Third-Party Security Risk Assessment Questionnaire

Date of Completation of the Form :

Name of Company:

Company's Website:

Contact Person Completing the Assessment:

Email Address:

Phone Number:

Description of the Service/Product: *(Please provide information about of Hardware and Software in scope of this Collaboration (Domain Controller, Application Servers))*

Users of the System:

Technical Description (client, agent, SSL, FTP transmission, hosted website etc) :

Outsourced/Contracted Service Arrangements (eg. Onsite support, remote support, temporary access, database management etc,)

Select the appropriate answer from the drop down in the Response column, and provide a brief description in the Comments section.

	Security Assessment Questions	Response	Comments
Organisational Information Security			
1	Does your organization have written policies and procedures in relation to data privacy and information security? *If so, please specify the related Information Security Policies and Procedures in place and how frequently are those policies and procedures reviewed?* - Data breach reporting - Data retention and storage - Data subject rights - Information Security management - Information access management - Auditing & Monitoring Access - Physical Security/Facility Security - Incident Management - Opertational Security/Network Security - Information Classification and Handling - Mobile Device and Remote Access - Information Security Risk Management - Asset Management and Disposal - Sanction Policy		
2	Do you have a member of your organisation with dedicated information security duties? *If so, please provide the name and contact information.*		
3	Does the organisation have a data protection officer or someone else who has been designated to take responsibility for data protection? *If so, please provide the name and contact information.*		
4	Is a background check required for all employees accessing and handling our data? *If yes, please specify the contact's information (name,position, mail address, tel)?*		
5	Do all staff receive information on data privacy and security awareness training? *If yes, please respond how often in the comments field as well as when was the last training held?*		
6	Does the organization have a formal change control process for IT changes? *If yes, what are the steps involved?*		
7	Does the organisation implement an international standards such ISO 27001, ISO 20000, ITIL etc.? *If so, please provide a copy of certificates.*		
8	Does the organisation have Disaster Recovery and/or Business Continuity Plan? *If yes, please provide the list of scenarios covered by BCP and a copy of plan if possible.*		
9	Does the organisation test its recovery Plans? *If yes, please respond how often in the comments field as well as when was the last test held?*		
10	Does the organisation established qualitative targets, which must be in compliance with the other objectives?		
11	Does the organisation take measures to ensure that its ICT systems are adequately maintained and managed to provide the stable and expected operation?		
External Hosting and your 3d Parties			
12	Has the organisation provided the whole or part of its ICT activity (or of its systems) by the external service suppliers. *If yes, has the organisation perform and adopt procedures and controls which ensure the compliance with the requirements, on the security and well functioning of these systems?*		
13	Where does your organization store the personal information you are managing on our behalf? If stored with a third-party subprocessor? Note: *If answer to question 23 is "Third party sub-processor", please submitt the form to the Third party sub-processor for completition*		
14	Will Tirana Bank data be hosted at a hosting provider? *If yes , please provide the hosting service name and their certifications?*		
15	Do you perform periodic reviews of your third parties that have access to Tirana Bank data? *How often?*		
Physical Security			
16	Does the organisation own their own Data Center? *Where are the data data center located?*		
17	Does the organisation employ the physical security/perimeter controls in the data center ?		
18	Do the organisation have effective physical access controls (e.g., door lock, badge/electronic key ID and access controls) in place that prevent unauthorised access to facilitities and especially to data center?		

19	Has your organization defined and adopted **physical security controls** in the selection, planning, design and management of premises containing information assets? *If yes can you specify this controls? Ex. fire safety , temperaturem humidity, battery backup.*		
Data and Software Security			
20	Has your organisation implemented encryption for all transmission of sensitive/confidential information outside of your organisation's network? *How do you maintain the security of data in transit when it's being sent externally?*		
21	Do the software support encryption of data in motion (e.g., SSL, etc.)? *Please describe for each software in scope.*		
22	Do the software has documentation showing where all TB confidential data (if any) is stored in the application? *Please describe for each software in scope.*		
23	Do the software support encryption of data at rest (e.g., column-level encryption, etc.)? *Please describe for each software in scope.*		
24	Do all softwares or solutions that TB staff will use perform audit logging? *Please describe for each software in scope.*		
Patch Management			
25	Does the organisation review, test, and apply software patches on a regular basis? *If yes, how do you regularly evaluate patches and updates?*		
26	Do all system/ software/network devices that will be used by TB Staff (ex Windows OS, X application, routers firmware) have a security patch process? *Please describe organisation's software security patch process, frequency of security patch releases, and how security vulnerabilities are identified.*		
Risk Assessment/ Vulnerability Assessment and Penetration Testings/ Audits			
27	Does the organisation conduct risk analyses to ensure this risk is maintained within the accepted limits related to the entity activity? *If yes, indicate the last risk assessement and provide a copy?*		
28	When was the last time your organisation performed an internal/external technical vulnerability assessment or Penetration Testing? Was the assessment performed internally or by a 3rd party? *If so, please provide a copy or summary of the finidings.*		
29	Are systems that will be used by TB Staff tested during the last Vulnerabiliy Scanning/Penetration Testing?		
30	Are vulnerabilites High or Critical identified? *If yes, are all vulnerabilites remediated? In case of unfixed vulnerabilites, is there a documented treatment plan and timeframe of remediation?*		
31	Has your organisation undergone a formal audit within the last year? *If so, please provide a summary of the audit and results, to include findings and corrective action that still needs to be remediated.*		
Account Management and Access Control			
32	Does the organisation have an access controls in place? *If yes please describe in the comments:*		
33	How many Domain Administrators exist?		
34	Do generic accounts exist? *If yes , are their owners identified ?*		
35	Can default accounts and passwords be changed by your organization Group Administrators?		
36	Can service accounts be configured to run as non-privileged user (i.e. non-Domain Admin)?		
37	Do you have a process to review user accounts and related access?		
Network Infrastructure			
38	Are internal and external networks separated by firewalls with access policies and rules? Provide supporting documentation.		
39	Is there a standard approach for protecting network devices to prevent unauthorized access/network related attacks and data-theft (e.g. firewall between public and private networks, internal VLAN, firewall separation, separate WLAN network, secure portal, etc)		
40	Is antivirus software installed and running on your computers and supporting systems (e.g., desktops, servers, gateways, etc.)?		
41	Is this antivirus product centrally managed (e.g., is the antivirus monitored to verify all endpoints have functional agents, agents are up to date with the latest signatures, etc.)? *Please explain your policies and procedures for management of antivirus software.*		
42	Do you have any Intrusion Protection System (IPS) or Intrusion Detection System (IDS) for systems that the Bank will use?		
43	Are third party connections to your network monitored and reviewed to confirm only authorized access and appropriate usage (i.e. with VPN logs, server event logs, system, application and data access logging, automated alerts, regular/periodic review of logs or reports, etc.)?		
Incident Response			
44	Does the organisation have an incident response plan?		
45	Has the organisation ever experiences a breach of customer data? *If yes, please explain the extent of the breach and controls implemented to prevent features breaches?*		
46	In the last 12 months have you either reported an incident happened within your organization to the Commissioner of Data Protection or been subject to any action from the Commissioner? *If yes, please provide further information*		
47	Do you have in place technical and organisational measures to assist your clients with their obligations as a data controller in respect of Subject Access Requests and the other data subject rights under GDPR? *If yes, please provide further information including how quickly you are able to respond.*		