those objectives. This includes the information technology and infrastructure supported by Nianet's operational organisation.

The description has been prepared with a view to cover most of Nianet's customers. Therefore, focus will be on the processes and controls that are used in the common processes. Specific customer relations and controls related to specific regulatory requirements concerning the processing of personal data (General Data Protection Regulation) are not covered by this description.

Description of Nianet

Nianet is an IT operations provider (information and communication technology) focusing on fibre-based data communication solutions for public sector and private sector businesses. Nianet is among the largest providers in the Danish market. Via many thousand kilometres of fibre, Nianet covers all of Denmark and owns fibre for more than 3,500 unique addresses. Nianet was founded in May 2003 and is owned by 13 Danish energy companies based across the country.

IT services

Nianet provides data communication solutions, co-location and cloud solutions.

Our services include:

- MPLS VPN
- Internet traffic
- Managed LAN
- Black and grey fibre
- DSL connections
- International connections
- Co-location/Housing
- Private Cloud, Virtual Server and Backup as a Service (BaaS)
- Hosted Firewall and nextgen firewall
- Anti-DDoS solutions
- Hardware and software VPN.

However, this description only includes the control aspects relating to physical protection, risk management and emergency preparedness, and it seeks to comply with ISO27001 for the service co-location/Housing.

Standards

The generic information and control criteria provided below were applied in drawing up the general systems and control description to assess whether the controls had been appropriately designed and whether the controls are operating effectively. These criteria are inspired by the international control standard ISO/IEC 27001 (Information security) and based on the Danish Act on network and information security and the four Executive Orders that regulate the Act on network and information security as well as the business-related requirements relative to the services offered by Nianet, including:

- Physical and logical protection
- Risk management
- Emergency preparedness.

3.2 Control environment, risk assessment and monitoring

Nianet's control environment reflects Management's assessment of the importance of controls and the importance attached to controls relative to policies, procedures, methods and organisational structure. The following list is a description of Nianet's control environment and Nianet's provision of IT services:

- Responsibility, Nianet's Executive Board and Board of Directors
- Nianet's organisational structure
- Risk management.

3.2.1 Responsibility, Nianet's Board of Directors and Executive Board

Nianet is owned by 13 Danish energy companies, which have elected a Board of Directors, the composition of which is as follows:

- Chairman - Rune Nygaard Bech Pedersen
- Six rank and file Board members
- Four staff-elected members.

Nianet's Board of Directors convenes once every quarter at a minimum to discuss:

- Business plans and business strategy
- Financial results
- Observations and recommendations
- Findings of an external audit, where relevant.

Nianet's Executive Board is ultimately responsible for ensuring compliance with Nianet's business policies. The Executive Board convenes on a weekly basis to discuss certain strategic presentations and any matter of a tactical or operational nature, general policies and general processes – in other words, ordinary management activities at a company experiencing solid growth with 120 employees.

Nianet's Executive Board is composed as follows:

CEO – Rasmus Helmich
 CFO – Søren Fæster Nielsen
 Sales Director and Marketing Director – Peter Sandahl Torp
 CDO – Mette Slesvig
 CTO - Per Skovgaard Rosen.

Nianet is headquartered in Glostrup, and has an office in Skanderborg, Denmark, and five data centres in the Danish cities of Glostrup, Taastrup, Vallensbæk, Skanderborg and Århus, respectively.

3.3 Risk management

Risk assessment

Management convenes regularly to discuss business risks, including financial and technological risks. In addition, all managers regularly have meetings with the employees to discuss any outstanding issues relating to the team's work.

Nianet's security organisation carries out annual risk assessments of Nianet's assets on the basis of ISO/IEC 27005. The model used for assessing risks involves an assessment of consequence, probability and vulnerability. The process takes into account both external and internal factors and threats in addition to Management's ability to focus on those factors' impact on operations.

The risk assessment contains a specification of risk owners, management assessment and risk management.

IT security policy and protection plans

An IT security policy and protection plans have been formulated based on the risk assessment and the vulnerability analysis. The IT security policy and the relevant protection plans were formulated to mitigate the risks identified.

The protection plans include plans intended to ensure that the vulnerability of particularly critical elements of the company's infrastructure, including data centres and major POPs (Point-Of-Presence), is low. The protection plans are tested against the defined and approved test plan. The IT security policy and protection plans are reassessed annually in connection with the annual risk assessment and the results of the test plans.

External suppliers

Based on the Danish Act on network and information security, Nianet requires that all of its sub-suppliers comply with the requirements of this Act. Nianet has drawn up a formal agreement specifying the compliance requirements. All suppliers are required to sign the agreement.

Monitoring and communication

Nianet monitors and records any IT security and personal data security breach through a formally documented incident management process. All incidents are recorded and documented in a case management system. Recording and documentation of incidents is saved indefinitely in the system and through backup.

When an incident occurs, including personal data security breaches and identification of special threats, end users and government agencies are informed thereof through the incident management process pursuant to relevant executive orders subject to the Danish Act on network and information security. Through this process, all high-priority incidents are reported to the CTO, who is responsible for informing the end users, the customers and the public authorities of such incidents and for reporting the incidents to them.

Injunctions and information issued by the government agencies are monitored by Nianet through a single point of contact for communication with the relevant public authority and the CTO.

3.4 Emergency preparedness

Contingency and crisis management plans

Based on annual risk assessments, Nianet has formulated and adopted an emergency policy and contingency plans to ensure compliance with Danish Executive Orders Nos. 564 and 567. The contingency plans and the emergency policy ensure protection of all areas specified in Executive Orders and the risk assessment performed. Nianet has formulated contingency plans to deal with any physical damage to all important locations and a crisis management plan governing all major incidents, including serious threats, in accordance with Danish Executive Order No. 567.

The contingency plans are reassessed annually in connection with the risk assessment.

Emergency drills

Based on the requirements of Danish Executive Order No. 567 (35), Nianet has prepared a five-year test plan involving emergency testing of all important elements of the company's emergency preparedness. The test plan is reassessed annually when reassessing the contingency plans.

Monitoring and communication

Nianet monitors and records any IT security breaches, including emergency incidents and crisis management, through a formally documented incident management process. All incidents are recorded and documented in a case management system. Recording and documentation of incidents is saved indefinitely in the system and through backup.

When an incident occurs, end users and government agencies are informed thereof through an incident management process in accordance with Danish Executive Order No. 566 (Executive Order on information and notification duties concerning network and information security). Through this process, all high-priority incidents are reported to the CTO, who is responsible for informing the end users, the customers and the public authorities of such incidents and for reporting the incidents to them.

Injunctions and information issued by public authorities are monitored by Nianet through a single point of contact for communication with the relevant government agency and the CTO.

3.5 Security

Business processes as well as written work and control descriptions are in place for important and critical areas relating to physical and logical security.

Security, physical access

Nianet A/S has formal policies and procedures in place regarding control of access to systems, facilities and data centres. These policies and procedures define the levels of access allowed in accordance with the classification of employees and describe the measures and authority necessary for gaining and monitoring access.

Access control management

Data centre entrances have been secured by electronic access card readers, which are connected to a centrally based computer. Access to data centres is managed by Nianet's Network Operations Centre (NOC) on the basis of job descriptions. In order to prepare and hand out access cards, the customer must provide details about the level of access requested accompanied by a proper permit. Personal access cards with related personal passwords are issued. External users with access to data centres only have access to their personal locked rack cabinets or areas defined for them.

Administration of user access to systems and data

A formal procedure for assigning user access rights has been prepared with a view to granting or revoking user access rights of all user types for all systems and data. Furthermore, the IT security handbook describes the requirements of Nianet's employees in relation to access rights. The users are only granted access to the network(s) and network services that they are specifically authorised to use. Upon termination of employment, the user's access rights to systems and data are revoked.

Surveillance

The data centre entrances are equipped with alarms and are under video surveillance. The video activities are transferred to a centrally based server. The security guards look into activated entrance alarms. The security guards confront any unauthorised or suspicious person attempting to gain access outside normal office hours. In addition, any access to data centres is under surveillance, meaning that controlled/authorised access is ensured. Where necessary, external technicians, who are to maintain the equipment at the data centres, will be escorted by Nianet employees.

Physical security measures

The data centres are built according to Uptime Tier2 or Tier3 definitions. The datacentres are supplied by the local electricity distributor and through stand-by generators and via a redundant UPS system, which ensures a stable supply of electricity in case of public supply failure. When the public supply of electrical power fails, generators (usually 500-1000 kVA diesel generators) automatically start and ensure continued electrical power supply. The generators are tested on a quarterly basis, and the UPS system is tested regularly – both solutions are tested in accordance with the protection plan.

The cooling of rack cabinets at the data centres is done beneath raised floors. The cooling system ensures that cool filtered air is "shoved" through the rack cabinets from beneath. Generally, cubes are being used in Nianet's data centres for blowing cold air into "cold corridors" while hot air from the equipment is blown into the adjoining rooms from which a cooling unit absorbs the heated air and burns the calories in outdoor units via cooling water. All areas and rack cabinets have a maximum temperature of 25°C and a maximum air humidity of 60%.

Facilities used for the storage of equipment are constructed from fire-resistant material. The data centres are protected by Agronite and Inergen units, which are connected to the fire alarm system. Optical and ionised smoke detectors installed in the ceiling and beneath the raised floors in the rooms have been connected to the system. These detectors constantly monitor the areas and serve as audio-visual alarms.

When two or more alarms go off, the extinguishing system is activated in the room concerned. At the same time, the alert is sent to the fire authorities.

The area is under video surveillance, and all activities are logged.

The data centres have been certified under S40.

3.6 User control – consideration for customers

Nianet's controls have been designed based on the assumption that certain internal controls are in place at the customers/users. The implementation of such internal controls is necessary for achieving the control objectives outlined in section 4. The users may have additional control objectives and related controls which may be appropriate in terms of transactions and which have not been included in this description.

This section outlines certain controls that have been implemented at the supplier's users in order to achieve the control objectives stated in the description. The control considerations stated below should not be seen as an exhaustive list of controls to be operated by the users:

Access control: The customer is personally responsible for establishing controls, which ensures that its users are created and revoked in accordance with the procedures for restricting unauthorised access adopted by it. The control should involve taking measures, which ensure periodic reviews of users' access with a view to ensuring that access remains appropriate, given the users' respective responsibilities as well as security requirements.

4 Information distributed by Deloitte

4.1 Introduction

This description has been prepared to inform Nianet's customers of the systems and controls in place, which may impact on the treatment of business-related transactions and informing the customers of the effectiveness of the controls tested. When combined with an understanding and assessment of the controls implemented in the company's business processes, this section is intended to help the auditors of Nianet's customers to (1) plan the audit of the financial statements and (2) assess the risk of material misstatement in the financial statements, which may be affected by the controls at Nianet.

Our test of Nianet's controls is limited to the control objectives and related controls, which are evident from the control matrix provided below in this section of the report, and has not been extended to all the controls stated in Nianet's systems description, or to the controls that may have been implemented at the user organisations. Every customer auditor is responsible for evaluating this information in relation to the controls existing at the user organisation.

Overall control environment

In addition to the test of the effectiveness of controls as referred to in the control matrix in this section of the report, we have tested Nianet's overall control environment, including risk management.

Our testing of the control environment involved making inquiries of relevant members of Management, supervisors and employees as well as examining Nianet's documents and recordings. The control environment has been assessed with a view to determining the nature, timing and scope of the effectiveness of controls.

4.2 Testing of effectiveness

Our testing of the effectiveness of controls includes the tests we consider necessary to assess whether the controls performed and the observance of those controls are sufficient to provide reasonable but not absolute assurance that the control objectives specified had been achieved in the period from 16 June 2017 to 7 June 2018. Our test of the effectiveness of controls was designed to cover a representative number of transactions during the period from 16 June 2017 to 7 June 2018 for every control, see below, designed to achieve the specific control objectives. In selecting specific tests, we considered (a) the nature of the areas tested, (b) the types of available documentation, (c) the nature of audit objectives to be achieved, (d) the control risk level assessed and (e) the estimated effectiveness of the test.

4.3 Security, control objectives and control activities

4.3.1 A.5.1. Information security policies (ISO 27001)

	Control activities	Customers' control considerations	Test plan	Test results
Control objective: To provide guidelines and support information security in accordance with business-related requirements and relevant laws and regulations. <i>DS/ISO IEC 27002:2013</i>				
A.5.1.1	<i>Information security policies</i> Management must establish and approve a set of information security policies to be published and communicated to employees and relevant external parties.	None	Through inquiry and inspection, we have noted that a management-approved IT security policy is available, and that it is available on the Intranet. Furthermore, we have checked that the IT security policy is reviewed annually to ensure adequacy.	No material comments

	Control activities	Customers' control considerations	Test plan	Test results
A.5.1.2	<p><i>Review of the information security policies</i></p> <p>The information security policies must be reviewed at planned intervals, or when significant changes occur to ensure their continued suitability, adequacy and effectiveness in terms of results.</p>	None	Cf. A.5.1.1	No material comments
A.5.1.3	<p><i>IT Risk Analysis</i></p> <p>An executive- and management-approved IT risk analysis has been prepared in SecureAware. The risk analysis includes the risk of loss of availability, integrity and confidentiality.</p>	None	Through inquiry and inspection, we have noted that the IT risk analysis had been prepared and approved by the management.	No material comments
A.5.1.4	<p><i>Review of the IT risk analysis</i></p> <p>The IT risk analysis must be reviewed at planned intervals, or when significant changes occur.</p> <p>On a monthly basis, changes to the IT risk are discussed on the change boards.</p>	None	Through inquiry and inspection, we have noted that the IT risk analysis was up-to-date and approved in 2018. Further, we noted that change boards were held on a monthly basis.	No material comments

4.3.2 A.6.1. Internal organisation (ISO 27001)

	Control activity	Customer's control considerations	Test plan	Test results
Control objective: To establish a management basis for initiating and managing the implementation and operations of information security in the organisation. <i>DS/ISO IEC 27002:2013</i>				
A.6.1.1	<p><i>Roles and areas of responsibility for information security</i></p> <p>Control: All areas of responsibility for information security must be defined and distributed.</p>	None	<p>Through inquiry and inspection, we have noted that a formal IT security organisation is in place.</p> <p>Furthermore, we have noted that it</p>	No material comments

	Control activity	Customer's control considerations	Test plan	Test results
			defines the organisation's responsibilities and describes the various member roles.	
A.6.1.2	<p><i>Segregation of duties</i></p> <p>Control: Conflicting functions and areas of responsibility must be segregated in order to reduce the risk of unauthorised or unintended use, change or misuse of the organisation's assets.</p>	None	Through inquiry and inspection, we have noted that a process for segregation of duties had been established. These processes require that the immediate manager completes a form where the physical and system access rights of the individual employees are defined.	No material comments
A.6.1.3	<p><i>Contact with authorities</i></p> <p>Control: Appropriate contact must be kept with relevant authorities.</p>	None	Through inquiry and inspection, we have noted that contact to the cyber security project unit had been established.	No material comments
A.6.1.4	<p><i>Contact to special interest groups.</i></p> <p>Control: Appropriate contact with special interest groups or other professional security forums and professional organisations must be maintained.</p>	None	Cf. A.6.1.3	No material comments
A.6.1.5	<p><i>Information security in connection with project management.</i></p> <p>Control: Information security must be applied in connection with project management, regardless of project type.</p>	None	<p>Through inquiry and inspection, we have noted that a formal change management process had been established.</p> <p>Based on completed network changes made in the audit period, we have checked, on a sample basis, that the change management process was followed.</p>	<p>One out of 25 samples did not have a formal approval.</p> <p>One out of 25 samples did not have a formal test plan or a fall-back strategy.</p> <p>No further comments.</p>

4.3.3 A.7.1. Before hiring (ISO 27001)

	Control activity	Customers' control considerations	Test plan	Test results
Control objective: To ensure that employees and contracting parties are familiar with their responsibilities and are suitable for the roles for which they are being considered. <i>DS/ISO IEC 27002:2013</i>				
A.7.1.1	<p><i>Screening</i></p> <p>Control: Background verification checks on all job candidates must be carried out in accordance with relevant laws, regulations and ethical requirements and must be proportional to the business requirements, the classification of the information to which access is granted and relevant risks.</p>	None	Based on the new hires made in the audit period, we have noted through inspection and on a sample basis that security clearance had been obtained from the Danish Probation Service (Kriminalforsorgen) and the Danish Defence Intelligence Service (Forsvarets Efterretningstjeneste).	No material comments
A.7.1.2	<p><i>Terms and conditions of employment</i></p> <p>Control: Contracts with employees and contracting parties must specify their information security responsibilities and those of the organisation.</p>	None	Based on the new hires made in the audit period, we have noted through inspection and on a sample basis that information security responsibilities are specified in contracts in addition to confidentiality.	No material comments

4.3.4 A.7.2. During the employment period (ISO 27001)

	Control activity	Customers' control considerations	Test plan	Test results
Control objective: To ensure that employees and contracting parties are aware of and fulfil their information security responsibilities. <i>DS/ISO IEC 27002:2013</i>				
A.7.2.1	<p><i>Management responsibility</i></p> <p>Control: Management must require that all employees and contracting parties maintain information security in accordance with the policies and procedures established at the organisation.</p>	None	Per inquiry of Management, we noted that they are aware of their information security responsibilities. Based on the new hires made in the audit period, we have noted through inspection and on a sample basis that the IT Security	<p>We have noted that 4 out of 25 samples on external clients gaining access to Nianet locations did not return a signed confidentiality requirement.</p> <p>No further comments</p>

	Control activity	Customers' control considerations	Test plan	Test results
			Handbook was distributed to Nianet employees and contracting parties on employment.	
A.7.2.2	<p><i>Awareness of and education and training in information security.</i></p> <p>Control: All employees of the organisation and, where relevant, contracting parties must be made aware of security through education and training and they must be regularly updated on the organisation's policies and procedures to the extent relevant to their job functions.</p>	None	<p>Based on the hiring made in the audit period, we have noted through inspection and on a sample basis that new employees have signed a statement saying that they are familiar with the IT security policy.</p> <p>Furthermore, we have noted that annual awareness exercises are carried out. Finally, we have checked that the IT security policy is available on the Intranet.</p>	No material comments
A.7.2.3	<p><i>Sanctions</i></p> <p>Control: A formal sanction process communicated to the employees must be in place to enable the organisation to take action against employees who have breached information security.</p>	None	We have obtained the information security policy and found that it specifies matters relating to sanctions.	<p>We were informed that, during the period, there were no observations or events calling for sanctions of the nature referred to.</p> <p>No further comments</p>

4.3.5 A.9.1 Business related requirements of access management (ISO 27001)

	Control activity	Customers' control considerations	Test plan	Test results
Control objective: To prevent unauthorised publication, change, removal or destruction of information stored on media. <i>DS/ISO IEC 27002:2013</i>				
A.9.1.1	<p><i>Access management policy</i></p> <p>Control: An access management policy must be drawn up, documented and</p>	None	Through inquiry and inspection, we have noted that the IT security handbook describes the requirements for Nianet's employees in	No material comments

	Control activity	Customers' control considerations	Test plan	Test results
	reviewed on the basis of business and information security requirements.		relation to access, including creation, identification and access.	
A.9.1.2	<i>Access to network and network services</i> Control: Users are only given access to the networks and network services that they are specifically authorised to use.	None	Through inquiry and inspection, we have noted that the IT security handbook defines guidelines for the use of VPN connections and open networks.	No material comments

4.3.6 A.9.2 Administration of user access rights (ISO 27001)

	Control activity	Customers' control considerations	Test plan	Test results
Control objective: To ensure access for authorised users and prevent unauthorised access to systems and services. <i>DS/ISO IEC 27002:2013</i>				
A.9.2.1	<i>User registration and deregistration</i> Control: An access management policy must be established, documented and reviewed on the basis of business and information security requirements.	None	Through inquiry and inspection, we have noted that a procedure for registration and deregistration of user access rights is in place.	No material comments
A.9.2.2	<i>Assigning user access rights</i> Control: A formal procedure for assigning user access rights must be implemented with a view to assigning or revoking access rights for all user types and for all systems and services.	None	Based on the hiring made in the audit period, we have noted through inspection and on a sample basis that access rights granted are formally approved and that the access management procedure had been followed.	No material comments

	Control activity	Customers' control considerations	Test plan	Test results
A.9.2.3	<p><i>Managing privileged access rights</i></p> <p>Control: The allocation and use of privileged access rights must be limited and managed.</p>	None	Based on the hiring made in the audit period, we have noted through inspection and on a sample basis that the allocation of privileged access rights had been formally approved and followed the access management procedure.	<p>We have noted that two newly hires in the IT staff function were given domain administrator rights. However, we have not been able to obtain formal approvals from their immediate managers.</p> <p>No further comments</p>
A.9.2.4	<p><i>Managing secret authentication information about users</i></p> <p>Control: The allocation of secret authentication information must be managed by means of a formal administration process.</p>	None	<p>Through inquiry and inspection, we have noted that Nianet has a formalised process in relation to the processing of sensitive data.</p> <p>Furthermore, based on the hiring made in the audit period, we have checked, on a sample basis, that employees are screened prior to employment.</p>	No material comments
A.9.2.5	<p><i>Review of user access rights</i></p> <p>Control: Asset owners must review the users' access rights regularly.</p>	None	<p>Through inquiry and inspection, we have inspected the access management procedure, including the guidelines for periodic review of allocated rights and access to systems.</p> <p>Furthermore, we have verified, on a sample basis, that Nianet has performed a periodic review of the allocated rights and access to systems.</p>	No material comments
A.9.2.6	<p><i>Revoking or adjusting access rights</i></p> <p>The access rights to information and</p>	None	Based on the resignations in the audit period, we have noted through inspection and on a	No material comments

	Control activity	Customers' control considerations	Test plan	Test results
	information processing facilities of employees and external users must be revoked upon termination of their employment, contract or agreement or adjustments thereof.		sample basis that the system access rights of resigned employees had been revoked.	

4.3.7 A.11.1 Physical security (ISO 27001)

	Control security	Customers' control considerations	Test plan	Test results
Control objective A.11.1: To prevent unauthorised physical access and damage to as well as interruption of the organisation's information and information processing facilities. DS/ISO IEC 27002:2013				
A.11.1.1	Physical perimeter security Control: Perimeter security must be defined and perimeter security measures must be taken to protect areas with either sensitive or critical information as well as information facilities.	None	Through inquiry and inspection, we have noted that the data centres have video surveillance, access control, locked rack cabinets, water and humidity detectors as well as raised floors are in place. Furthermore, we have inspected the AIA alarm systems and access hatchway.	No material comments
A.11.1.2 Internal staff	Physical access control (internal staff) Control: Secured areas must be protected through adequate access control to ensure access for authorised staff only	None	Based on access granted/access changes in the period under review, we have verified through inspection and on a sample basis that access granted during the period had been properly approved.	No material comments
A.11.1.2 External staff	Physical access control (external parties) Control: Secured areas must be protected through adequate access control to ensure access for authorised staff only.	None	Based on access rights granted to external parties / access changes in the period under review, we have verified through inspection and on a sample basis that access granted during the period had been properly approved.	No material comments

Control security		Customers' control considerations	Test plan	Test results
A.11.1.3	<p>Protection of offices, rooms and facilities</p> <p>Control: The physical protection of offices, rooms and facilities must be planned and established.</p>	None	<p>As for the data centres, we have verified through inspection that video surveillance, access control, locked rack cabinets, water and humidity detectors and raised floors are in place.</p> <p>Based on access rights granted to external parties/access changes in the period under review, we have verified through inspection and on a sample basis that key tags had been duly approved and distributed.</p>	No material comments

	Control security	Customers' control considerations	Test plan	Test results
A.11.1.4	<p>Protection against external and environmental threats</p> <p>Control: Physical protection against natural disasters, malicious attacks or accidents must be planned and established.</p>	None	<p>Through inquiry and inspection, we have noted that the following devices were installed:</p> <p>1) Redundant UPS and diesel generators</p> <p>2) Fire-fighting equipment and fire alarms and smoke detectors</p> <p>3) Air-conditioning systems and the CTS system for automatic monitoring of the climate system, and checked that the CTS system automatically creates alerts in NOC.</p> <p>Also, we have checked whether the UPS system and the diesel generators, the fire-fighting equipment and the air-conditioning systems have been subject to periodic service checks.</p>	No material comments
A.11.1.5	<p>Working in safe areas</p> <p>Control: Procedures for working in safe areas must be planned and established.</p>	None	<p>Through inquiry and inspection, we have noted that procedures for granting access to Nianet's data centres had been established, and we have checked, on a sample basis, that when access to the data centres was granted, the grantee had given his/her signature to confirm that he/she had read the procedures for granting access to Nianet's data centres.</p>	No material comments
	Control security	Customers' control considerations	Test plan	Test results

A.11.1.6	<p>Areas for loading and offloading</p> <p>Control: Access areas such as areas for loading and offloading and other areas from where unauthorised persons may access the area must be managed and, to the extent possible, be kept separate from the information processing facilities to prevent unauthorised access.</p>	None	Through inquiry and inspection, we have noted that areas for loading and offloading are separate from the rest of the data centre. We have also inspected AIA alarm systems and access hatchway.	No material comments
----------	--	------	--	----------------------

4.3.8 A.16.1 Management of information security incidents and improvements (ISO 27001)

	Control activity	Customers' control considerations	Test plan	Test results
Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses. DS/ISO IEC 27002:2013.				
A.16.1.1	<p><i>Incident management</i></p> <p>Information security events shall be assessed, and it shall be decided whether they are to be classified as information security incidents.</p>	None	<p>We have inspected the procedure for handling events concerning breach of information security.</p> <p>Furthermore, we have inspected incidents and inquired whether there have been any with exceptional risk in the audit period.</p>	<p>We have concluded that 6 of 25 incident samples are not prioritised in the ticket system.</p> <p>1 of 25 samples is categorised as medium priority; however, according to the incident management policy, it should have been categorised as high.</p> <p>No further comments</p>
A.16.1.2	<p><i>Incident management – communication</i></p> <p>Information security events shall be reported through appropriate management channels as quickly as possible.</p> <p>The CTO is responsible for reporting all security events of high criticality to regulatory authorities and effected customers.</p>	None	<p>We have inspected the procedure for handling events concerning breach of information security.</p> <p>Furthermore, we have inspected incidents and inquired whether there have been any with an exceptional risk in the audit period.</p>	<p>See remark for A.16.1.1</p> <p>No further comments</p>

4.3.9 A.17.1 Information security continuity (ISO 27001)

	Control security	Customers' control considerations	Test plan	Test results
Objective: Information security continuity shall be embedded in the organisation's business continuity management systems. DS/ISO IEC 27002:2014				
A.17.1.1	<p><i>Planning of information security continuity</i></p> <p>Nianet has determined its requirements for information security, and the continuity of information security management and Network circuits are prioritised for adverse situations, e.g. during crises or disaster.</p>	None	We have inspected the network monitoring system and found that the system contains information about line ID, capacity and fiber cable termination. Furthermore, we found that Nianet has a priority list which indicates the most vital circuits with the highest priority.	No material comments
A.17.1.2	<p><i>Implementing information security continuity</i></p> <p>Nianet has established, documented, implemented and maintains processes, procedures and controls to ensure the required level of continuity for information security in adverse situations.</p>	None	Through inquiry and inspection, we have noted that Nianet has established a contingency plan that is based on the risk analysis. We have verified that the contingency plan takes into account that Nianet can maintain the provision of networks and services in emergency situations and in other extraordinary situations.	No material comments
A.17.1.3	<p><i>Verify, review and evaluate information security continuity</i></p> <p>Annually, Nianet verifies the established and implemented information security controls. A five-year rotation plan ensures that relevant parts of the information security continuity are tested during this period.</p>	None	We have inspected the 5-year test plan for emergency preparedness exercises and obtained documentation for the preparedness test in the declaration period.	No material comments

5 Supplementary information provided by Nianet

The information included in section 5 of this report is presented by Nianet to provide additional information and is not a part of the Service Organisation's description of the system made available to user entities. The information included here in section 5 has not been subjected to the to the procedures applied in the examination of the description and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the system and, accordingly, Deloitte expresses no opinion on it.

As to the observation in A.6.1.5 *Information security in connection with project management.*

Management's responsibility:

- Nianet has emphasised the Change Management procedure in the organisation, and regular efforts are made to strengthen the internal processes and controls in this area.

As to the observation in A.7.2.1 *Management's responsibility:*

- Nianet has emphasised the procedure relating to confidentiality agreements, security clearance etc. of supplier staff. Regular efforts are made to strengthen the internal processes and controls in this area.

As to the observation in A.9.2.3 *Managing privileged access rights:*

- As part of the employment process, the two employees' immediate superior has approved their Domain Admin rights, following which the approval procedure was specified within the organisation. The IT management of Nianet has provided supplementary information that those two employees are employed as systems administrators and therefore have a clear work-related need for Domain Admin rights.

As to the observation in A.16.1.1 *Incident Management:*

- Nianet has emphasised the Incident Management procedure in the organisation, and regular efforts are made to strengthen the internal processes and controls in this area.