Statement of Applicability version 1.0 City Public Cloud

citynetwork

Introduction

This is a SOA intended for distribution to customers and the columns “Proof of implementation” and “Responsible manager” has intentionally been redacted. Information in these columns are classified Confidential and for company internal eyes only.

City Network Goal with ISMS

City Network shall be able to provide one or more offerings of programmable infrastructure with a pay as you go element that warrants to meet or exceed all EU compliance demands. Both present and future EU compliance demands. The offering may span Public Cloud, Community Cloud, Private Cloud and Hybrid Cloud.

City Network shall never be the weakest link in the security chain with the customer. City Network shall have as much or more security controls implemented than the Customer. The controls shall be verified by an independent authorised certification body.

SCOPE

City Network Hosting AB organisation.

ISO Certificate

Lloyd's Register

Certificate of Approval

This is to certify that the Management System of:

City Network Hosting AB

Borgmästaregatan 18, 371 34 Karlskrona, Sweden

has been approved by LRQA to the following standards:

ISO/IEC 27001:2013

P.G. Cornelissen - Area Manager North Europe

Issued By: LRQA Sverige AB

for and on behalf of: Lloyd's Register Quality Assurance Limited

Current Issue Date: 20 May 2018
Expiry Date: 19 May 2021
Certificate Identity Number: 10072127

Original Approvals:
ISO/IEC 27001 – 20 May 2015

Approval Number(s): ISO/IEC 27001 – 0001794

The scope of this approval is applicable to:
The Information Security regarding all services of City Public Cloud according to the Statement of Applicability version 1.0.

UKAS MANAGEMENT SYSTEMS
001

Statement of Applicability

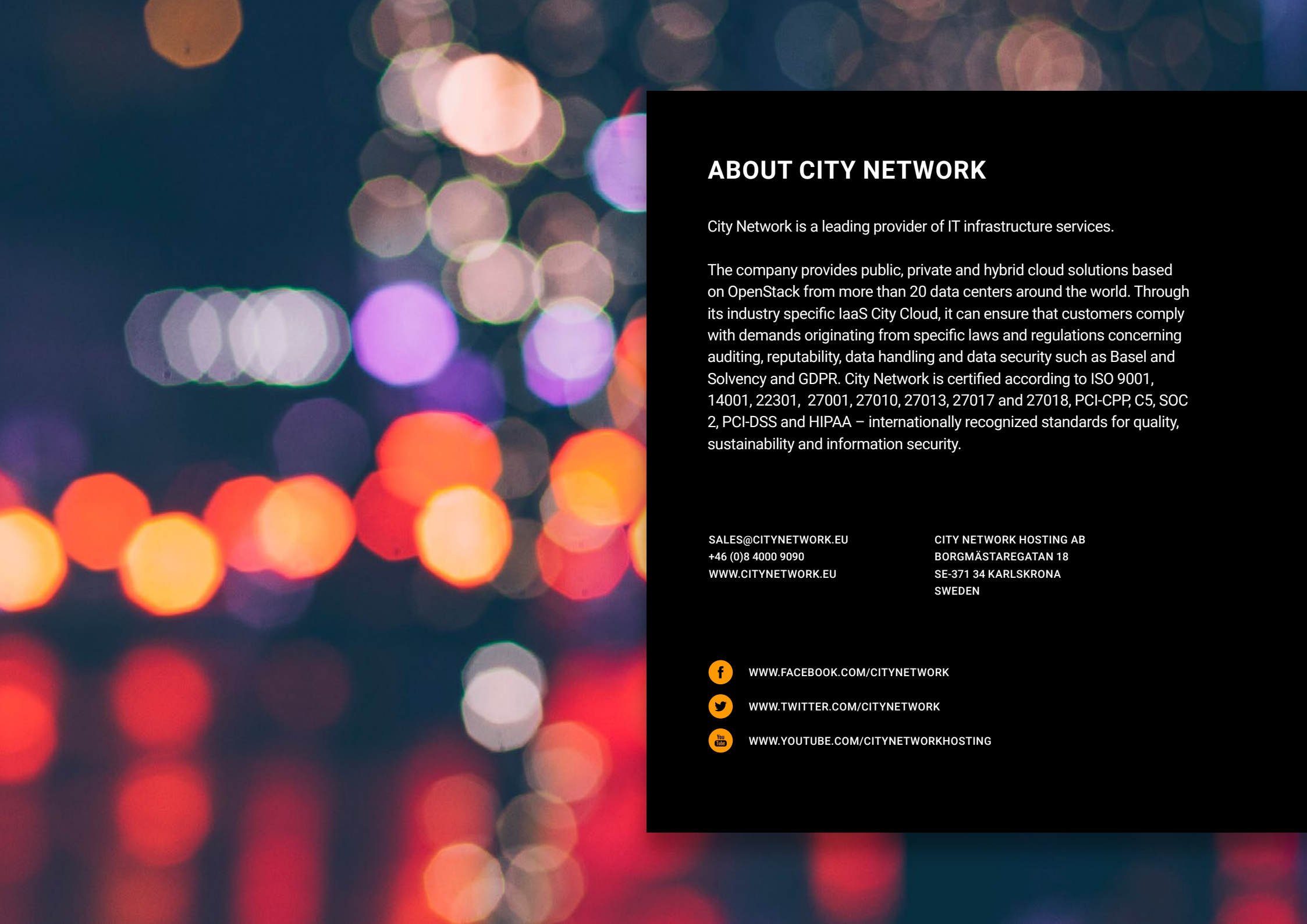
Row No	Control name	Frameworks	Control text	Status	Justification	Internal audit schedule	Proof of implemenww-tation	Responsible manager
1	5.1.1 Policies for information security	27002	A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties.	Included and implemented	Control deemed relevant by Senior Management	once per year		
2	5.1.2 Review of the policies for information security	27002	The policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	Included and implemented	Control deemed relevant by Senior Management	once per year		
3	6.1.1 Information security roles and responsibilities	27002	All information security responsibilities should be defined and allocated.	Included and implemented	Control deemed relevant by Senior Management	once per year		
4	6.1.2 Segregation of duties	27002	Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	Included and implemented	Control deemed relevant by Senior Management	once per year		
5	6.1.3 Contact with authorities	27002	Appropriate contacts with relevant authorities should be maintained	Included and implemented	Control deemed relevant by Senior Management	once per year		
6	6.1.4 Contact with special interest groups	27002	Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained	Included and implemented	Control deemed relevant by Senior Management	once per year		
7	6.1.5 Information security in project management	27002	Information security should be addressed in project management, regardless of the type of the project.	Included and implemented	Control deemed relevant by Senior Management	once per year		
8	6.2.1 Mobile device policy	27002	A policy and supporting security measures should be adopted to manage the risks introduced by using mobile devices.	Included and implemented	Control deemed relevant by Senior Management	once per year		
9	6.2.2 Teleworking	27002	A policy and supporting security measures should be implemented to protect information accessed, processed or stored at teleworking sites.	Included and implemented	Control deemed relevant by Senior Management	once per year		
11	7.1.1 Screening	27002	Background verification checks on all candidates for employment should be carried out in accordance with relevant laws, regulations and ethics and should be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	Included and implemented	Control deemed relevant by Senior Management	twice per year		
12	7.1.2 Terms and conditions of employment	27002	The contractual agreements with employees and contractors should state their and the organization's responsibilities for information security.	Included and implemented	Control deemed relevant by Senior Management	twice per year		
13	7.2.1 Management responsibilities	27002	Management should require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.	Included and implemented	Control deemed relevant by Senior Management	twice per year		
14	7.2.2 Information security awareness, education and training	27002	All employees of the organization and, where relevant, contractors should receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.	Included and implemented	Control deemed relevant by Senior Management	weekly		
15	7.2.3 Disciplinary process	27002	There should be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.	Included and implemented	Control deemed relevant by Senior Management	once per year		
16	7.3.1 Termination or change of employment responsibilities	27002	Information security responsibilities and duties that remain valid after termination or change of employment should be defined, communicated to the employee or contractor and enforced.	Included and implemented	Control deemed relevant by Senior Management	twice per year		
17	8.1.1 Inventory of assets	27002	Assets associated with information and information processing facilities should be identified and an inventory of these assets should be drawn up and maintained.	Included and implemented	Control deemed relevant by Senior Management	daily		
18	8.1.2 Ownership of assets	27002	Assets maintained in the inventory should be owned.	Included and implemented	Control deemed relevant by Senior Management	once per year		
19	8.1.3 Acceptable use of assets	27002	Rules for the acceptable use of information and of assets associated with information and information processing facilities should be identified, documented and implemented.	Included and implemented	Control deemed relevant by Senior Management	once per year		
20	8.1.4 Return of assets	27002	All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.	Included and implemented	Control deemed relevant by Senior Management	monthly		
22	8.2.1 Classification of information	27002	Information should be classified in terms of legal requirements, value, credibility, priority, criticality and sensitivity to unauthorized disclosure or modification.	Included and implemented	Control deemed relevant by Senior Management	once per year		

23	8.2.2 Labelling of information	27002	An appropriate set of procedures for information labelling should be developed and implemented in accordance with the information classification scheme adopted by the organization.	Included and implemented	Control deemed relevant by Senior Management	monthly		
24	8.2.3 Handling of assets	27002	Procedures for handling assets should be developed and implemented in accordance with the information classification scheme adopted by the organization.	Included and implemented	Control deemed relevant by Senior Management	monthly		
25	8.3.1 Management of removable media	27002	Procedures should be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.	Included and implemented	Control deemed relevant by Senior Management	monthly		
26	8.3.2 Disposal of media	27002	Media should be disposed of securely when no longer required, using formal procedures.	Included and implemented	Control deemed relevant by Senior Management	monthly		
27	8.3.3 Physical media transfer	27002	Media containing information should be protected against unauthorized access, misuse or corruption during transportation.	Included and implemented	Control deemed relevant by Senior Management	monthly		
35	9.1.1 Access control policy	27002	An access control policy should be established, documented and reviewed based on business and information security requirements.	Included and implemented	Control deemed relevant by Senior Management	monthly		
36	9.1.2 Access to networks and network services	27002	Users should only be provided with access to the network and network services that they have been specifically authorized to use.	Included and implemented	Control deemed relevant by Senior Management	daily		
37	9.2.1 User registration and de-registration	27002	A formal user registration and de-registration process should be implemented to enable assignment of access rights.	Included and implemented	Control deemed relevant by Senior Management	twice per year		
38	9.2.2 User access provisioning	27002	A formal user access provisioning process should be implemented to assign or revoke access rights for all user types to all systems and services.	Included and implemented	Control deemed relevant by Senior Management	twice per year		
39	9.2.3 Management of privileged access rights	27002	The allocation and use of privileged access rights should be restricted and controlled.	Included and implemented	Control deemed relevant by Senior Management	monthly		
40	9.2.4 Management of secret authentication information of users	27002	The allocation of secret authentication information should be controlled through a formal management process.	Included and implemented	Control deemed relevant by Senior Management	monthly		
41	9.2.5 Review of user access rights	27002	Asset owners should review users' access rights at regular intervals.	Included and implemented	Control deemed relevant by Senior Management	monthly		
42	9.2.6 Removal or adjustment of access rights	27002	The access rights of all employees and external party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change.	Included and implemented	Control deemed relevant by Senior Management	monthly		
43	9.3.1 Use of secret authentication information	27002	Users should be required to follow the organization's practices in the use of secret authentication information.	Included and implemented	Control deemed relevant by Senior Management	twice per year		
44	9.4.1 Information access restriction	27002	Access to information and application system functions should be restricted in accordance with the access control policy.	Included and implemented	Control deemed relevant by Senior Management	twice per year		
45	9.4.2 Secure log-on procedures	27002	Where required by the access control policy, access to systems and applications should be controlled by a secure log-on procedure.	Included and implemented	Control deemed relevant by Senior Management	monthly		
46	9.4.3 Password management system	27002	Password management systems should be interactive and should ensure quality passwords.	Included and implemented	Control deemed relevant by Senior Management	monthly		
47	9.4.4 Use of privileged utility programs	27002	The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled.	Included and implemented	Control deemed relevant by Senior Management	monthly		
48	9.4.5 Access control to program source code	27002	Access to program source code should be restricted.	Included and implemented	Control deemed relevant by Senior Management	twice per year		
51	10.1.1 Policy on the use of cryptographic controls	27002	A policy on the use of cryptographic controls for protection of information should be developed and implemented.	Included and implemented	Control deemed relevant by Senior Management	once per year		
52	10.1.2 Key management	27002	A policy on the use, protection and lifetime of cryptographic keys should be developed and implemented through their whole lifecycle.	Included and implemented	Control deemed relevant by Senior Management	twice per year		
53	11.1.1 Physical security perimeter	27002	Security perimeters should be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	Included and implemented	Control deemed relevant by Senior Management	once per year		
54	11.1.2 Physical entry controls	27002	Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	Included and implemented	Control deemed relevant by Senior Management	monthly		
55	11.1.3 Securing offices, rooms and facilities	27002	Physical security for offices, rooms and facilities should be designed and applied.	Included and implemented	Control deemed relevant by Senior Management	once per year		
56	11.1.4 Protecting against external and environmental threats	27002	Physical protection against natural disasters, malicious attack or accidents should be designed and applied.	Included and implemented	Control deemed relevant by Senior Management	once per year		

57	11.1.5 Working in secure areas	27002	Procedures for working in secure areas should be designed and applied.	Included and implemented	Control deemed relevant by Senior Management	once per year		
58	11.1.6 Delivery and loading areas	27002	Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.	Included and implemented	Control deemed relevant by Senior Management	once per year		
59	11.2.1 Equipment siting and protection	27002	Equipment should be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	Included and implemented	Control deemed relevant by Senior Management	once per year		
60	11.2.2 Supporting utilities	27002	Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities.	Included and implemented	Control deemed relevant by Senior Management	once per year		
61	11.2.3 Cabling security	27002	Power and telecommunications cabling carrying data or supporting information services should be protected from interception, interference or damage.	Included and implemented	Control deemed relevant by Senior Management	once per year		
62	11.2.4 Equipment maintenance	27002	Equipment should be correctly maintained to ensure its continued availability and integrity.	Included and implemented	Control deemed relevant by Senior Management	monthly		
63	11.2.5 Removal of assets	27002	Equipment, information or software should not be taken off-site without prior authorization.	Included and implemented	Control deemed relevant by Senior Management	monthly		
64	11.2.6 Security of equipment and assets off-premises	27002	Security should be applied to off-site assets taking into account the different risks of working outside the organization's premises.	Included and implemented	Control deemed relevant by Senior Management	once per year		
65	11.2.7 Secure disposal or re-use of equipment	27002	All items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	Included and implemented	Control deemed relevant by Senior Management	monthly		
66	11.2.8 Unattended user equipment	27002	Users should ensure that unattended equipment has appropriate protection.	Included and implemented	Control deemed relevant by Senior Management	once per year		
67	11.2.9 Clear desk and clear screen policy	27002	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted.	Included and implemented	Control deemed relevant by Senior Management	monthly		
68	12.1.1 Documented operating procedures	27002	Operating procedures should be documented and made available to all users who need them.	Included and implemented	Control deemed relevant by Senior Management	once per year		
69	12.1.2 Change management	27002	Changes to the organization, business processes, information processing facilities and systems that affect information security should be controlled.	Included and implemented	Control deemed relevant by Senior Management	monthly		
70	12.1.3 Capacity management	27002	The use of resources should be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	Included and implemented	Control deemed relevant by Senior Management	monthly		
71	12.1.4 Separation of development, testing and operational environments	27002	Development, testing, and operational environments should be separated to reduce the risks of unauthorized access or changes to the operational environment.	Included and implemented	Control deemed relevant by Senior Management	once per year		
73	12.2.1 Controls against malware	27002	Detection, prevention and recovery controls to protect against malware should be implemented, combined with appropriate user awareness.	Included and implemented	Control deemed relevant by Senior Management	monthly		
74	12.3.1 Information backup	27002	Backup copies of information, software and system images should be taken and tested regularly in accordance with an agreed backup policy.	Included and implemented	Control deemed relevant by Senior Management	monthly		
75	12.4.1 Event logging	27002	Event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed.	Included and implemented	Control deemed relevant by Senior Management	daily		
76	12.4.2 Protection of log information	27002	Logging facilities and log information should be protected against tampering and unauthorized access.	Included and implemented	Control deemed relevant by Senior Management	once per year		
77	12.4.3 Administrator and operator logs	27002	System administrator and system operator activities should be logged and the logs protected and regularly reviewed.	Included and implemented	Control deemed relevant by Senior Management	daily		
78	12.4.4 Clock synchronisation	27002	The clocks of all relevant information processing systems within an organization or security domain should be synchronised to a single reference time source.	Included and implemented	Control deemed relevant by Senior Management	once per year		
81	12.5.1 Installation of software on operational systems	27002	Procedures should be implemented to control the installation of software on operational systems.	Included and implemented	Control deemed relevant by Senior Management	monthly		
82	12.6.1 Management of technical vulnerabilities	27002	Information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	Included and implemented	Control deemed relevant by Senior Management	monthly		
83	12.6.2 Restrictions on software installation	27002	Rules governing the installation of software by users should be established and implemented.	Included and implemented	Control deemed relevant by Senior Management	once per year		

84	12.7.1 Information systems audit controls	27002	Audit requirements and activities involving verification of operational systems should be carefully planned and agreed to minimize disruptions to business processes.	Included and implemented	Control deemed relevant by Senior Management	once per year		
86	13.1.1 Network controls	27002	Networks should be managed and controlled to protect information in systems and applications.	Included and implemented	Control deemed relevant by Senior Management	monthly		
87	13.1.2 Security of network services	27002	Security mechanisms, service levels and management requirements of all network services should be identified and included in network services agreements, whether these services are provided in-house or outsourced.	Included and implemented	Control deemed relevant by Senior Management	monthly		
88	13.1.3 Segregation in networks	27002	Groups of information services, users and information systems should be segregated on networks.	Included and implemented	Control deemed relevant by Senior Management	monthly		
90	13.2.1 Information transfer policies and procedures	27002	Formal transfer policies, procedures and controls should be in place to protect the transfer of information through the use of all types of communication facilities.	Included and implemented	Control deemed relevant by Senior Management	once per year		
91	13.2.2 Agreements on information transfer	27002	Agreements should address the secure transfer of business information between the organization and external parties.	Included and implemented	Control deemed relevant by Senior Management	once per year		
92	13.2.3 Electronic messaging	27002	Information involved in electronic messaging should be appropriately protected.	Included and implemented	Control deemed relevant by Senior Management	once per year		
93	13.2.4 Confidentiality or non-disclosure agreements	27002	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified, regularly reviewed and documented.	Included and implemented	Control deemed relevant by Senior Management	once per year		
94	14.1.1 Information security requirements analysis and specification	27002	The information security related requirements should be included in the requirements for new information systems or enhancements to existing information systems.	Included and implemented	Control deemed relevant by Senior Management	once per year		
95	14.1.2 Securing application services on public networks	27002	Information involved in application services passing over public networks should be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.	Included and implemented	Control deemed relevant by Senior Management	once per year		
96	14.1.3 Protecting application services transactions	27002	Information involved in application service transactions should be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	Included and implemented	Control deemed relevant by Senior Management	once per year		
98	14.2.1 Secure development policy	27002	Rules for the development of software and systems should be established and applied to developments within the organization.	Included and implemented	Control deemed relevant by Senior Management	once per year		
99	14.2.2 System change control procedures	27002	Changes to systems within the development lifecycle should be controlled by the use of formal change control procedures.	Included and implemented	Control deemed relevant by Senior Management	once per year		
100	14.2.3 Technical review of applications after operating platform changes	27002	When operating platforms are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	Included and implemented	Control deemed relevant by Senior Management	once per year		
101	14.2.4 Restrictions on changes to software packages	27002	Modifications to software packages should be discouraged, limited to necessary changes and all changes should be strictly controlled.	Included and implemented	Control deemed relevant by Senior Management	once per year		
102	14.2.5 Secure system engineering principles	27002	Principles for engineering secure systems should be established, documented, maintained and applied to any information system implementation efforts.	Included and implemented	Control deemed relevant by Senior Management	once per year		
103	14.2.6 Secure development environment	27002	Organizations should establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.	Included and implemented	Control deemed relevant by Senior Management	once per year		
104	14.2.7 Outsourced development	27002	The organization should supervise and monitor the activity of outsourced system development.	Included and implemented	Control deemed relevant by Senior Management	once per year		
105	14.2.8 System security testing	27002	Testing of security functionality should be carried out during development.	Included and implemented	Control deemed relevant by Senior Management	once per year		
106	14.2.9 System acceptance testing	27002	Acceptance testing programs and related criteria should be established for new information systems, upgrades and new versions.	Included and implemented	Control deemed relevant by Senior Management	once per year		
107	14.3.1 Protection of test data	27002	Test data should be selected carefully, protected and controlled.	Included and implemented	Control deemed relevant by Senior Management	once per year		
108	15.1.1 Information security policy for supplier relationships	27002	Information security requirements for mitigating the risks associated with supplier's access to the organization's assets should be agreed with the supplier and documented.	Included and implemented	Control deemed relevant by Senior Management	once per year		
109	15.1.2 Addressing security within supplier agreements	27002	All relevant information security requirements should be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.	Included and implemented	Control deemed relevant by Senior Management	once per year		
110	15.1.3 Information and communication technology supply chain	27002	Agreements with suppliers should include requirements to address the information security risks associated with information and communications technology services and product supply chain.	Included and implemented	Control deemed relevant by Senior Management	once per year		

111	15.2.1 Monitoring and review of supplier services	27002	Organizations should regularly monitor, review and audit supplier service delivery.	Included and implemented	Control deemed relevant by Senior Management	monthly		
112	15.2.2 Managing changes to supplier services	27002	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.	Included and implemented	Control deemed relevant by Senior Management	once per year		
113	16.1.1 Responsibilities and procedures	27002	Management responsibilities and procedures should be established to ensure a quick, effective and orderly response to information security incidents.	Included and implemented	Control deemed relevant by Senior Management	once per year		
114	16.1.2 Reporting information security events	27002	Information security events should be reported through appropriate management channels as quickly as possible.	Included and implemented	Control deemed relevant by Senior Management	twice per year		
115	16.1.3 Reporting information security weaknesses	27002	Employees and contractors using the organization's information systems and services should be required to note and report any observed or suspected information security weaknesses in systems or services.	Included and implemented	Control deemed relevant by Senior Management	twice per year		
116	16.1.4 Assessment of and decision on information security events	27002	Information security events should be assessed and it should be decided if they are to be classified as information security incidents.	Included and implemented	Control deemed relevant by Senior Management	twice per year		
117	16.1.5 Response to information security incidents	27002	Information security incidents should be responded to in accordance with the documented procedures.	Included and implemented	Control deemed relevant by Senior Management	monthly		
118	16.1.6 Learning from information security incidents	27002	Knowledge gained from analysing and resolving information security incidents should be used to reduce the likelihood or impact of future incidents.	Included and implemented	Control deemed relevant by Senior Management	monthly		
119	16.1.7 Collection of evidence	27002	The organization should define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.	Included and implemented	Control deemed relevant by Senior Management	once per year		
121	17.1.1 Planning information security continuity	27002	The organization should determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.	Included and implemented	Control deemed relevant by Senior Management	once per year		
122	17.1.2 Implementing information security continuity	27002	The organization should establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	Included and implemented	Control deemed relevant by Senior Management	once per year		
123	17.1.3 Verify, review and evaluate information security continuity	27002	The organization should verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.	Included and implemented	Control deemed relevant by Senior Management	once per year		
124	17.2.1 Availability of information processing facilities	27002	Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.	Included and implemented	Control deemed relevant by Senior Management	once per year		
125	18.1.1 Identification of applicable legislation and contractual requirements	27002	All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements should be explicitly identified, documented and kept up to date for each information system and the organization.	Included and implemented	Control deemed relevant by Senior Management	once per year		
126	18.1.2 Intellectual property rights	27002	Appropriate procedures should be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.	Included and implemented	Control deemed relevant by Senior Management	once per year		
127	18.1.3 Protection of records	27002	Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.	Included and implemented	Control deemed relevant by Senior Management	once per year		
128	18.1.4 Privacy and protection of personally identifiable information	27002	Privacy and protection of personally identifiable information should be ensured as required in relevant legislation and regulation where applicable.	Included and implemented	Control deemed relevant by Senior Management	once per year		
129	18.1.5 Regulation of cryptographic controls	27002	Cryptographic controls should be used in compliance with all relevant agreements, legislation and regulations.	Included and implemented	Control deemed relevant by Senior Management	once per year		
131	18.2.1 Independent review of information security	27002	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) should be reviewed independently at planned intervals or when significant changes occur.	Included and implemented	Control deemed relevant by Senior Management	once per year		
132	18.2.2 Compliance with security policies and standards	27002	Managers should regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.	Included and implemented	Control deemed relevant by Senior Management	once per year		
133	18.2.3 Technical compliance review	27002	Information systems should be regularly reviewed for compliance with the organization's information security policies and standards.	Included and implemented	Control deemed relevant by Senior Management	once per year		



ABOUT CITY NETWORK

City Network is a leading provider of IT infrastructure services.

The company provides public, private and hybrid cloud solutions based on OpenStack from more than 20 data centers around the world. Through its industry specific IaaS City Cloud, it can ensure that customers comply with demands originating from specific laws and regulations concerning auditing, reputability, data handling and data security such as Basel and Solvency and GDPR. City Network is certified according to ISO 9001, 14001, 22301, 27001, 27010, 27013, 27017 and 27018, PCI-CPP, C5, SOC 2, PCI-DSS and HIPAA – internationally recognized standards for quality, sustainability and information security.

SALES@CITYNETWORK.EU
+46 (0)8 4000 9090
WWW.CITYNETWORK.EU

CITY NETWORK HOSTING AB
BORGMÄSTAREGATAN 18
SE-371 34 KARLSKRONA
SWEDEN

WWW.FACEBOOK.COM/CITYNETWORK

WWW.TWITTER.COM/CITYNETWORK

WWW.YOUTUBE.COM/CITYNETWORKHOSTING