NOVEMBER 2017

LINK MOBILITY A/S

ISAE 3402 TYPE 2 ASSURANCE REPORT

Independent auditor's report on general IT controls in relation to the operation of SMS service.

Beierholm
Statsautoriseret Revisionspartnerselskab
Knud Højgaards Vej 9
2860 Søborg
CVR-nr. 32 89 54 68
Tlf +45 39 16 76 00

www.beierholm.dk

BEIERHOLM
VI SKABER BALANCE

Structure of the assurance report

Chapter 1:
LINK Mobility A/S' Letter of Representation.

Chapter 2:
LINK Mobility A/S' description of general IT controls for the operation of SMS service.

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

Chapter 4:
Auditor's description of control objectives, security measures, tests and findings.

CHAPTER 1:

LINK Mobility A/S' Letter of Representation

This description in Chapter 2 of LINK Mobility A/S' general IT controls has been prepared for customers, who have used or plan to use LINK Mobility SMS service, and their auditors, who have sufficient understanding to consider the description, along with other information, including information about controls operated by customers themselves, when assessing the risks of material misstatement in their financial statements. LINK Mobility A/S hereby confirms that

(A) The description in Chapter 2 gives a true and fair description of LINK Mobility SMS service's general IT controls throughout the period 1 June 2016 - 31 October 2017. The criteria for this assertion are that this description:

(i) gives an account of, how the controls were designed and implemented, including:
- the types of services delivered, when relevant
- the processes in both IT and manual systems that are used to manage the general IT controls
- relevant control objectives and control procedures designed to achieve these goals
- control procedures that we have assumed – with reference to the system's design – would be implemented by LINK Mobility A/S and which, if necessary to fulfil the control objectives mentioned in the description, have been identified in the description together with the specific control objectives that we cannot fulfil ourselves
- other aspects of our control environment, risk assessment process, information system and communication, control activities and monitoring controls that have been relevant for the general IT controls

(ii) includes relevant information about changes in LINK Mobility A/S' general IT controls made during the period 1 June 2016 - 31 October 2017

(iii) does not omit or misrepresent information that is relevant for the scope of the controls described, taking into consideration that the description has been prepared to meet the common needs of a broad range of customers and their auditors, and may not, therefore, include every aspect of the system that each individual customer may consider important in their 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 1 June 2016 to 31 October 2017. The criteria for this assertion are that:

(i) The risks that threatened the fulfilment of the control objectives mentioned in the description were identified

(ii) The identified controls would, if used as described, provide reasonable assurance that the risks in question would not prevent the fulfilment of these control objectives, and

(iii) The controls were applied consistently as designed, including that manual controls were performed by persons with adequate competences and authority throughout the period 1 June 2016 - 31 October 2017.

(C) the accompanying description and the related criteria for fulfilling the control objectives and controls, Chapter 2, have been prepared based on compliance with LINK Mobility A/S' standard agreement, the basis for SMS service and services regarding the general IT controls. The criteria for this basis were:

(i) IT-sikkerhedspolitik version 2016/03/23

(ii) Service Level Agreement for SMS-service version1

Kolding, 14 November 2017

Mikkel Robin Nielsen
Adm. direktør

Christian Møller Hjelmager
Driftschef/ COO

CHAPTER 2:

LINK Mobility A/S' description of general IT controls related to SMS service operations

Introduction

The purpose of the present description is to inform LINK Mobility A/S' customers and their auditors of the requirements of ISAE 3402, which is the international standard for Assurance Reports on Controls at a Service Organisation.

Moreover, the description provides information on the controls applied to the operation of LINK Mobility A/S' SMS services for the period 1 June 2016 - 31 October 2017.

Description of LINK Mobility A/S and LINK Mobile A/S

Today eight employees are employed by LINK Mobility A/S, and in addition employees from LINK Mobility ASA, Oslo are connected to LINK Mobility A/S.

LINK Mobility is a SMS aggregator providing tools to send and receive SMS text messages primarily for the Danish market.

Scope of present description

LINK Mobility A/S is a service provider in the information technology field. LINK Mobility A/S' core activity concerns the delivery and reception of SMS text messages for the Danish telecom networks as well as the operation of the related platform, but the company also has major coverage abroad. In the present document, these activities are collectively referred to as SMS services.

Monitoring and support services are performed centrally from the office, and operations are located in floor-rent facilities at GlobalConnect.

As a provider, and in order to conform to the requirements set out in the agreements that govern its activities, LINK Mobility A/S is responsible for establishing and maintaining appropriate procedures and controls for the purpose of identifying and preventing errors. It is precisely this core activity—SMS handling and maintenance of same—that forms the basis for the present description.

Business/IT security strategy

LINK Mobility A/S' strategy is to incorporate sufficient security measures into its business ensuring that the company is not exposed to unacceptable risks.

LINK Mobility A/S applies the following general strategic reference points:

- We want to secure the confidential data our customers transmit through the LINK Mobility Group;
- We want to deliver a product that has the best possible uptime and accessibility;
- We want to give our customers a product that is market-leading;
- We want to ensure that our employees' knowledge is relevant and up-to-date;
- We want to make our objectives common across the entire organisation.

LINK Mobility A/S is working with IT security at a business-strategic level and is therefore making a continuous effort to secure high service and quality levels. In the company's security policy, Management emphasises that IT security is and must be an important part of the company's business culture.

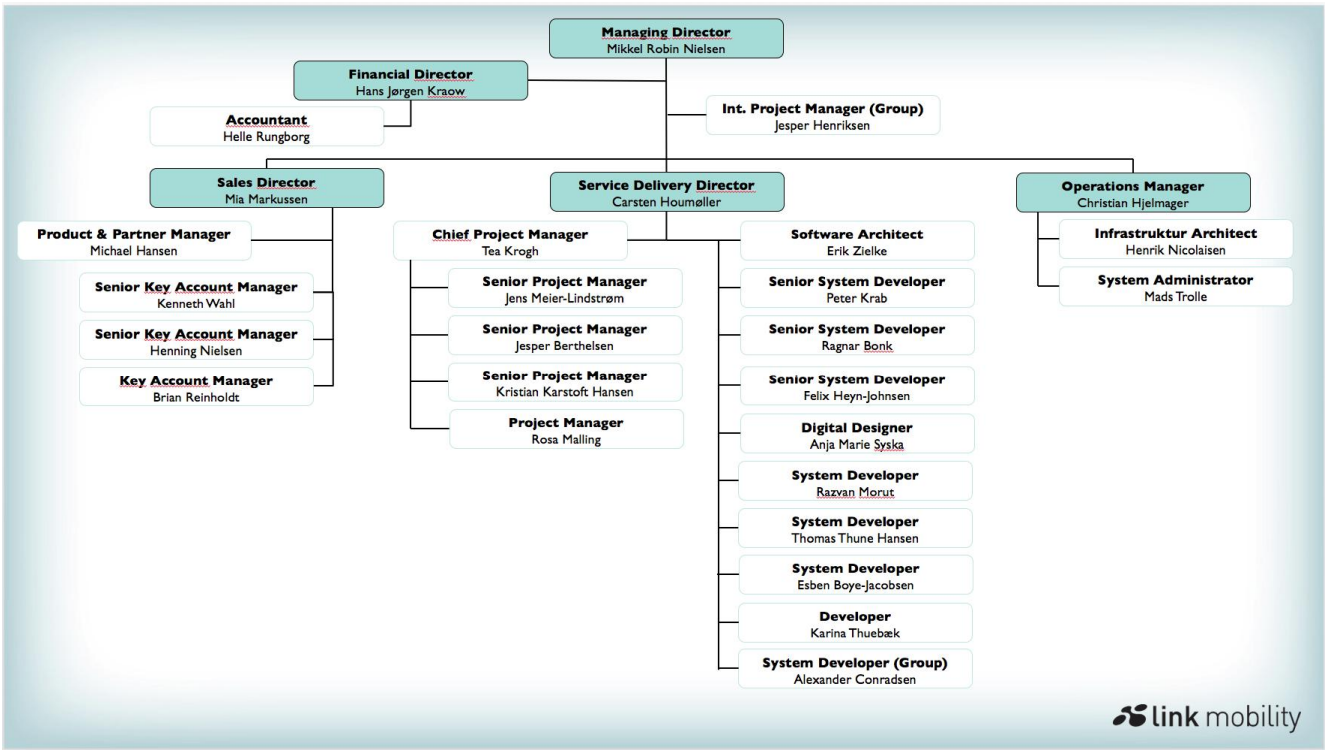
LINK Mobility is basing its IT security strategy on ISO27002:2013 and is thus applying the ISO methodology to implement relevant security measures within the following areas:

- Information security policies;
- Organisation of information security;
- Human resource security;
- Asset management;
- Access control;
- Physical and environmental security;
- Operations security;
- Communication security;
- Supplier security;
- Information security incident management;
- Information security aspects of business;
- continuity management

The security measures implemented at LINK Mobility A/S are set out in Appendix 1 of this description.

LINK Mobility A/S's organisation and IT security structure

LINK Mobility A/S has eight employees and a flat organisational structure. The company is managed on a daily basis by Adm. direktør Mikkel Robin Nielsen, who also holds overall responsibility for IT security. driftschef/COO Christian Møller Hjelmager is responsible for performing audit as well as for control and updating of relevant procedures.



Risk management at LINK Mobility A/S

LINK Mobility A/S' policy is for the risks related to the company's activities to be covered or limited to such an extent that the company will have the capacity to maintain normal operations. LINK Mobility A/S performs risk management and internal controls across several areas and at various levels. The company performs continuous risk and threat assessments.

LINK Mobility A/S has incorporated regular procedures to perform risk assessments of its business. This allows us to ensure that risks associated with the services provided by us are minimised to an acceptable level. Risk assessments are performed periodically and as changes are made to existing systems, or when new systems subject to assessment are implemented. The risk assessment is part of the IT security manager's responsibility and will subsequently be accepted and approved by the company's Management.

As part of the above-mentioned IT security strategy, LINK Mobility A/S is applying ISO27002:2013, which is the international standard for IT security, as its primary framework for IT security. The IT security work process is a continuous and dynamic process designed to ensure that LINK Mobility A/S lives up to its customers' requirements and needs at all times.

IT security management

Management has detailed LINK Mobility A/S' IT security structure in its central IT security policy. The IT security policy is revised at least once a year.

LINK Mobility A/S' general objective is to provide stable and secure SMS services to its customers based on the SLA as it applies at all times. In order to support this effort, policies and procedures have been introduced that ensure that our deliveries are consistent and transparent.

LINK Mobility A/S' IT security policy has been prepared with reference to the above and applies to all employees and all deliveries. In the event of errors and security breaches in our operation environment, the error/breach will be remedied immediately.

All servers and network devices are documented in LINK Mobility A/S' documentation system. This is where all changes to the operation environment are registered. Configuration files for network devices (firewall, routers, switches, etc.) are stored automatically in the monitoring system.

The security policy has been prepared for providing LINK Mobility A/S with a common set of rules that, in turn, produces a stable operation environment and a high level of security. We make improvements to our policies, procedures and operations on a continuous basis.

In the general IT security area, LINK Mobility A/S has implemented the requisite procedures and controls in relation to the individual areas as specified in ISO27002:2013 and defined in Appendix 1, which shows the security structure and the control objectives implemented at LINK Mobility A/S.

Human resources and training

All active operations staff possesses the requisite competencies within their respective fields of work. This is ensured by, e.g. recruiting through networks and, if needed, by verifying relevant references.

Moreover, digital criminal records are obtained for all employees once a year. This control is performed in connection with an annual "IT Security Day", when the current IT security policy is reviewed with the entire staff. This day also serves as a training day at which staff is trained in relevant topics related to IT security.

Physical and environmental security

LINK Mobility A/S' operation environment is located in two geographically separated GlobalConnect data centres. The data centres have redundancies for all significant infrastructure components, such as power, UPS, emergency generators, network as well as internet connections.

Persons accessing GlobalConnect must use access cards and personal numeric codes. Moreover, any entry to a data centre is always reported to GlobalConnect and so is any exit, in order to ensure that all alarms, etc. remain active.

Operation environment in the data centre is placed in locked cabinets. Only authorised persons have access.
There is redundancy built into the provision of Internet connection both with respect to the service from GlobalConnect but also from the alternative provider, Nianet.

Only authorised persons are permitted to access the data centres via the established procedure and access privileges for such persons are reviewed annually at a minimum.

External persons (suppliers or customers) are solely permitted to access the premises, when accompanied by an authorised employee.

User management/access security

Access to the operating environment is possible by connecting physically in a data centre or externally solely via an SSL, VPN connection. Such connections are exclusively reserved for authorised persons and are divided into roles and responsibilities as set out in the relevant employee's job description. Such access is reviewed annually at a minimum.
Logical security is designed to ensure that only authorised users have access to the systems.

The IT security policy sets out the following requirements:

- Password requirements—all users created in LINK Mobility A/S' central user database are required to change passwords every 120 days; Passwords must contain at least eight alphanumeric characters and the last four passwords used must not be reused.
- Clients must be updated with the most recent security patches; and
- The operation environment can only be accessed via SSL-encrypted VPN access.

Monitoring

LINK Mobility A/S has established automatic monitoring of the operating environment, including for the SMS delivery, and has support staff on duty 24/7/365; this means that the necessary competencies are always available.

If an error is identified, an alarm is sent visually both on a monitoring screen and by SMS. In the event errors are identified in a component not subjected to automatic monitoring, measures will be taken to register such errors in the future.

If incidents occur that might affect operations, the monitoring system will automatically alert the contingency team and well-established escalation procedures exist with ultimate involvement of the IT Security Manager.

Backup

The purpose of backup is to ensure that data in the LINK Mobility A/S' operation environment can be recreated, accurately and rapidly, in this way avoiding unnecessary downtime for the customer.

A complete image is taken daily of each data centre, and the image stored in the other centre. This ensures that, in case of major crashes, an entirely new data centre can be re-established within a few minutes.

Managing IT security incidents

Security incidents and weaknesses in LINK Mobility A/S' systems are required to be reported in a manner that allows for timely adjustments.

All LINK Mobility A/S' employees are familiar with reporting procedures for various types of incidents and weaknesses that might affect the security of LINK Mobility A/S' operations. Security incidents and weaknesses must be reported to Management as quickly as possible. It is Management's responsibility to define and coordinate a structured management process ensuring appropriate responses to security incidents.

Business continuity management

The purpose of continuity management at LINK Mobility A/S is to ensure business continuity, secure critical information as-
sets and the rapid and sound recovery for customers in the event of a disaster or a major operating environment system crash or other factors resulting in the failure to effect delivery of services.

In the event of a major crash, customers using the affected services are informed via the e-mail list system and on LINK Mobility A/S' website. Such messages will contain a provisional status update, an error description and, if possible, an estimate of when the error will be remediated. Customers will be kept continuously notified through the e-mail list system and the LINK Mobility A/S' website, until the error has been remediated.

An internal escalation procedure has been prepared with a continuity description based on the scope of the crash or disaster. The full documentation for continuity management is reviewed and revised annually by the operating team.

Patch management

The purpose of patch management is to ensure that all relevant updates, such as patches, fixes and service packs are implemented to protect the systems against downtime and unauthorised access and that the implementation is carried out in a well-managed manner.

Internal machinery that is critical for the operations is not updated automatically. All local machinery and test servers are security patched every night between 03:00 and 04:00.

Servers included in the production, are security patched every Sunday between 20:00 and 21:00. Critical security patches are installed according to LINK Mobility A/S' policy for operational software management. LINK Mobility A/S makes back-up every day. The purpose of back-up is ensuring, inter alia, that the systems are able to return to normal operations, if updates do not perform as intended.

Change management

The purpose of change management is to ensure that changes are tested and tried, before actual production is started up and operation commenced.

LINK Mobility A/S' software intended to be part of the direct operations of SMS are subject to directions, including following a standard procedure, see current regulations. Source codes are placed in a secure test environment and are subject to version control. The test environment must be as close to the real world as it is possible without violating the security policies.

Significant changes in relation to IT security

During the period under review, there have been no significant changes in relation to IT security.

Customer responsibility (complementary customer controls)

Customers with direct access to the administrative system have full responsibility for safeguarding such access, since it provides access to any confidential information in the form of, e.g. track/trace and related message contents. In other words, LINK Mobility A/S is not responsible for access rights—including provisions, changes and cancelations—in relation to individual customers' users and their access to SMS service. The customer is responsible for ensuring any controls necessary in connection with this control objective.

Customers are responsible for data transmission to the LINK Mobility A/S' operating environment and it is the customers' responsibility to create the required data transmission to the LINK Mobility A/S' operating environment. Customers are required to ensure any controls necessary for this control objective.

LINK Mobility A/S' continuity management is structured around an overall contingency plan that describes the approach and procedures to be applied, if there is a need to recover LINK Mobility A/S' SMS delivery. Factors pertaining to customer installations or environments have not been taken into account.

APPENDIX 1:

LINK Mobility A/S applies the following control objectives and security measures from ISO27002:2013

5. Information security policies
- 5.1 Management direction for information security

6. Organisation of information security
- 6.1 Internal organisation
- 6.2 Mobile devices and teleworking

7. Human resource security
- 7.1 Prior to employment
- 7.2 During employment
- 7.3 Termination or change of employment

8. Asset management
- 8.1 Responsibility for assets
- 8.3 Handling of media

9. Access control
- 9.1 Business requirements of access control
- 9.2 User access management
- 9.3 Users' responsibility

12. Operations security
- 12.1. Operational procedures and responsibilities
- 12.2. Protection from malware
- 12.3. Backup
- 12.4. Logging and monitoring
- 12.5. Operational software management

13. Communication security
- 13.1. Network security management

15. Supplier security
- 15.1. Information security in supplier relationships
- 15.2. Supplier service delivery management

16. Information security incident management
- 16.1. Management of Information security incidents and improvements

17. Information security aspects of business continuity management
- 17.1. Information security continuity
- 17.2. Redundancies

CHAPTER 3:

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

For the customers of LINK Mobility A/S' SMS service and their auditors

Scope

We have been engaged to report on LINK Mobility A/S's description in Chapter 2 (including appendix 1), which is a description of general IT controls conducted in connection with the operation of LINK Mobility A/S' SMS service for processing customers' transactions during the period 1 June 2016 - 31 October 2017, and on the design and operating effectiveness of controls related to the control objectives mentioned in the description.

We express our opinion with reasonable assurance.

The report is based on a partial approach, which means that the present report does not include the IT security controls and control activities related to the use of external business partners. LINK Mobility A/S uses the following external partners in connection with operations of their SMS services in the following areas: Co-location / data centre – the physical security in relation to LINK Mobility A/S' production equipment.

The report does not cover customer-specific conditions. Furthermore, the report does not cover the complementary controls and control activities conducted by the user company; see the description of the company in Chapter 2 under the section about complementary controls.

LINK Mobility A/S' responsibility

LINK Mobility A/S is responsible for the preparation of the description and accompanying assertion in Chapter 2 (including appendix 1), including the completeness, accuracy and method of presentation of the description and assertion; for providing the services covered by the description; for stating the control objectives; and for designing, implementing and effectively operating controls to achieve the stated control objectives.

Beierholm's independence and quality management

We have complied with the requirements of independence and other ethical requirements laid down in FSR's Ethical Rules based on fundamental principles of integrity, objectivity, professional competence and requisite care, confidentiality and professional conduct.

We apply ISQC 1 and thus sustain a comprehensive system of quality management, including documented policies and procedures for compliance with ethical rules, professional standards as well as requirements in force under existing laws and additional regulation.

Auditor's responsibility

Our responsibility is to express an opinion on LINK Mobility A/S's description and on the design and operation of controls related to the control objectives stated in that description based on our procedures. We conducted our engagement in accordance with ISAE 3402, Assurance Reports on Controls at a Service Organisation, issued by the IAASB.
The standard requires that we comply with ethical requirements and that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and whether the controls are appropriately designed and operate effectively in all material respects.

An assurance engagement to report on the description, design and operating effectiveness of controls at a service 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 judgement of the service organisation's auditor, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed or not operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein, and the suitability of the criteria specified and described in Chapter 2 (including appendix 1) by LINK Mobility A/S.

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

Limitations of controls at LINK Mobility A/S

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

Opinion

Our opinion is based on the matters outlined in this report. The criteria on which our opinion is based are those described in Chapter 1 under Letter of Representation. In our opinion,

a) The description fairly presents the general IT controls of LINK Mobility A/S for SMS service, such as they were designed and implemented throughout the period 1 June 2016 – 31 October 2017 in all material respects; and

b) The controls related to the control objectives stated in the description were in all material respects suitably designed throughout the period 1 June 2016 - 31 October 2017; and

c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved in all material respects, operated effectively throughout the period 1 June 2016 - 31 October 2017.

Description of tests of controls

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

Intended users and purpose

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

Søborg, 14 November 2017

Beierholm
State-Authorized Public Accountant Partner Company

Kim Larsen
State Authorised Public Accountant

Jesper Aaskov Pedersen
IT Auditor, Manager

CHAPTER 4:

Auditor's Description of Control Objectives, Security Measures, Tests and Findings

We have structured our engagement in accordance with IASE 3402 – Assurance Reports on Controls at a Service Organisation. For each control objective, we start with a brief summary of the control objective as described in the frame of reference ISO27002:2013.

With respect to the period, we have tested whether LINK Mobility A/S has complied with the control objectives throughout the period 1 June 2016 - 31 October 2017.

Below the field with the summary of the control objective are three columns:

- The first column tells the activities LINK Mobility A/S, according to its documentation, has put into practice in order to comply with the requirements.
- The second column tells how we have decided to test, whether facts tally with descriptions.
- The third column tells the findings of our test.

The Tests Performed

The tests performed in connection with establishing the control measures' design, implementation and operational efficiency are conducted using the methods described below:

Inspection	Reading of documents and reports containing information about execution of the control. This includes, inter alia, reading and deciding about reports and other documentation in order to asses, whether it can be expected that the design of specific control measures will be efficient, if implemented. Furthermore, it is assessed, whether control measures are monitored and controlled sufficiently and with appropriate intervals.
Enquiries	Enquiries to/interview with relevant staff at LINK Mobility A/S. Enquiries have included how control measures are performed.
Observation	We have observed the performance of the control.
Repeating the control	Repeated the relevant control measure. We have repeated the performance of the control in order to verify that the control measure works as assumed.

PRELIMINARY CONTROL OBJECTIVE:

Risk Assessment and Management

The risk assessment must identify and prioritise the risks based on the operation of SMS services. The findings are to contribute to the identification and prioritisation of management interventions and precautionary measures necessary to address relevant risks.

LINK Mobility A/S' control procedures	Auditor's test of controls	Test findings
Through a risk assessment, risks have been identified and prioritised. The SMS services defined in the description is used as basis for the assessment. The findings contribute to the identification and prioritisation of management interventions and precautionary measures necessary to address relevant risks.	We have requested and obtained the relevant material in connection with the audit of risk management. We have checked that regular risk assessments are carried out for SMS services in relation to business conditions and their development. We have checked that the risk assessment is deployed down through the organisational levels. We have checked that company's risk profile is managed on a current basis and that relevant adaptations of consequences and probabilities are made regularly.	During our test, we did not identify any material deviations.

CONTROL OBJECTIVE 5:

Information Security Policies

Management must prepare an information security policy that covers, among other things, management's security objectives, policies and overall action plan. The information security policy is maintained, taking the current risk assessment into consideration.

LINK Mobility A/S' control procedures	Auditor's test of control procedures	Test findings
There is a written strategy covering, among other things, Management's security objectives, policies and overall action plan. The IT security policy and accompanying supporting policies are approved by the company's Management and then deployed down through the company's organisation. The policy is available for all relevant employees. The policy is re-evaluated according to planned intervals.	We have obtained and audited LINK Mobility A/S' latest IT security policy. During our audit, we checked that maintenance of the IT security policy is conducted on a continuous basis. At the same time, we checked during our audit that the underlying supporting policies have been implemented. We have checked that the policy is approved and signed by the company's Supervisory and Executive Boards and made available for the employees on LINK Mobility A/S' intranet.	During our test, we did not identify any material deviations.

CONTROL OBJECTIVE 6:

Organisation of Information Security

Management of the IT security must be established in the company. Organisational responsibility for the IT security must be placed with appropriate business procedures and instructions. The person responsible for IT security must ensure, among other things, compliance with security measures, including continuous updating of the overall risk assessment.

LINK Mobility A/S' control procedures	Auditor's test of control procedures	Test findings
Organisational responsibility for IT security has been placed, documented and implemented. The IT security has been coordinated across the company's organisation. Appropriate business procedures exist for employees regarding professional secrecy statements.	Through inspection and tests, we have ensured that the organisational responsibility for IT security is documented and implemented. We have checked that the IT security is deployed across the organisation in relation to SMS service. Through interviews, we have checked that the person responsible for IT security knows his/her role and responsibilities. Through enquiries and samples from employment contracts, we checked that LINK Mobility A/S' employees are familiar with their professional secrecy.	During our test, we did not identify any material deviations.
Risks in relation to use of mobile devices and teleworking are identified, and managing security conditions is appropriate.	We checked that formal cooperation agreements exist in connection with the use of mobile devices and teleworking. On a test basis, we have inspected that the policy is implemented regarding employees using mobile devices. Regarding the use of teleworking at LINK Mobility A/S we have checked whether appropriate security measures have been implemented ensuring that this area is covered in relation to the risk assessment of the area.	During our test, we did not identify any material deviations.

CONTROL OBJECTIVE 7:

Human Resource Security

It must be ensured that all new employees are aware of their specific responsibilities and roles in connection with the company's information security in order to minimise the risk of human errors, theft, fraud and abuse of the company's information assets.

LINK Mobility A/S' control procedures	Auditor's test of control procedures	Test findings
Based on the specified work processes and procedures, it is ensured that all new employees are informed of their specific responsibilities and roles in connection with their employment at LINK Mobility A/S. This includes the framework laid down for the work and the IT security involved. Security responsibilities, if any, are determined and described in job descriptions and in the terms of the employment contract. The employees are familiar with their professional secrecy based on a signed employment contract and through LINK Mobility A/S' HR policy.	We have verified that routines and procedures developed by Management in connection with start of employment and termination of employment have been adhered to. Based on random samples, we have tested whether the above routines and procedures have been complied with in connection with start of employment and termination of employment. Through interviews, we have checked that employees of significance to SMS service are familiar with their professional secrecy. We have examined the job descriptions of key employees and subsequently tested the awareness of the individual employee of their roles and related security responsibility. We have ensured that LINK Mobility A/S' HR policy is easily accessible and has a section on terms for professional secrecy with respect to information obtained in connection with work conducted at LINK Mobility A/S.	During our test, we did not identify any material deviations.

CONTROL OBJECTIVE 8:

Asset Management

The required protection of the company's information assets must be ensured and maintained, and all of the company's physical and functional information-related assets must be identified, and a responsible "owner" must be appointed. The company must ensure that the information assets in relation to SMS service are suitably protected.

LINK Mobility A/S' control procedures	Auditor's test of control procedures	Test findings
All information assets have been identified and an updated list of all significant assets has been established. An "owner" of all significant assets is appointed in connection with the operation of SMS service.	We have examined and checked the company's central IT register for significant IT entities in connection with the operation of LINK Mobility' SMS service. Through observation and control, we have checked relations to central knowhow systems for the operation of SMS service. By observations and enquiries, we have checked that LINK Mobility A/S complies with all material security measures for the area in accordance with the security standard.	During our test, we did not identify any material deviations.
Information and data in relation to SMS service and the subsequent hosting centre operation are classified based on business value, sensitivity and need for confidentiality.	We have checked that appropriate division exists and related procedures/business procedures in connection with protection of ownership between applications and data as well as other entities in relation to LINK Mobility A/S' operation of SMS service. We have checked that contracts and SLA are used as central tools to ensure the definition, segregation and delimitation of LINK Mobility A/S' responsibilities and the customer's responsibilities with respect to access to information and data. Accordingly, the customer is typically responsible for ensuring that a suitable protection level exists for own information and data.	During our test, we did not identify any material deviations.
Procedures of dealing with destruction of data media are established.	We have: • Asked Management which procedures/control activities are performed. • On a sample basis gone through the procedures for destruction of data media as confirmation that these are formally documented.	During our test, we did not identify any material deviations.

CONTROL OBJECTIVE 9:

Access Control

Access to the company's systems, information and network must be controlled based on business and statutory requirements. Authorised users' access must be ensured and unauthorised access must be prevented.

LINK Mobility control procedures	Auditor's test of control procedures	Test findings
Documentation and updated directions exist for LINK Mobility A/S' access control.	We have: • asked Management whether access control procedures have been established at LINK Mobility A/S. • verified on a test basis that access control procedures exist and have been implemented; see LINK Mobility A/S' directions. • by interviewing key personnel and by inspection on a test basis, we have verified that access control for the operations environment comply with LINK Mobility A/S' directions, and authorisations are granted according to agreement.	During our test, we did not identify any material deviations.
A formal business procedure exists for granting and discontinuing user access. Granting and application of extended access rights are limited and monitored.	We have asked Management whether access control procedures have been established at LINK Mobility A/S. By inspection on a test basis, we have verified • that adequate authorisation systems are used in relation to access control at LINK Mobility A/S. • that the formalised business procedures for granting and discontinuing user access have been implemented in LINK Mobility A/S' systems and registered users are subject to regular follow-up.	During our test, we did not identify any material deviations.
Internal users' access rights are reviewed regularly according to a formalised business procedure.	By inspection on test basis, we have verified that a formalised business procedure exists for follow-up on authorisation control according to the directions, including: • that formal management follow-up is performed on registered users with extended rights every three months. • that formal management follow-up is performed on registered users with ordinary rights every six months.	During our test, we did not identify any material deviations.
The granting of access codes is controlled through a formalised and controlled process, which ensures, among other things,	We have asked Management whether access code granting procedures have been established at LINK Mobility A/S.	During our test, we did not identify any material deviations.

that standard passwords are changed.	By inspection on a test basis, we have verified • that an automatic systems control takes place, when access codes are granted to check that passwords are changed after first login. • that standard passwords are changed in connection with implementation of systems software etc. • if this is not possible, that procedures ensure that standard passwords are changed manually.	
Access to operating systems and networks is protected by passwords. Quality requirements have been specified for passwords, which must have a minimum length (8 characters), no requirements as to complexity, maximum duration (max 120 days), and in addition password setup means that passwords cannot be reused (remembers the latest 4 versions). Furthermore, the user will be barred in the event of repeated unsuccessful attempts to login.	We have asked Management whether procedures ensuring quality passwords in LINK Mobility A/S are established. By inspection on a test basis, we have verified that appropriately programmed controls have been established to ensure quality passwords complying with the policies for: • minimum length of password • maximum life of password • minimum history of password • lockout after unsuccessful login attempts	During our test, we did not identify any material deviations.

CONTROL OBJECTIVE 12:

Operations Security

Control objective: Operations procedures and areas of responsibility.

A correct and adequate running of the company's operating systems must be ensured. The risk of technology related crashes must be minimised. A certain degree of long-term planning is imperative in order to ensure sufficient capacity. A continuous capacity projection must be performed based on business expectations for growth and new activities and the capacity demands derived hereof.

LINK Mobility A/S' control procedures	Auditor's test of control procedures	Test findings
The operations procedures for business critical systems have been documented, and they are available to staff with work-related needs. Management has implemented policies and procedures to ensure satisfactory segregation of duties.	We have: • asked Management whether all relevant operations procedures have been documented. • in connection with our audit of the individual areas of operation verified on a test basis that documented procedures exist and that there is concordance between the documentation and the actions actually performed. • inspected users with administrative rights in order to verify that access is justified by work-related needs and does not compromise the segregation of duties.	During our test, we did not identify any material deviations.
Management of operational environment is established in order to minimise the risk of technology related crashes. Continuous capacity projection is performed based on business expectations for growth and new activities and the capacity demands derived hereof.	We have: • asked Management about the procedures and control activities performed. • on a test basis examined that the operation environment's consumption of resources is monitored and adapted to the expected and necessary capacity requirements.	During our test, we did not identify any material deviations.

Control objective: Protection from malware

To protect from malicious software, such as virus, worms, Trojan horses and logic bombs. Precautions must be taken to prevent and detect attacks from malicious software.

LINK Mobility A/S' control procedures	Auditor's test of control procedures	Test findings
Preventive, detecting and remedial security and control procedures have been established, including the required training and provision of information for the company's users of information systems against malicious software.	We have: • enquired about and inspected the procedures/ control activities performed in the event of virus attacks or outbreaks. • enquired about and inspected the activities meant to increase the employees' awareness of precautions against virus attacks or outbreaks. • verified that anti-virus software has been installed on servers and inspected signature files documenting that they have been updated.	During our test, we did not identify any material deviations.

Control objective: Backup

To ensure the required accessibility to the company's information assets. Standard procedures must be established for backup, and for regular testing of the applicability of the copies.

LINK Mobility A/S' control procedures	Auditor's test of control procedures	Test findings
Backup is made of all the company's significant information assets, including, e.g. parameter setup and other operations-critical documentation, according to the specified directions.	We have: • asked Management about the procedures/ control activities performed. • examined backup procedures on a test basis to confirm that these are formally documented. • examined backup log on a test basis regarding backup to confirm that backup has been completed successfully and that failed backup attempts are handled on a timely basis. • examined physical security (e.g. access limitations) for internal storage location to confirm that backup is safely stored.	During our test, we did not identify any material deviations.

Control objective: Logging and monitoring

To reveal unauthorised actions. Business-critical IT systems must be monitored, and security incidents must be registered. Logging must ensure that unwanted conditions are detected.

LINK Mobility A/S' control procedures	Auditor's test of control procedures	Test findings
Operating systems and network transactions or activities involving special risks are monitored. Abnormal conditions are examined and resolved on a timely basis. LINK Mobility A/S logs, when internal users log off and on the systems. User are only actively monitored in the event of suspected or identified abuse of the systems.	We have: • asked Management about the procedures/ control activities performed, and have examined the system setup on servers and important network units as well as verified that parameters for logging have been set up, thus transactions made by users with extended rights are being logged. • checked on a test basis that logs from critical systems are subject to sufficient follow-up.	During our test, we did not identify any material deviations.
A central monitoring tool is used which sends alerts, if known errors occur. If possible, it is monitored whether an error is about to occur in order to react proactively. Alerts are shown on the monitoring screen mounted in the project and operations department. Critical alerts are also sent by email and SMS. Status reports are sent by email from different systems. Some every day – others when incidents occur in the system. The operations monitoring function is responsible for checking these emails on a daily basis.	We have: • asked Management about the procedures/ control activities performed. • ensured that a monitoring tool is used and that this is available to all employees. • ensured that alerts are sent by email and SMS, if errors occur. • examined status reports. • ensured that an operations monitoring service is established and that this function checks reports on a daily basis.	During our test, we did not identify any material deviations.

Control objective: Managing operations software and managing vulnerability

Ensuring establishment of appropriate procedures and controls for implementation and maintenance of operating systems.

LINK Mobility A/S' control procedures	Auditor's test of control procedures	Test findings
Changes in the operation environment comply with established procedures.	We have asked Management, whether procedures for change management are established at LINK Mobility A/S. By inspection on test basis, we have verified that • adequate procedures are applied, when controlled implementation of changes to the production environments of LINK Mobility A/S are performed. • changes to LINK Mobility A/S' operation environments comply with directions in force, including correct registration and documentation of change requests. On a test basis, we have inspected that the operating systems are updated in compliance with procedures in force and that current status is registered.	During our test, we did not identify any material deviations.
Changes in operating systems and operation environments comply with formalised procedures and processes.	We have asked Management, whether procedures for patch management are established in LINK Mobility A/S. By inspection on test basis, we have verified that adequate procedures are applied for controlled implementation of changes in the production environments, including that demands to the patch management controls ensure that • change requests are registered and described • all changes are subject to formal approval before implementation • changes are subject to formal impact assessments • fall-back plans are described • systems affected by changes are identified • documented test of changes is performed before implementation • documentation is updated reflecting the implemented changes in all material respects • procedures are subject to managing and coordination in a "change board".	During our test, we did not identify any material deviations.

Communication Security

To ensure protection of information in networks and protection of support of information processing facilities.

LINK Mobility A/S' control procedures	Auditor's test of control procedures	Test findings
Networks must be protected against threats in order to secure network based systems and the transmitted data. Production environment must be secured against failing supply in relation to redundancy to network connection to the internet. Network traffic/access from production environment to the outside world is available by means of multiple supply entries or access from more than one supplier.	It has been checked that necessary protection against unauthorised access is implemented, including: • Appropriate procedures for managing network equipment are established. • Segregation of user functions is established. • Appropriate logging and monitoring procedures are established. • Managing the company's network is coordinated in order to ensure optimal utilisation and a coherent security level. • Ensured that connections for data communication with the internet are established via more than one ISP supplier. • On a sample basis gone through documentation from the supplier about written basis for contract, as well as regular settlement of accounts for services rendered by the ISP supplier.	During our test, we did not identify any material deviations.
Adequate procedures for managing threats in the form of attacks from the internet (cyber-attacks) must be implemented. In this connection, tools for managing the contingency approach in the event of a cyber-attack must be devised.	• We have controlled that an adequate number of procedures with accompanying contingency plans regarding managing threats in relation to cyber-attacks are implemented. We have by inspection on a test basis ensured • that appropriate framework for managing cyber-attacks are devised. • that plans for managing the threat are devised and implemented. • that the plans include cross-organisational collaboration between internal groups.	During our test, we did not identify any material deviations.

CONTROL OBJECTIVE 15:

Supplier Security

External business partners are obliged to comply with the company's established framework for IT security level.

LINK Mobility A/S' control procedures	Auditor's test of control procedures	Test findings
Risks related to external business partners are identified, and security in third-party agreements and security in relation to customers are managed.	We have verified that in connection with the use of external business partners there are formal cooperation agreements. On a test basis, we have inspected that the cooperation agreements with external suppliers comply with the requirements about covering relevant security conditions in relation to the individual agreement.	During our test, we did not identify any material deviations.
In case of changes with impact on the production environment, and where services from external suppliers are used, suppliers are selected by the IT Security Manager. Solely recognised suppliers are used.	We have asked Management about relevant procedures applied in connection with choosing external partners. We have ensured that appropriate procedures for managing cooperation with external partners are established. We have tested that key suppliers have updated and approved contracts.	During our test, we did not identify any material deviations.
Monitoring must be conducted regularly, including supervision of external business partners.	We have ensured that there are appropriate processes and procedures for ongoing monitoring of external suppliers. We have checked that ongoing supervision is conducted by means of independent auditor's reports.	During our test, we did not identify any material deviations.

CONTROL OBJECTIVE 16:

Information Security Incident Management

To achieve reporting of security incidents and weaknesses in the company's information processing systems in a way that allows for timely corrections.

LINK Mobility A/S' control procedures	Auditor's test of control procedures	Test findings
Security incidents are reported to Management as soon as possible, and the managing is performed in a consistent and efficient way.	We have asked Management whether procedures have been established for reporting of security incidents. We have verified that procedures and business procedures have been developed for reporting and managing security incidents, and that the reporting is submitted to the right places in the organisation; see the directions. We have verified that the responsibility for managing critical incidents is clearly placed and that the related business procedures ensure that security breaches are managed expediently, efficiently and methodically.	During our test, we did not identify any material deviations.

CONTROL OBJECTIVE 17:

Information Security Aspects of Business Continuity Management

Business continuity management must counteract interruption in the company's business activities, protect critical information assets against the impact of a major crash or disaster, as well as ensure fast recovery.

LINK Mobility A/S' control procedures	Auditor's test of control procedures	Test findings
A consistent framework has been established for the company's contingency plans to ensure that all the plans are coherent and meet all security requirements, and to determine the prioritisation of tests and maintenance.	We have asked Management, whether business continuity management has been developed for LINK Mobility A/S' SMS service. By inspection on a test basis, we have verified • that appropriate framework for preparation of business continuity management has been established • that contingency plans are prepared and implemented • that the plans include business continuity management across the organisation • that the plans include appropriate strategy and procedures for communication with the interested parties of LINK Mobility A/S. • that contingency plans are tested on a regular basis • that maintenance and reassessment of the total basis for business continuity management is undertaken on a regular basis.	During our test, we did not identify any material deviations.