Statement of Applicability

The Statement of Applicability contains justification for inclusion and exclusion of the Annex A controls.

Scope description

Information security related to:

- The development, production, and publication of e-procurement software
- Consultancy on the implementation, maintenance, specification, and governance of e-procurement frameworks
- Online services related to the exchange of e-procurement documents, and testing and publication of e-procurement capabilities

The hosting of these services is outsourced.

Detailed Description

General Ionite services:

- Consultancy: help service providers implement e-invoicing according to the relevant specifications. Provide technical support to organizations that implement and govern e-procurement frameworks.
- Software development: create new software solutions and customize existing software solutions related to e-procurement.

Specific services provided by Ionite:

- ion-SMP: a Peppol Service Metadata Provider, which is used to determine the servers that represent a trading entity on the PEPPOL network. See https://ion-smp.net/documentation/about/role/.
- ion-AP: a Peppol Access Point, which is used to send and receive documents on the Peppol network
- Test Tool: A Peppol access point that service providers can use to test their own access point implementation, and whether e-invoicing documents they create are valid according to the latest specification. See https://peppol-test.nl/documentation/introduction/whatsthis/

Our services use a combination of standard components and components developed in-house.

We process and protect the following data:

- Customer data, including data about trading entities and e-invoicing service providers, as provided by our customers.
  - Customer data, such as company and billing information, for our direct customers
  - Data of trading entities, provided to us by our customers with the explicit goal of publication on the network.
- User data, pertaining to the public sections of our services for which no contract with Ionite is required.
  - Access logs for auditing and security
  - Anonimized usage statistics, for reporting and service improvement.

The following processes are (partially) outsourced, but fall within the scope of the ISMS:

- Hosting for our servers and services

Controls

Control	Applicable	Requirement	Status	Reason
A.5.1 Policies for information security	YES	Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	Implemented	Risk assessment
A.5.2 Information security roles and responsibilities	YES	Information security roles and responsibilities shall be defined and allocated according to the organization needs.	Implemented	Risk Assessment
A.5.3 Segregation of duties	YES	Conflicting duties and areas of responsibility shall be segregated.	Implemented	Risk assessment
A.5.4 Management responsibilities	YES	Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.	Implemented	Risk assessment
A.5.5 Contact with authorities	YES	The organization shall establish and maintain contact with relevant authorities.	Implemented	Risk Assessment
A.5.6 Contact with special interest groups	YES	The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.	Implemented	Risk assessment

Control	Applicable	Requirement	Status	Reason
A.5.7 Threat intelligence	YES	Information relating to information security threats shall be collected and analysed to produce threat intelligence.	Implemented	Risk assessment
A.5.8 Information security in project management	YES	Information security shall be integrated into project management.	Implemented	Risk assessment
A.5.9 Inventory of information and other associated assets	YES	An inventory of information and other associated assets, including owners, shall be developed and maintained.	Implemented	Risk assessment
A.5.10 Acceptable use of information and other associated assets	YES	Rules for the acceptable use and procedures for the handling of information and other associated assets shall be identified, documented and implemented.	Implemented	Risk assessment
A.5.11 Return of assets	YES	Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.	Implemented	Risk assessment
A.5.12 Classification of information	YES	Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.	Implemented	Risk assessment
A.5.13 Labelling of information	YES	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Implemented	Risk assessment
A.5.14 Information transfer	YES	Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties.	Implemented	Risk assessment
A.5.15 Access control	YES	Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.	Implemented	Risk assessment
A.5.16 Identity management	YES	The full life cycle of identities shall be managed.	Implemented	Risk assessment
A.5.17 Authentication information	YES	Allocation and management of authentication information shall be controlled by a management process, including advising personnel of appropriate handling of authentication information.	Implemented	Risk assessment
A.5.18 Access rights	YES	Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization’s topic-specific policy on and rules for access control.	Implemented	Risk assessment
A.5.19 Information security in supplier relationships	YES	Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier’s products or services.	Implemented	Risk assessment
A.5.20 Addressing information security within supplier agreements	YES	Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.	Implemented	Risk assessment
A.5.21 Managing information security in the ICT supply chain	YES	Processes and procedures shall be defined and implemented to manage information security risks associated with the ICT products and services supply chain.	Implemented	Risk assessment
A.5.22 Monitoring, review and change management of supplier services	YES	The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	Implemented	Risk assessment
A.5.23 Information security for use of cloud services	YES	Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization’s information security requirements.	Implemented	Risk assessment
A.5.24 Information security incident management planning and preparation	YES	The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.	Implemented	Risk assessment
A.5.25 Assessment and decision on information security events	YES	The organization shall assess information security events and decide if they are to be categorized as information security incidents.	Implemented	Risk assessment

Control	Applicable	Requirement	Status	Reason
A.5.26 Response to information security incidents	YES	Information security incidents shall be responded to in accordance with the documented procedures.	Implemented	Risk assessment
A.5.27 Learning from information security incidents	YES	Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.	Implemented	Risk assessment
A.5.28 Collection of evidence	YES	The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	Implemented	Risk assessment
A.5.29 Information security during disruption	YES	The organization shall plan how to maintain information security at an appropriate level during disruption.	Implemented	Risk assessment
A.5.30 ICT readiness for business continuity	YES	ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	Implemented	Risk assessment
A.5.31 Identification of legal, statutory, regulatory and contractual requirements	YES	Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements shall be identified, documented and kept up to date.	Implemented	Risk Assessment
A.5.32 Intellectual property rights	YES	The organization shall implement appropriate procedures to protect intellectual property rights.	Implemented	Risk assessment
A.5.33 Protection of records	YES	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	Implemented	Risk assessment
A.5.34 Privacy and protection of PII	YES	The organization shall identify and meet the requirements regarding preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	Implemented	Risk assessment
A.5.35 Independent review of information security	YES	The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur.	Implemented	Risk assessment
A.5.36 Compliance with policies and standards for information security	YES	Compliance with the organization's information security policy, topic-specific policies and standards shall be regularly reviewed.	Implemented	Risk assessment
A.5.37 Documented operating procedures	YES	Operating procedures for information processing facilities shall be documented and made available to personnel who need them.	Implemented	Risk assessment
A.6.1 Screening	YES	Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	Implemented	Risk assessment
A.6.2 Terms and conditions of employment	YES	The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.	Implemented	Risk assessment
A.6.3 Information security awareness, education and training	YES	Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.	Implemented	Risk assessment
A.6.4 Disciplinary process	YES	A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.	Implemented	Risk assessment
A.6.5 Responsibilities after termination or change of employment	YES	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.	Implemented	Risk assessment
A.6.6 Confidentiality or non-disclosure agreements	YES	Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	Implemented	Risk assessment
A.6.7 Remote working	YES	Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.	Implemented	Risk assessment

Control	Applicable	Requirement	Status	Reason
A.6.8 Information security event reporting	YES	The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	Implemented	Risk assessment
A.7.1 Physical security perimeter	YES	Security perimeters shall be defined and used to protect areas that contain information and other associated assets.	Implemented	Risk assessment
A.7.2 Physical entry controls	YES	Secure areas shall be protected by appropriate entry controls and access points.	Implemented	Risk assessment
A.7.3 Securing offices, rooms and facilities	YES	Physical security for offices, rooms and facilities shall be designed and implemented.	Implemented	Risk assessment
A.7.4 Physical security monitoring	YES	Premises shall be continuously monitored for unauthorized physical access.	Implemented	Risk assessment
A.7.5 Protecting against physical and environmental threats	YES	Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.	Implemented	Risk assessment
A.7.6 Working in secure areas	YES	Security measures for working in secure areas shall be designed and implemented.	Implemented	Risk assessment
A.7.7 Clear desk and clear screen	YES	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.	Implemented	Risk assessment
A.7.8 Equipment siting and protection	YES	Equipment shall be sited securely and protected.	Implemented	Risk assessment
A.7.9 Security of assets off-premises	YES	Off-site assets shall be protected.	Implemented	Risk assessment
A.7.10 Storage media	YES	Storage media shall be managed through its life cycle of acquisition, use, transportation and disposal in accordance with the organization’s classification scheme and handling requirements.	Implemented	Risk assessment
A.7.11 Supporting utilities	YES	Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.	Implemented	Risk assessment
A.7.12 Cabling security	YES	Cables carrying power, data or supporting information services shall be protected from interception, interference or damage.	Implemented	Risk assessment
A.7.13 Equipment maintenance	YES	Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.	Implemented	Risk assessment
A.7.14 Secure disposal or re-use of equipment	YES	Items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	Implemented	Risk assessment
A.8.1 User endpoint devices	YES	Information stored on, processed by or accessible via user endpoint devices shall be protected.	Implemented	Risk assessment
A.8.2 Privileged access rights	YES	The allocation and use of privileged access rights shall be restricted and managed.	Implemented	Risk assessment
A.8.3 Information access restriction	YES	Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.	Implemented	Risk assessment
A.8.4 Access to source code	YES	Read and write access to source code, development tools and software libraries shall be appropriately managed.	Implemented	Risk assessment
A.8.5 Secure authentication	YES	Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.	Implemented	Risk assessment
A.8.6 Capacity management	YES	The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.	Implemented	Risk assessment
A.8.7 Protection against malware	YES	Protection against malware shall be implemented and supported by appropriate user awareness.	Implemented	Risk assessment
A.8.8 Management of technical vulnerabilities	YES	Information about technical vulnerabilities of information systems in use shall be obtained, the organization’s exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.	Implemented	Risk assessment
A.8.9 Configuration management	YES	Configurations, including security configurations, of hardware, software, services and networks shall be	Implemented	Risk assessment

Control	Applicable	Requirement	Status	Reason
		established, documented, implemented, monitored and reviewed.		
A.8.10 Information deletion	YES	Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.	Implemented	Risk assessment
A.8.11 Data masking	YES	Data masking shall be used in accordance with the organization’s topic-specific policy on access control and other related topic-specific, and business requirements, taking applicable legislation into consideration.	Implemented	Risk assessment
A.8.12 Data leakage prevention	YES	Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.	Implemented	Risk assessment
A.8.13 Information backup	YES	Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	Implemented	Risk assessment
A.8.14 Redundancy of information processing facilities	YES	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	Implemented	Risk assessment
A.8.15 Logging	YES	Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.	Implemented	Risk assessment
A.8.16 Monitoring activities	YES	Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	Implemented	Risk assessment
A.8.17 Clock synchronization	YES	The clocks of information processing systems used by the organization shall be synchronized to approved time sources.	Implemented	Risk assessment
A.8.18 Use of privileged utility programs	YES	The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled.	Implemented	Risk assessment
A.8.19 Installation of software on operational systems	YES	Procedures and measures shall be implemented to securely manage software installation on operational systems.	Implemented	Risk assessment
A.8.20 Network controls	YES	Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.	Implemented	Risk assessment
A.8.21 Security of network services	YES	Security mechanisms, service levels, and service requirements of network services shall be identified, implemented and monitored.	Implemented	Risk assessment
A.8.22 Segregation in networks	YES	Groups of information services, users, and information systems shall be segregated in the organization’s networks.	Implemented	Risk assessment
A.8.23 Web filtering	YES	Access to external websites shall be managed to reduce exposure to malicious content.	Implemented	Risk assessment
A.8.24 Use of cryptography	YES	Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.	Implemented	Risk assessment
A.8.25 Secure development life cycle	YES	Rules for the secure development of software and systems shall be established and applied.	Implemented	Risk assessment
A.8.26 Application security requirements	YES	Information security requirements shall be identified, specified and approved when developing or acquiring applications.	Implemented	Risk assessment
A.8.27 Secure system architecture and engineering principles	YES	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities.	Implemented	Risk assessment
A.8.28 Secure coding	YES	Secure coding principles shall be applied to software development.	Implemented	Risk assessment
A.8.29 Security testing in development and acceptance	YES	Security testing processes shall be defined and implemented in the development life cycle.	Implemented	Risk assessment

Control	Applicable	Requirement	Status	Reason
A.8.30 Outsourced development	NO	The organization shall direct, monitor and review the activities related to outsourced system development.	Not implemented	We do not outsource development. All custom software is done in-house.
A.8.31 Separation of development, test and production environments	YES	Development, testing, and production environments shall be separated and secured.	Implemented	Risk assessment
A.8.32 Change management	YES	Changes to information processing facilities and information systems shall be subject to change management procedures.	Implemented	Risk assessment
A.8.33 Test information	YES	Test information shall be appropriately selected, protected and managed.	Implemented	Risk assessment
A.8.34 Protection of information systems during audit and testing	YES	Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management.	Implemented	Risk assessment