VI. Risk management, data management, information security and assurance statement

This Annex to the EETS Domain Statement Blankenburgverbinding contains the requirements that the services of (E)ETS providers must meet in terms of risk management, data management and information security and sets out the requirements for the assurance statement referred to in Article 19.5 of the EETS Domain Statement.

1. Assurance statement

1.1. The assurance statement referred to in article 19.5 of the EETS Domain Statement, shall in any case cover the elements mentioned in Article 8 of Annex IV of the EETS Domain Statement, Article 2 and Article 3 of this Annex VI.

1.2. The costs for the assurance statement shall be borne by the (E)ETS provider, as well as the costs to implement findings and concerns following from (external) audits as soon as possible and in coordination with the Toll charger.

1.3. If the (E)ETS provider does not have an assurance statement referred to in Article 19.5 of the EETS Domain Statement, the (E)ETS provider shall have an assurance statement as referred to in article 17.7 no later than six (6) calendar months after the start of its services. 19.5 of the EETS Domain Statement.

1.4. To test the assurance declaration, the Toll charger reserves the right to carry out or arrange for inspections in accordance with Article 18 of the EETS Domain Statement. If the (E)ETS provider does not cooperate with the inspections as required, the Toll charger shall have the right, after prior written notice with a deadline of at least 30 days and no more than once per calendar year, to have an authorised party perform an inspection on behalf of the Toll charger at the (E)ETS provider.

1.5. In case the Toll charger deems it necessary to perform penetration tests on the (E)ETS provider's services to verify information security, the (E)ETS provider shall provide a signed safeguard declaration prior to the penetration tests.

2. Data Management

With respect to data management, the (E)ETS provider shall, as a minimum:

(i) create an overview of the data (or data objects and data attributes) it records in relation to its services in the EETS domain Blankenburgverbinding, by recording at least the following for each piece of data:

(a). definition;

(b). business process(es) for which this data is necessary;

(c). data format;

(d). Whether the data is optional or mandatory;

(e). if applicable, reference dates or a control mechanism applied for this data;

(f). classification of the sensitivity of the data with respect to privacy, fraud and competition;

(g). Who or what roles have access to this data, as well as what rights this person or role is given;

(h). How long this data may be kept under applicable laws and regulations;

(i). reference to standards relevant to this data (e.g., ISO, NEN, etc.);

(ii) ensure that when entering data into its systems, the actual mandatory data is entered in accordance with the correct data format, including the use of reference data or control mechanisms;

(iii) Conduct a data impact analysis for each system change that reevaluates and updates previous points;

(iv) Periodically check data to determine its quality through the use of data formats, obligations, standards, reference data and control mechanisms.

3. Risk management and information security

3.1. The (E)ETS provider shall comply with the requirements in this article 2 and implements the requirements set out in this Article 2 regarding risk management and information security measures, taking into account the further specification in article 3.11, Table 1, of this Annex VI.

3.2. If and to the extent that the (E)ETS provider uses third party services, then the requirements and obligations to implement measures pursuant to this Article 2 shall also apply to the relevant third parties. The (E)ETS provider shall ensure that the relevant third parties comply with the requirements and obligations to implement measures pursuant to this article 2.

3.3. The (E)ETS provider shall implement measures that ensure that changes referred to in Article 16 and 17 of the EETS Domain Statement:

(i) Be implemented through a change management process; and

(ii) have been tested and do not compromise implemented security measures.

3.4. The (E)ETS provider shall implement measures to periodically install patches on IT components.

3.5. The (E)ETS provider shall implement the following measures for access security:

(i) measures to restrict access to and use of company assets to authorised users and administrators on a least-privilege basis;

(ii) Measures to regularly review access rights to assets;

(iii) measures so that passwords meet complexity requirements;

(iv) implemented measures to apply multifactor authentication when accessing trusted areas from untrusted zones (e.g. internet).

3.6. The (E)ETS provider shall implement measures that ensure the availability of the service in accordance with the requirements referred to in Article 31 is ensured. These measures shall be demonstrably tested periodically but at least once a year and in case of relevant changes.

3.7. The (E)ETS provider shall implement the following technical security measures:

(i) measures to harden IT components (the process of securing a system by reducing its vulnerability);

(ii) implemented measures to centrally store and monitor security logging for all IT components, including management and user access;

(iii) measures to secure networks and communication flows to prevent data from being intercepted, leaked or altered.

3.8. The (E)ETS provider shall implement the following measures in relation to security incidents and data breaches:

(i) measures to detect, record and handle security incidents according to procedures;

(ii) measures to maintain detection processes and procedures;

(iii) measures to immediately report security incidents, the consequences of which for the Toll charger cannot reasonably be excluded, to the Toll charger.

3.9. The (E)ETS provider shall implement the following vulnerability management measures:

(i) measures to receive and assess security risk reports from external bodies;

(ii) measures to periodically (automatically) examine IT components for the existence of known vulnerabilities, security

threats, or policy deviations. The (E)ETS provider shall monitor incidents and report incidents and their follow-up to the Toll charger.

(iii) measures to test, at least once a year, the interfaces with the Toll charger back office and underlying IT components for the existence of vulnerabilities by means of penetration tests. The (E)ETS provider shall remedy findings following the penetration tests as soon as possible. The (E)ETS provider shall report to the Toll charger on the status and progress of the follow-up and respectively remedial actions.

3.10. The (E)ETS provider shall require that the employees to be deployed by it provide a Certificate of Good Conduct ("VOG"), or a certificate of equivalent purport and status in the case of employees who are not Dutch nationals. The VOG must have been issued for the purpose of the position to be held by the relevant employee within the operations of the (E)ETS provider and the associated job description. The VOG must not be older than six months from the date of commencement of employment of the employee concerned with the (E)ETS provider.

3.11. The (E)ETS provider shall comply with the following additional requirements on risk management and information security. The requirements in Table 1 are a further specification of the requirements in this article 2. A reference to the relevant part of this Article 2 is included in the table below.

Table 1 Digital security requirements and measures

Article	Reference	Category	Claim
3.3	ID.AM.02	Asset Management	The (E)ETS provider shall keep a register of all components and systems used, linking them to a system owner. The (E)ETS provider shall provide periodic insight to the Toll charger regarding this register.
3.3	PR.CM.3	Configuration Change control	The (E)ETS provider shall have a change management process that ensures a controlled way of implementing changes.
3.3	ID.RM	Risk Management Strategy	Risk management processes shall be established and implemented to identify, assess and manage risks within the toll chain.
3.3	ID.SC	Supply chain risk management	Risk management processes shall be established and implemented to identify, assess and manage risks related to (sub)contractors within the toll chain.
3.4	ID.AM.02	Asset Management	The (E)ETS provider shall implement measures to periodically (at least monthly) install patches on IT components to prevent vulnerabilities.
3.5	PR.AC	Identity Management and Access Control	User accounts and (secret) authentication credentials shall be issued, managed, verified, revoked and monitored for authorised devices, users and processes.

3.5	PR.AC.01	Identity Management and Access Control	The (E)ETS provider shall use strong keys according to current valid algorithms and key lengths used in communication between systems in different domains, and shall adequately secure access to these keys.
3.5	PR.AC.02	Identity Management and Access Control	The (E)ETS provider shall have a set of minimum security requirements for creating, exchanging and storing keys, which comply with 'Webtrust for Certification Authorities' or with 'ETSI TS 101 456 Policy requirements for certification authorities issuing qualified certificates'.
3.5	PR.AC.03	Identity Management and Access Control	The (E)ETS provider shall follow the specifications in the security framework ISO/TS 19299:2015 for setting up key management.
3.5	PR.AC.07	Identity Management and Access Control	The (E)ETS provider shall ensure that the authorisation management, is configured to comply with NEN-ISO/IEC27001:2017.
3.5	PR.AC.08	Identity Management and Access Control	The (E)ETS provider shall set requirements for how authorisation management is designed, e.g. through specifications of roles, authorisation matrix and password policy.
3.5	PR.AC.09	Identity Management and Access Control	The (E)ETS provider shall specify for each component in the (E)ETS provider's system: - how access is determined - - when access is revoked
3.5	PR.AC.10	Identity Management and Access Control	All user accounts and privileges for all components in the chain shall be analysed periodically. Here, access shall be arranged in such a way that the principle of least privilege and separation into function and/or roles is met.
3.43.5	PR.AC.11	Identity Management and Access Control	The (E)ETS provider shall ensure that each system grants access to the stored data only after authorisation.
3.5	PR.AC.12	Identity Management and Access Control	The (E)ETS provider shall ensure that access to the stored data is only granted via established procedure and via approved interfaces.
3.5	PR.AT	Awareness and Training	All staff and all partners of the (E)ETS provider shall be periodically trained on cybersecurity.
3.6	RC.RP	Recovery Planning	Recovery processes and procedures shall be implemented and maintained to ensure successful recovery.
3.6	RC.CO	Recovery Communications	Recovery processes and procedures shall be coordinated and communicated to internal and external stakeholders.
3.6	RC.IM	Recovery Improvements	Recovery processes and procedures shall be improved from current and previous cybersecurity activities.
3.6	PR.MA	Maintenance	Equipment shall be properly maintained to ensure its continuous availability and integrity.
3.6	PR.MA.01	Maintenance	The (E)ETS provider shall organise the management and maintenance processes

			according to the best practices defined in [NIST Cyber Security Framework] or NEN-ISO/IEC 27002:2013.
3.7	PR.DS	Data Security	Confidentiality, integrity and availability of data shall be ensured.
3.7	PR.DS.01	Data Security	The (E)ETS provider shall ensure that for all (temporarily) stored data: - the data remain unchanged; - the confidentiality of the data is guaranteed when access is granted; - the origin of the data is traceable at all times.
3.7	PR.DS.04	Data Security	The exchange of data shall take place over a channel for which: - the availability is reliable; - the confidentiality of the data is guaranteed; - the content of the data remains unchanged; - the identity of the sender is established; - it is indisputable that the data has been received or sent respectively; - both parties have verified each other prior to the exchange; - resent messages are detected; - large amounts of non-arrived data (such as toll declarations or billing details) are detected (to protect against interface errors).
3.7	PR.DS.16	Data Security	The (E)ETS provider shall verify the origin of the toll data received before accepting the received data.
3.7	PR.DS.17	Data Security	The (E)ETS provider shall provide the Toll charger with the cryptographically signed exception list.
3.7	PR.DS.18	Data Security	The (E)ETS provider shall provide a cryptographically signed acknowledgement of receipt of the toll data to the Toll charger.
3.7	PR.DS.24	Data Security	The (E)ETS provider enables users to check the accuracy of invoices.
3.7	PR.IP	Information Protection Processes and Procedures	Cybersecurity processes and procedures are established, managed and implemented to secure information systems and components of the (E)ETS provider.
3.7	PR.IP.01	Information Protection Processes and Procedures	The (E)ETS provider establishes guidelines for secure configurations of all IT components in the chain and to be implemented before they may be used in the Netherlands.
3.7	PR.IP.14	Information Protection Processes and Procedures	The (E)ETS provider stores all sensitive data (at rest) adequately encrypted.
3.7	PR.IP.15	Information Protection Processes and Procedures	The (E)ETS provider shall transmit customer lists exclusively in encrypted form. Here, at least TLS1.3 based on Public-Key-Infrastructure (PKI) shall be used.
3.7	PR.IP.22	Information Protection	Besides encrypting communications based on TLS1.3 based on Public-Key-Infrastructure (PKI), the (E)ETS provider

		Processes and Procedures	additionally encrypts invoices and registrations before sending them.
3.7	PR.PT	Protective Technology	Technical security measures are implemented and managed to ensure the security of systems and components, in accordance with policies, procedures and agreements.
3.7	PR.PT.02	Protective Technology	The (E)ETS provider shall establish technical specifications and additional security measures for the secure establishment of communication flows between two actors.
3.7	PR.PT.05	Protective Technology	The (E)ETS provider shall ensure that the level of security does not decrease when implementing and integrating external products or services.
3.7	DE.AE	Anomalies and Events	Data breaches and other suspicious events are detected and handled properly.
3.7	DE.CM	Security Continuous Monitoring	The (E)ETS provider's information systems and components are monitored to identify cybersecurity events.
3.7	DE.CM.01	Security Continuous Monitoring	The (E)ETS provider shall set up logging and monitoring on (administrative) user access.
3.7	DE.DP	Detection Processes	Detection processes and procedures are maintained and tested to provide insight into cybersecurity events and incidents.
3.7	DE.DP.01	Detection Processes	The (E)ETS provider and subcontractors set up processes to prevent, detect and handle cybersecurity incidents within 24 hours.
3.8	RS.RP	Response Planning	Cyber-response activities are implemented and maintained to ensure timely response to an incident.
3.8	RS.CO	Communications	Cyber-response activities are coordinated and communicated to internal and external stakeholders.
3.8	RS.CO.03	Communications	The (E)ETS provider shall report a detected cybersecurity incident to the Toll charger within 24 hours.
3.8	RS.AN	Analysis	Analyses on cybersecurity events and incidents are conducted to support cyber-response activities.
3.8	RS.MI	Mitigation	The handling of cybersecurity events is done in collaboration between internal and external stakeholders.
3.8	RS.MI.02	Mitigation	The (E)ETS provider supports in the event of an incident concerning cybersecurity support n those responsible for resolving these events.
3.8	RS.IM	Improvements	Cyber-response activities are enhanced from current and previous cybersecurity activities.
3.9	ID.GV.05	Governance	The (E)ETS provider and subcontractors of the (E)ETS provider shall prepare and submit its own cybersecurity policy to the Toll charger. This cybersecurity policy shall comply with the standard NIST Cybersecurity Framework or NEN-EN-ISO/IEC27001:2017.

3.9	ID.GV.07	Governance	The (E)ETS provider and its subcontractors shall periodically report the status of cybersecurity to the Toll charger.
3.9	ID.GV.08	Governance	The (E)ETS provider and its subcontractors shall establish guidelines for the safe use of components in toll chain. These guidelines should be followed by any administrator with authorised access to components.