Annex 4 Catalogue of selection criteria – IT features

The selection criteria consist of 199 IT features, subdivided into nineteen (19) IT domains. For each IT domain, it is indicated what is the maximum points per domain and what is the passing mark (i.e. the number of points).

ID	IT Domain	Maximum points per Domain	Points to pass per Domain
23	Access Management	6.5	4
24	Asset Management	12	6
25	Business Continuity Management	19	9
26	Change Management D	8.5	6
27	Cryptography	6	3
28	Exception Management	9	4
29	HR/Organizational Context	7	5
30	Incident Management	6	4
31	Information Management	11.5	6
32	Log Management	6.5	3
33	Physical Security	10.5	5
34	Risk Management	6.5	5
35	Service Provider Management	6.5	4
36	System Development Lifecycle	11	6
37	Teleworking	5	3
38	Secure platform access for network users	5.5	3
39	Peak service load	5	2
40	Graphical user interface of the platform in English	6	3
41	Helpdesk availability (outside business hours)	5.5	3

23. Access Management **Rationale:** The organisation shall develop, document and implement procedures related to the **management of user accounts and access** covering: responsibilities, access request and approval, access provisioning, review of access rights, special procedures (e.g. password reset). **Requirements for user accounts** and quality passwords shall be decided, documented, approved, communicated and implemented. Access to IT assets shall be based on business needs and user responsibilities. Access of specific administrative functions shall be subject to additional controls and to additional security measures, if applicable. Administrative and functional **roles should be properly separated**, where possible.	
	Score
a.1 Are the platform's (user) accounts related to a single identifiable natural person? a) Yes b) No	**1/0**
a.2 Are platform users from the same organisation identified and managed separately in terms of personal accounts of the platform? a) Yes b) No	**1/0**
a.3 Is a list of accounts not linked to natural persons available for the platform? a) Yes b) No	**0.5/0**
a.4 Is the list of non-personally identifiable accounts approved by a manager with an assigned responsibility for the concerned process of the platform? a) Yes b) No	**0.5/0**
a.5 Is access to the information stored in the platform based on business needs? a) Yes b) No	**1/0**
a.6 Is access to information stored in the platform based on "need to know" principle of the concerned operators? a) Yes b) No	**1/0**
a.7 Do you have a clear separation between the operational accounts and the administrative accounts of the platform? a) Yes b) No	**0.5/0**

a.8 Are administrative accounts capable to access only those information that they need to know and that they need to access in order to perform their duties? a) Yes b) No	**0.5/0**
a.9 Do the system administrators of the platform have personal accounts with limited user rights to perform tasks in the scope of operational business activities on the need (e.g. testing and verifying coherence of any change to the platform)? a) Yes b) No	**0.5/0**
Maximum points per this domain/ Total Pass Mark per this domain:	**6.5/4**

24. Asset Management **Rationale:** The organisation should maintain an **up-to-date inventory of IT assets** containing sufficient information (including assets' sensitivity marking and asset owners) to uniquely identify and locate each IT asset and to ensure its usage is compliant with legal and contractual requirements (Sys licenses, document copyright, design rights, etc.). Phases of the implementation of **IT asset management** should include controls ensuring that deployment into production or removal from use does not increase IT security risks beyond the acceptable threshold. **Monitoring performance and preparing remediation plans** (including additional IT asset assurance) to mitigate risks related to technical failures should be in place. **Vulnerabilities of IT systems** should be regularly **monitored** based on IT system sensitivity marking and risk assessment.	
	Score
a.10 Does your organization maintain an up-to-date inventory of the platform's IT assets containing sufficient information (including assets' owners and sensitivity marking) to uniquely identify and locate each IT asset? a) Yes b) No	**1/0**
a.11 Do you have documented procedures in order to manage intellectual property rights e.g. the inventory checks ensuring that usage of platform's IT assets is compliant with legal and contractual requirements such as valid software licenses, document copyright, design rights, etc.? a) Yes b) No	**1/0**
a.12 Does your organization maintain vendor software installed at the level (version) supported or suggested by the supplier for the specific business needs? a) Yes b) No	**0.5/0**
a.13 Does your organization allow exceptions approved by the IT asset owner in case that vendor software installed is not at the level (version) supported or suggested by the supplier for the specific business needs? a) Yes b) No	**0.5/0**
a.14 Are the security configuration baselines of the platform's IT systems determined and documented? a) Yes b) No	**1/0**
a.15 Do the security configuration baselines consider the industry good practice?	**0.5/0**

a) Yes b) No	
a.16 Are you controlling the implementation lifecycle of IT assets in order to prevent that its' deployment in the production does not increase IT security risk beyond the acceptable threshold? a) Yes b) No	**1/0**
a.17 Do you have a process to guarantee that if an IT asset is removed from usage (e.g. destroyed) that any sensitive or personal information on that asset cannot be retrieved? a) Yes b) No	**0.5/0**
a.18 Do you perform regular vulnerability checks of the platform's IT systems? a) Yes b) No	**0.5/0**
a.19 Are the vulnerability checks of the platform's IT systems followed by the identification of remediation measures, their planning and monitoring based on IT system sensitivity marking and risk assessment? a) Yes b) No	**1/0**
a.20 Are the networks used by the platform segregated based on trust level and need to know principle taking into account sensitivity marking and risk scenarios? a) Yes b) No	**1/0**
a.21 Do you have measures in place related to monitoring the platform's IT system performance/capacity? a) Yes b) No	**0.5/0**
a.22 Do you have measures in place alerting in case of reaching pre-defined critical values of the platform's IT system operations? a) Yes b) No	**1/0**
a.23 Are the procedures and operational instructions describing emergency procedures in case of errors or failures of an IT asset of the platform documented and known to the relevant organization roles? a) Yes b) No	**1/0**

a.24 Do you have in place appropriate plan and measures to mitigate risks related to technical failures of the platform's IT system (e.g. the alternative additional assets or secondary site or other appropriate contingency measure)? a) Yes b) No	**1/0**
Maximum points per this domain/ Total Pass Mark per this domain:	**12/6**

25. Business Continuity Management

Rationale: Booking platforms shall consider existing business requirements and objectives in the process for the determination of the recovery time objective (RTO).
The organisation shall define and document a backup policy, taking into account risk analysis and requirements regarding the completeness of data. Each platform shall implement, monitor and test backup arrangements to ensure completeness of data. In the case of a severe incident, the platform will re-establish processes and services as soon as possible and according to pre-defined service priority.
The organisation shall identify, quantify and qualify the **business impacts of a loss, interruption or disruption** of business processes on the organisation and collect information from which appropriate continuity strategies can be determined.
The organisation shall prepare a **continuity strategy** to ensure the protection of the ability to provide the services for which the platform is meant to be used. The strategy shall include all resources necessary to ensure business continuity that were revealed during the business impact assessment including: people and knowledge, premises, information, IT capabilities, suppliers, stakeholders, communication channels.
The organisation shall prepare and implement **plans, measures** and needed resources to enable the organisation to manage an interruption, whatever its cause.
An out of date Business Continuity (BC) plan without regular exercise has no value and could result in damage additional to the damage caused by the original incident. The organisation shall prepare and exercise a test plan for the BC plan, review and maintain a BC plan and improve the BC programme based on review reports, test results and lessons learned from real incidents.
The successful establishment of a **Business Continuity Management (BCM)** within the organisation depends on its integration into the business culture. The organisation shall regularly identify gaps between the current and target levels of awareness and commitment to BCP, and provide education and training to close the identified gaps.

	Score
a.25 Have you established a procedure/process to define the Recovery Time Objective for the main business objectives of the concerned platform? a) Yes b) No	**1/0**
a.26 Have you determined the Recovery Time Objective for the main business objectives of the concerned platform? a) Yes b) No	**1/0**
a.27 Does the determined Recovery Time Objective take into consideration requirements imposed by the business (of the platform)? a) Yes b) No	**1/0**
a.28 Do you have a backup policy, which takes into due consideration risk analysis and completeness of the information handled by the platform? a) Yes	**1/0**

b) No	
a.29 Do you have a backup plan, which implements the backup policy referred at the point before? a) Yes b) No	**0.5/0**
a.30 Is the backup plan defined and fully implemented as planned? a) Yes b) No	**1/0**
a.31 Do you regularly monitor the implementation of the backup plan (of the platform)? a) Yes b) No	**0.5/0**
a.32 Do you regularly test the backup plan of the platform making sure that data sets and recovery can assure availability, integrity and confidentiality of the concerned data? a) Yes b) No	**1/0**
a.33 Do you have procedures to verify completeness and recovery of data after a failure of the system of the platform? a) Yes b) No	**0.5/0**
a.34 Do you have procedures to verify and recover business after an incident based on priorities linked to the platform functionalities? a) Yes b) No	**0.5/0**
a.35 Do you have procedures to identify, quantify and qualify business impacts of a loss, interruption or disruption of business processes and their impact on your business and on the business of your stakeholders (business means the business ran by the platform)? a) Yes b) No	**0.5/0**
a.36 Have you defined a Business Continuity Strategy specific for your platform? a) Yes b) No	**1/0**
a.37 Have you documented a Business Continuity Strategy specific for your platform? a) Yes b) No	**0.5/0**

a.38 Does the Business Continuity Strategy for your platform clearly mention the resources (financial, human, knowledge, skills or of any other kind) which shall be used in order to implement the strategy? a) Yes b) No	**1/0**
a.39 Is the Business Continuity Strategy built as the result of a preliminary Business Impact analysis? a) Yes b) No	**1/0**
a.40 Did you develop a Business Continuity Plan for each of the critical functions related to your platform which includes also the resources and their usage? a) Yes b) No	**0.5/0**
a.41 Do you regularly test the Business Continuity Plans defined at the previous point (at least yearly, or more often)? a) Yes b) No	**0.5/0**
a.42 Do you have and do you regularly update the Test Plan for the Business Continuity Functions? a) Yes b) No	**0.5/0**
a.43 Following a test, do you revise, update, and re-validate the Business Continuity Plan of the platform or the part concerned by the test? a) Yes b) No	**0.5/0**
a.44 Do you keep records (reports, any proof which may testify the existence and execution) of the Business Continuity Plan Tests of the platform and of their results? a) Yes b) No	**1/0**
a.45 Do you keep records of the incidents related to business continuity of the platform? a) Yes b) No	**1/0**
a.46 Do you have a process to analyse business continuity incidents of the platform and to make sure that they could not repeat or that their impact would be properly mitigated? a) Yes b) No	**1/0**

a.47 Do all people working on the platform receive a specific Business Continuity Training? a) Yes b) No	**1/0**
a.48 Do you have a specific training and awareness program for Business Continuity of the platform for the staff working on the platform and for the platform activities, more in general? a) Yes b) No	**0.5/0**
a.49 Have you set a process to review the effectiveness of Business Continuity training and awareness? a) Yes b) No	**0.5/0**
Maximum points per this domain/ Total Pass Mark per this domain:	**19/9**

26. Change Management **Rationale:** To determine the **impact on business processes and IT services and to minimise the risk of possible adverse effects on the operational environment**, all change requests should be logged, prioritised, categorised and assessed. Only authorised changes should be planned and scheduled for implementation. Stakeholders should have the possibility to propose changes as well as have a reasonable time for transition. As a consequence and result of the change, the stakeholders shall receive training and support, especially during the transition phase, .	
	Score
a.50 Does your platform follow a transparent and documented change management process for the implementation of improvements and changes? a) Yes b) No	**1/0**
a.51 Is there any change approval body that supervises changes and improvements of the platforms' IT system? a) Yes b) No	**1/0**
a.52 Do stakeholders have the possibility to propose a change or an improvement? a) Yes b) No	**1/0**
a.53 Does composition (membership) of the change approval body allow that stakeholders participate in the decision-making process (prioritization and approval)? a) Yes b) No	**0.5/0**
a.54 Are the changes approved by the change approval body the only changes approved for implementation in the system of the platform? a) Yes b) No	**1/0**
a.55 Are there exceptions to the fact that the changes approved by the change approval body are the only ones approved for implementation in the system? a) Yes (0) b) No (0.5)	**0/0.5**
a.56 Is the emergency change implementation documented and controlled by a specific process for the platform? a) Yes b) No	**1/0**

a.57 Are the change approval body members (or chair) always informed about emergency changes prior to their implementation on the platform? a) Yes b) No	**0.5/0**
a.58 Are stakeholders always timely informed and/or instructed about emergency or other changes implementation plan and their impacts in case it may affect the platform? a) Yes b) No	**1/0**
a.59 Does a change implementation plan for the platform exists (or any other equivalents document(s) related to medium and major system changes) covering implementation, acceptance criteria and testing of changed? a) Yes b) No	**0.5/0**
a.60 Does a tracking and/or reporting change management system exist for the platform, which allows an insight of the process (from planning to post implementation review) as well as provides visibility on the decision making reasoning concerning proposed/implemented or rejected changes? a) Yes b) No	**0.5/0**
Maximum points per this domain/ Total Pass Mark per this domain:	**8.5/6**

27. Cryptography **Rationale:** Based on risk assessment and the sensitivity level of information, the **required level of protection** shall be ensured using encryption of information. An appropriate key length and hash size shall be selected based on good practice, depending on the algorithms used. Encryption key management shall be implemented to ensure that **data can be decrypted** when access to data is necessary. To ensure effective use of cryptography for security, proper management of cryptographic keys shall be established. **Security of information protected by cryptography** depends on the strength of the keys and protection afforded to the keys. All keys shall be protected against modification, unauthorised use and disclosure. Key management shall ensure secure generation, storage, distribution, and destruction of keys. Users' awareness and responsibilities regarding the importance of keeping their keys secure shall be ensured.	
	Score
a.61 Do you evaluate the use of encryption to information based on a proper risk assessment and depending on the sensitivity of information and on the required level of protection of the platform? a) Yes b) No	**1/0**
a.62 Have you documented and implemented a governance for the use of cryptographic artefacts of the platform? a) Yes b) No	**1/0**
a.63 Do you have specific standards for the use of cryptographic artefacts on the platform, which are based on existing best practices (e.g. declaring the minimum key length, hash size, algorithms to be used, and any other information to avoid the use of any weakly encrypted information)? a) Yes b) No	**0.5/0**
a.64 Have you established key management mechanisms (composed of both technical and organisation measures) which can ensure that data can always be decrypted when access to platform data is necessary by authorised parties? a) Yes b) No	**1/0**
a.65 Is the encryption key management system applicable for the platform duly protected in order to allow access only to authorised people and to those who need to access? a) Yes b) No	**0.5/0**
a.66 Are the encryption keys protected by mechanisms to avoid their modification and unauthorised use? a) Yes	**0.5/0**

b) No	
a.67 Do you have systems and procedures to generate, store, distribute and erase safely and securely encryption keys used to protect platform data? a) Yes b) No	**1/0**
a.68 Do you have an awareness and training programme for the use of encryption in your platform for your staff and for the stakeholders using your platform? a) Yes b) No	**0.5/0**
Maximum points per this domain/ Total Pass Mark per this domain:	**6/3**

28. Exception Management **Rationale:** To ensure **proper identification, assessment, approval and follow-up of information security exceptions** to the information security policy requirements. A formal approval process shall be defined, documented and implemented. Approval levels for different types of information security exceptions shall be defined. All exceptions to the information security policy shall be identified and recorded. A request for information security exception shall be based on business reasons. Information security exceptions shall be **based on a clear business reason** where there is a lack of alternatives. Risks arising from the information security exception shall be assessed. Potential compensating controls shall be considered and if feasible implemented before the information security exception approval. All information security exceptions are temporary only and shall be **approved** at the appropriate level. Organisations shall be informed about information security exceptions if such information is necessary to take countermeasures to mitigate the risk arising from such exceptions and if doing so does not increase the risk. Information security exception expiration shall be **monitored on a regular basis**. An information security exception is closed on its expiration date or by announcement by the requester that the exception is no longer needed. It is possible to reapply for the same information security exception after expiration.	
	Score
a.69 Have you established a proper and formal approval process for any exception to the information security policies regulating information security of your platform? a) Yes b) No	**1/0**
a.70 Following the previous point, is there a process in place to document and implement the exception(s)? a) Yes b) No	**1/0**
a.71 Does the exception approval path take into consideration the potential impact of the exception and the risks generated by having the exception in place? a) Yes b) No	**0.5/0**
a.72 Do you document exceptions in writing (for the platform)? a) Yes b) No	**0.5/0**
a.73 Are exceptions allowed for business reasons? a) Yes b) No	**1/0**
a.74 Do you evaluate and assess in writing the risks arising from an exception? a) Yes	**0.5/0**

b) No	
a.75 In case of an exception, do you consider the possibility and feasibility of compensating controls? a) Yes b) No	**0.5/0**
a.76 Can exceptions be permanent? a) Yes b) No	**0.5/0**
a.77 Shall the exceptions be approved by an internal person accountable for the platform? a) Yes b) No	**1/0**
a.78 Do you inform Staff and Stakeholders of the exceptions and of the countermeasures and mitigating controls in place in order to reduce the risks? a) Yes b) No	**1/0**
a.79 Is the expiration date of an exception regularly monitored (for the platform)? a) Yes b) No	**0.5/0**
a.80 Is the closure of an exception communicated to the Staff and, where applicable, to all the stakeholders of the platform? a) Yes b) No	**0.5/0**
a.81 Is it possible to prolong the expiration date of an **Exception** after its natural expiration? a) Yes b) No	**0.5/0**
Maximum points per this domain/ Total Pass Mark per this domain:	**9/4**

29. HR/Organizational Context **Rationale**: The organization has implemented the quality and security management system in the business operations and has in place **appropriate measures for quality and security management** assurance including appropriately **selected or trained and informed human resources**.	
	Score
a.82 Is your quality management system established, and does it include a description of the platform processes and their sequence and interaction? a) Yes b) No	**1/0**
a.83 Is within your organizational context quality and security management embedded into routine business operations that cover the platform? a) Yes b) No	**0.5/0**
a.84 Has the highest decisional level of the platform taken accountability for the effectiveness of the quality management system? a) Yes b) No	**1/0**
a.85 Do you have a general strategy for the platform, which takes into consideration the inputs from all customers and stakeholders? a) Yes b) No	**0.5/0**
a.86 Has the organisation determined and provided the resources needed for the establishment, implementation, maintenance and continual improvement of the quality and security management system (including people, environmental and infrastructure requirements) in use for the platform operations? a) Yes b) No	**1/0**
a.87 Has the organisation ensured that those persons who can affect the performance of the quality and security management system are competent on the basis of appropriate education, training, or experience or taken action to ensure that those persons can acquire the necessary competence? a) Yes b) No	**1/0**
a.88 Has the organisation ensured that a natural person for a specific information security or business role with information security requirements can be trusted to take on these roles? a) Yes b) No	**1/0**

a.89 Has the organisation ensured that information security requirements and responsibilities, including the responsibilities and duties that remain valid after termination or change of employment, are defined and communicated to the relevant person prior to handing over security related tasks? a) Yes b) No	**1/0**
Maximum points per this domain/ Total Pass Mark per this domain:	**7/5**

30. Incident Management **Rationale:** The responsibilities and procedures for incident management and information security incident **reporting, logging, assessing, responding to, dealing with, and learning** from it shall be **clearly defined, documented and implemented**.	
	Score
a.90 Have you defined, documented and implemented **an incident management system** that includes incident logging, assessing, prioritization, responding to, dealing with it and learning from it? a) Yes b) No	**1/0**
a.91 Have you determined what needs to be monitored and measured (including methods, analysis and evaluation) to ensure an efficient incident management system of your platform is established? a) Yes b) No	**1/0**
a.92 Are the procedures and operational instructions describing emergency procedures in case of errors or major failures of the platform's IT system documented and available to the responsible people? a) Yes b) No	**1/0**
a.93 Have you established a **security incident prevention procedure** which includes a categorisation of the information security incident types (taking into account the incident severity level)? a) Yes b) No	**1/0**
a.94 Do you maintain an information **security incident register** or equivalent document(s) containing the information about events, assessments, decisions, response plans, post-implementation analyses and review? a) Yes b) No	**1/0**
a.95 Has the organisation determined and implemented measures for the continual improvement of the incident and in particular security incident management process? a) Yes b) No	**1/0**
Maximum points per this domain/ Total Pass Mark per this domain:	**6.0/4**

31. Information Management

Rationale: To ensure an appropriate level of protection, all **information shall be assigned a level of sensitivity**. In accordance with the sensitivity marking scheme, procedures for information labelling and information handling shall be developed and implemented.

All information shall be **identified, inventoried and an information owner shall be allocated**. The information owner shall be responsible to designate the sensitivity level of information and for the protection of information throughout the entire information life cycle.

Procedures for information labelling and information handling shall be developed and implemented in accordance with the sensitivity marking. Rules of acceptable use shall be defined, documented and implemented for all information.

When information is no longer in use, it shall be retained or eliminated according to legal, regulatory or business requirements. **Protection of information** according to the information sensitivity level shall be ensured in archiving and in the disposal of information.

To ensure an appropriate level of information protection, all media containing information shall be assigned a level of sensitivity. In accordance with the sensitivity marking scheme, procedures for labelling and handling removable media in use, transit and disposal shall be defined and documented, implemented and monitored.

	Score
a.96 Are all information sets listed in an information asset inventory which allows also to identify them and their location? a) Yes b) No	**1/0**
a.97 Are all information in the information asset inventory assigned with a specific level of sensitivity? a) Yes b) No	**1/0**
a.98 Is the information owner identified for each information set? a) Yes b) No	**1/0**
a.99 Has the information owner assigned the sensitivity level to the information s/he owns? a) Yes b) No	**1/0**
a.100 Is the process of sensitivity assignation revised regularly by the information owner through a documented process? a) Yes b) No	**0.5/0**
a.101 Does a procedure exist for labelling information based on sensitivity of the information and is it implemented?	**1/0**

c) Yes d) No	
a.102 Does a procedure exist for handling information based on sensitivity of the information and is it implemented? a) Yes b) No	**0.5/0**
a.103 Are rules for acceptable use of information defined, documented and implemented separately for each information set, based on its sensitivity? a) Yes b) No	**0.5/0**
a.104 Do rules exist for the dismissal of information based on legal, regulatory or business requirements? a) Yes b) No	**0.5/0**
a.105 Are rules for the dismissal of information based on legal, regulatory or business requirements, implemented? a) Yes b) No	**0.5/0**
a.106 Do rules exist for protecting archived information based on sensitivity, legal, regulatory or business requirements? a) Yes b) No c)	**0.5/0**
a.107 Are rules for protecting archived information based on sensitivity, legal, regulatory or business requirements, also implemented? a) Yes b) No	**0.5/0**
a.108 Are all media containing information designated in terms of level of sensitivity based on the sensitivity marking scheme? a) Yes b) No	**1/0**
a.109 Do procedures exists for labelling and handling removable media in use, transit and disposal and are they documented based on the sensitivity marking scheme? a) Yes b) No	**1/0**
a.110 Are the procedures for labelling removable media in use, transit and disposal implemented based on the sensitivity marking scheme? a) Yes	**0.5/0**

b) No	
a.111 Are there procedures for handling removable media in use, transit and disposal regularly monitored based on the sensitivity marking scheme? a) Yes b) No	**0.5/0**
Maximum points per this domain/ Total Pass Mark per this domain:	**11.5/6**

32. Log Management **Rationale:** The organisation shall **develop policies** related to log management covering: responsibilities, log generation, log protection, log analysis, log preservation and disposal. The organisation shall plan, implement and maintain IT infrastructure with a **capability to generate, transmit, store and dispose of log information**. The infrastructure shall support the security and analysis of logged records. Controls shall be designed and implemented to provide protection and ensure accountability of privileged users.	
	Score
a.112 Do you have a policy or more policies related to the management of logs of your platform covering at least: log generation, log protection, log analysis, log preservation and disposal? a) Yes b) No	**1/0**
a.113 Are responsibilities related to logs identified and communicated to all involved parties in the information security management of your platform? a) Yes b) No	**1/0**
a.114 Have you planned and implemented the Log Policies? a) Yes b) No	**1/0**
a.115 Do you regularly revise and maintain Log Management functionality of your platform? a) Yes b) No	**0.5/0**
a.116 Does your platform allow keeping logs in a secure way through technical and/or organisational security measures? a) Yes b) No	**0.5/0**
a.117 Does your platform allow analysing logs through proper technical means or through documented and well-disseminated processes? a) Yes b) No	**0.5/0**
a.118 Have you established rules to prevent log manipulation by administrative or any other class of users? a) Yes b) No	**0.5/0**

a.119 Have you allocated responsibilities in order to prevent that any user with administrative rights may abuse of her/his rights in respect to systems for which he/she may also be an end user? a) Yes b) No	**0.5/0**
a.120 Have you put in place controls which would allow to monitor or eventually to detect in due time any abusive access to logs or any alteration to logs? a) Yes b) No	**0.5/0**
a.121 Have you provided training and awareness to actors involved in the application of the Log Policies? a) Yes b) No	**0.5/0**
Maximum points per this domain/ Total Pass Mark per this domain:	**6.5/3**

33. Physical Security **Rationale:** Physical security perimeters, taking into account the **sensitivity marking of information and risk analysis**, shall be defined to protect areas containing sensitive information and equipment from unauthorised access, prevent physical damage and protect against environmental threats. **Adequate controls** shall be selected, documented and implemented for each security perimeter depending on the sensitivity of information and equipment located within the perimeter. The **management of access rights** to access the security perimeters shall be established and implemented. Access to security perimeters, containing sensitive information and equipment, shall be restricted on a "need to be" basis. Requirements to establish **acceptability of equipment** in the specific security perimeter must be established. Procedures to check equipment and their configuration upon entry into security zones, managing sensitive information and equipment shall be implemented. Before moving equipment among security zones, information stored shall be checked and removed from equipment. **Control over all activities within a security perimeter** shall be designed, implemented and communicated.	
	Score
a.122 Have you defined and marked physical security perimeters for the platform, taking into account the sensitivity marking of information and a proper risk analysis? a) Yes b) No	**1/0**
a.123 Are physical perimeters surrounded by access control systems or any other measure capable to grant access to the platform only to those people who are authorised to process and manage the specific information in the specific area? a) Yes b) No	**1/0**
a.124 Are security measures identified in order to protect the areas inside the security perimeters of the platform against environmental threats based on proper risk analysis? a) Yes b) No	**1/0**
a.125 Are additional security controls established for the platform depending on the sensitivity of information and equipment located within the perimeter and the risks related to the information? a) Yes b) No	**0.5/0**
a.126 Are the procedures for the management of access rights of the platform documented, implemented and, when executed, duly recorded? a) Yes b) No	**1/0**

a.127 Is access to the areas containing sensitive information for the platform subject to a strict "need to be" basis? a) Yes b) No	**1/0**
a.128 Are processes and procedures for the acceptance of technical equipment in the specific security perimeter established and implemented? a) Yes b) No	**0.5/0**
a.129 Is every piece of equipment and its configuration checked and inspected prior its admission to any inner part of a Security Perimeter containing sensitive information through a documented procedure? a) Yes b) No	**0.5/0**
a.130 Do you perform and document checks and/or inspections on devices potentially containing information assets accessing or leaving a secure area where your platform is physically located (meaning in the server rooms)? a) Yes b) No	**0.5/0**
a.131 Are information assets properly removed and then cross checked in a documented manner from any device which leaves any secure perimeter for the platform? a) Yes b) No	**0.5/0**
a.132 Are specific controls within specific security perimeters documented (e.g. Access Control, CCTV and others)? a) Yes b) No	**1/0**
a.133 Are specific controls within specific security perimeters executed? a) Yes b) No	**1/0**
a.134 Are specific controls within specific security perimeters monitored? a) Yes b) No	**0.5/0**
a.135 Are staff and stakeholders of the platform informed of controls performed within the different security perimeters? a) Yes b) No	**0.5/0**

Maximum points per this domain/ Total Pass Mark per this domain:	**10.5/5**

34. Risk Management **Rationale:** The purpose of information security risk management is to support the development and operation of the booking platform in the sense that **it involves the organization in identifying, assessing, and treating risks to the confidentiality, integrity, and availability of an organization's assets**. The risk management methodology should be based on an international or national standard or good practice and shall address risk management criteria.	
	Score
a.136 Does the platform use a risk management methodology based on an international standard or good practice addressing basic criteria such as: risk evaluation criteria, risk impact criteria, risk acceptance criteria, gap analysis etc.? a) Yes b) No	**1/0**
a.137 Does your organization maintain an information security risk assessment matrix or equivalent document containing also risks associated to the platform? a) Yes b) No	**1/0**
a.138 Do the existing measures in place with respect to the platform ensure that acceptable risk levels correspond to the referenced risk acceptance criteria? a) Yes b) No	**1/0**
a.139 Are all the risks with regard to the threats and vulnerabilities of the platform's IT assets and operations identified and risks assessed according to a predefined and documented methodology for risk assessment? a) Yes b) No	**1/0**
a.140 Are you implementing all remedial actions according to the risk treatment plan in case of unacceptable risks? a) Yes b) No	**1/0**
a.141 Do you perform remedial measures for the unacceptable risks in a period of less than a year from the logging? a) Yes b) No	**0.5/0**
a.142 Do you regularly re-assess organizational and infrastructure risks related to the platform's activities? a) Yes b) No	**1/0**

Maximum points per this domain/ Total Pass Mark per this domain:	**6.5/5**

35. Service Provider Management **Rationale: Information security requirements/assessment** should be included in service requirements definition as part of a request for tender or a request for service**. Metrics and performance indicators should be defined** for the purpose of provider selection and subsequent service monitoring to ensure that the requirements are met. **Service Level Agreements shall include information security requirements** and should be part of the contract.	
	Score
a.143 Are the information security requirements included in each service requirements' definition as part of a request for service for outsourced activities of your platform? a) Yes b) No	**1/0**
a.144 Does the selection procedure for the service providers for the platform include a service provider assessment (including appropriate information security assessment)? a) Yes b) No	**1/0**
a.145 Are the relevant metrics and performance indicators defined for the purpose of the platform service provider selection as well as the subsequent service monitoring in order to ensure that service provider complies with the requirements? a) Yes b) No	**0.5/0**
a.146 Does a service level agreement with every platform service provider establish a common understanding about the services supplied and their intended quality and information security requirements? a) Yes b) No	**0.5/0**
a.147 Do you have the right to audit or to request a third party audit which as the scope to audit the service provider, the provided services, its premises, processes and performances? a) Yes b) No	**0.5/0**
a.148 Are the security requirements (in the Service Level Agreement), reporting and monitoring mechanisms an integral part of the contract between you and the platform service provider for the platform? a) Yes b) No	**0.5/0**

a.149 Does the platform service provider regularly deliver reports on service performance and report on indicators defined in the service description? a) Yes b) No	**0.5/0**
a.150 Does your organization regularly supervise, review and monitor the activity of the service platform provider (outsourced)? a) Yes b) No	**1/0**
a.151 Does your organization ensure that an appropriate level of information security awareness and needed knowledge (including responsibilities and duties that remain valid after termination of the contract or change of the service provider) is defined and communicated to the service provider and to their staff (outsourced staff on/off site) during the contract execution, the transition-in or transition-out periods? a) Yes b) No	**1/0**
Maximum points per this domain/ Total Pass Mark per this domain:	**6.5/4**

36. System Development Lifecycle **Rationale:** To ensure that information systems and services security shall be addressed properly, information security related requirements shall be included in the requirements for **new information systems or enhancements to existing information systems**. **Principles and rules for the development process** shall be defined, documented and applied during any information system implementation efforts. To minimise the risk of the negative impact of changes within the development lifecycle, formal change control procedures shall be used. **Appropriate security** of development environments for system development and integration shall be ensured. An appropriate level of separation of development, testing and operational environments shall be ensured. **Testing of security functionality** shall be carried out during development. Acceptance criteria shall be defined, and testing performed, for new information systems, upgrades and new versions. In the event that operational data shall be used for testing purpose, controlled procedures shall be used and appropriate protection shall be ensured.	
	Score
a.152 Are information security requirements included in the requirements for new platform developments? a) Yes b) No	**1/0**
a.153 Are enhancements to information security requirements included in all developments? a) Yes b) No	**1/0**
a.154 Are principles and rules for the development process defined at platform level? a) Yes b) No	**0.5/0**
a.155 Are principles and rules for the development process documented at platform level? a) Yes b) No	**1/0**
a.156 Are principles and rules for the development process applied for any platform development activity? a) Yes b) No	**1/0**
a.157 Have you adopted formal change control procedures? a) Yes b) No	**0.5/0**
a.158 Do you apply the adopted change control procedures?	**0.5/0**

a) Yes b) No	
a.159 Do you provide to all platform staff awareness raising and training about the adopted and applicable change control procedures? a) Yes b) No	**0.5/0**
a.160 Is an appropriate security of the development environments for platform system development and integration ensured through their separation? a) Yes b) No	**1/0**
a.161 Is there an appropriate level of separation of platform development, testing and operational environments? a) Yes b) No	**0.5/0**
a.162 Is testing of security functionality performed already during development? a) Yes b) No	**1/0**
a.163 Are acceptance criteria for security testing defined prior the testing of security functionalities? a) Yes b) No	**1/0**
a.164 Are tests for security functionalities performed, for new information systems, upgrades and new versions? a) Yes b) No	**1/0**
a.165 In the event that operational data shall be used for testing purposes, are there controlled procedures to use those data for testing in a controlled environment? a) Yes b) No	**0.5/0**
Maximum points per this domain/ Total Pass Mark per this domain:	**11/6**

37. Teleworking for platform employees having administrative roles on the platform

Rationale: Threats regarding premises, network, IT systems and clients not under the control of the organisation shall be assessed under the assumption that no controls are implemented except in the case that credible assurance of the contrary is provided.
The organisation shall **develop policies and instruction related to remote access and teleworking** covering: responsibilities, access requirements, including permitted access methods (technologies), permitted clients, access rules (e.g. combining level of access, clients, etc.), access granting criteria and instructions for remote access and teleworkers.
The organisation shall **plan, implement, maintain and monitor remote access infrastructure** capable of ensuring compliance with the policy requirements.

	Score
a.166 Do you have a policy in place covering telework or remote access to the platforms from outside the premises? a) Yes b) No	**1/0**
a.167 In such a policy, do you mention responsibilities, access requirements, including allowed technologies, access rules and access granting criteria? a) Yes b) No	**1/0**
a.168 In such a policy, do you have processes to grant, monitor and revoke remote access to the platform resources? a) Yes b) No	**1/0**
a.169 Do you plan, implement, and maintain monitoring of the remote access infrastructure? a) Yes b) No	**1/0**
a.170 Do you provide awareness and training to the users who may aim to request, or who may have obtained the use of Remote Access, prior to opening the remote access? a) Yes b) No	**0.5/0**
a.171 Do you have documentation and information related to the use and to the acceptable use of Remote Access for the platform? a) Yes b) No	**0.5/0**
Maximum points per this domain/ Total Pass Mark per this domain:	**5/3**

38. Secure platform access for network users **Rationale:** Available data security protocols in place for network user access	
	Score
a.172 Does your platform offer a Secure Connection? a) Yes b) No	**1/0**
a.173 Does your platform offer secure authentication? a) Yes b) No	**1/0**
a.174 Does your platform offer multi-factor authentication? a) Yes b) No	**1/0**
a.175 Does your platform enable to use standards for Secure Connections and Secure Authentication? a) Yes b) No	**1/0**
a.176 Does your platform uses secure network protocols in all levels of its architecture? a) Yes b) No	**0.5/0**
a.177 Does your platform use secure authentication protocols in all levels of its architecture? a) Yes b) No	**0.5/0**
a.178 Do you apply the AS4 protocol and the Edig@s-XML (or equivalent) format for document based data exchange for the platform? a) Yes b) No	**0.5/0**
Maximum points per this domain/ Total Pass Mark per this domain:	**5.5/3**

39. Peak service load **Rationale:** IT Infrastructure capacity available and used, and scalability of IT infrastructure to deal with a high amount of transactions, users, etc.	
	Score
a.179 Have you stipulated specific metrics to evaluate the compliance of your system with expected technical and performance requirements of your platform users (e.g. response time per transaction)? a) Yes b) No	**1/0**
a.180 Can your platform scale adding more devices to the existing architecture? a) Yes b) No	**1/0**
a.181 Can your platform scale virtually (increasing resources assigned to the already existing virtual machines, if any)? a) Yes b) No	**1/0**
a.182 Is your platform designed to scale horizontally? a) Yes b) No	**0.5/0**
a.183 Is your platform designed to scale vertically? a) Yes b) No	**0.5/0**
a.184 Is your platform highly available and fault tolerant? a) Yes b) No	**0.5/0**
a.185 Do you have information related to scalability percentage, and the underlining conditions and costs? a) Yes b) No	**0.5/0**
Maximum points per this domain/ Total Pass Mark per this domain:	**5/2**

40. Graphical user interface of the platform in English **Rationale:** Usability of the web front-end of the platform	
	Score
a.186 Does the graphical interface follow a best practice in terms of usability of the platform? a) Yes b) No	**1/0**
a.187 Can your user interface be customised based on the user profile and its skills, as well as based on the role s/he plays on the platform? a) Yes b) No	**1/0**
a.188 Is usability of the user interface subject to testing by regular users prior to adoption? a) Yes b) No	**1/0**
a.189 Do you do regular revision of usability of your platform through questionnaires or other ways to involve stakeholders? a) Yes b) No	**1/0**
a.190 Does your graphical interface offer an on-line contextual help which can guide inexperienced end-users? a) Yes b) No	**0.5/0**
a.191 Does your graphical interface allow to be tailored to the desire of the end user (e.g. selecting plug-ins, widgets or any other kind of removable/additional tool-set)? a) Yes b) No	**0.5/0**
a.192 Is your graphical user interface offered in English? a) Yes b) No	**1/0**
Maximum points per this domain/ Total Pass Mark per this domain:	**6/3**

41. Helpdesk availability (outside business hours) **Rationale:** Technical and business support available 24/7. The Technical and business support is provided in English.	
	Score
a.193 Is the platform's technical helpdesk available 24/7? a) Yes b) No	**1/0**
a.194 Is the platform's business helpdesk/support available 24/7? a) Yes b) No	**1/0**
a.195 Do you have metrics in place (eventually included also in a Standard Level Agreement with the platform users) to monitor the performances of the technical helpdesk of the platform? a) Yes b) No	**0.5/0**
a.196 Do you have metrics in place (eventually included in a Standard Level Agreement with the platform users) to monitor the performances of the business helpdesk/support of the platform? a) Yes b) No	**0.5/0**
a.197 Is platform's technical helpdesk available in English? a) Yes b) No	**1/0**
a.198 Is the platform's business helpdesk/support available in English? a) Yes b) No	**1/0**
a.199 Is the platform's business helpdesk/support available in more than one EU Official Language? a) Yes b) No	**0.5/0**
Maximum points per this domain/ Total Pass Mark per this domain:	**5.5/3**