TIRANA BANK

Third-Party Risk Assessment Questionnaire

Date of Completation of the Form :

Name of Company:

Company's Website:

Contact Person Completing the Assessment:

Email Address:

Phone Number:

DISCLAIMER: Tirana Bank may request proof of declaration on any of the below self-declared questions during the initial or any ongoing evaluation of your company.

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	**Do you hold a valid information security/cybersecurity third-party attestation or certification?** (e.g., ISO 27001, SOC 2 Type 2, ISO 27018, ISO27701, PCI-DSS, Cybersecurity Maturity Assessment, etc.) If "yes" , please state the program and date that you were certified, and provide a copy of the certification.	Yes	
2	**Has your organization implemented an Information Security Management System (ISMS) aligned with international standards and best practices?** If yes, please specify which standard the ISMS is based on (e.g., ISO/IEC 27001), describe the related information security policies and procedures in place, and indicate how often they are reviewed in the Comments section	Yes	Internation Standard that ISMS is based: _____ Name of Information Security related policies / procedures: _____ Revision Cycle:
3	**Do you have a member of your organisation with dedicated information security duties?** *If so, please provide the name and contact information n the Comments session.*	Yes	Name:____ E-mail:____
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) in the Comments session.*	Yes	
5	**Do all staff receive 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.*	Yes	
6	Does the organization have a **formalized change management process**?	Yes	
7	Does the organisation have a **Disaster Recovery and/or Business Continuity Plan?** *If yes, explain in the comment session if the service provided to Tirana Bank are covered in BCP plans?* *Please provide in the comment session, the list of scenarios covered by BCP and a copy of plan if possible.*	Yes	
8	**Does the organisation periodically test its Recovery Plans?** *If yes, select how frequently.*	annually	
Physical Security			
9	**Does the organisation own their own Data Center?** *Present where are the data centers located in the Comments session.*		Primary Data Center Location:_____ DRS Location:_____
10	Does the organisation employ the **physical security/perimeter controls in the data center**? Are physical security controls defined and adopted 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.		
11	Does 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?		
Data and Software Security			
12	Is information security assessed in every stage of **Software Development LiveCycle (secure SDLC)**?		
13	Has your organisation implemented **encryption for all transmission of sensitive/confidential information** outside of your organisation's network?		
14	Has your organisation implemented **encryption at rest**? If yes, will Tirana Bank data be encrypted at rest?		
Patch Management			
15	Does the organisation **review, test, and apply software patches on a regular basis**? *If yes, describe in the Comments session how do you regularly evaluate patches and updates.*		
Risk Assessment/ Vulnerability Assessment and Penetration Testing/ Audits			
16	Does the organisation conduct **regular risk assessments** to ensure risks are identified and maintained within acceptable levels? *If yes, provide the date of the last risk assessement.*		Date of last risk assessment: _____
17	Do you regularly perform **internal/external technical vulnerability assessment or Penetration Testing**? *If yes, in the comments session provide when was the last date of such assessments/testing as well as whether it was performed internally or by a third party.*		Last date of vulnerab/pentest:_____
18	Are systems under the scope of the requested service/solution from Tirana Bank subject of testing during the last Vulnerabiliy Scanning/Penetration Testing?		
19	At the moment of this assessment are there uncorrected / pending critical or high level vulnerabilities related to systems under the scope of the request service / solution? *If yes, is there a documented treatment plan and timeframe of remediation?*		
20	**Has your organisation undergone a formal IT / Information Security audit within the last year?**		
Account Management and Access Control			
21	Does the organisation have an **access controls in place**? *If yes please describe in the comments session.*		
22	Do you perform **regular reviews of user accounts, inclouding service accounts and related access**?		
Network Infrastructure			
23	**Are internal and external networks separated by firewalls with access policies and rules**?		
24	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)		
25	**Is antivirus software installed and running on your computers and supporting systems** (e.g., desktops, servers, gateways, etc.)?		
26	**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.)?		
27	Do you have any **Intrusion Protection System (IPS) or Intrusion Detection System (IDS)**?		
28	**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			
29	**Does the organisation have an incident response plan?**	Yes	
30	**Has the organisation experienced a security breach or data leak during the last 2 years?** *If yes, explain in the comments session the extent of the breach and controls implemented to prevent features breaches.*		
Sub-contractors			
31	Do you rely on **any sub-contractor or third parties for any part of the service you will/are offering to Tirana Bank?** *If YES describe the service. (in case of"data hosting" services provide SUB-CONTRACTOR NAME & LOCATION)*		Service description: _____
32	Do you manage **supply chain risks** and have a plan in the event of disruption or failures?		
33	Do you conduct **due diligence on your sub-contractors or third party service providers?**		
34	Do you perform **periodic reviews of your sub-contractors or third party service providers?**		
Cloud Providers			
35	**Will Tirana Bank data be hosted at a Cloud provider?** *If yes, please provide the Cloud provider service name, the country that Tirana Bank data will be hosted and their certifications in the comments session.*	Yes	Cloud Provider Name: _____ Location:_____ Security Certifications: _____
36	**Is Tirana Bank data hosted in a multi-tenant environment?** I*f yes, please describe in the comments section how is data segregated between tenants?*	Yes	Data segregation description:_____
37	**Is your architecture designed for high availability and scalability?** *Please describe in the comments section what are your uptime/service level guarantees (SLAs).*		Uptime SLA:_____
Exit Strategy			
38	Do you ensure **data handover and a secured transition** upon service termination?		
39	Are Tirana Bank **data deleted** upon service termination?		
40	Are **backups also securely deleted** upon service termination?		
41	Will you assist with data migration or platform transition?		
42	Can the vendor provide a data desctruction certificate?		
Compliance			
43	**Does the organisation have a Data Protection Officer (DPO)** or someone else who has been designated to take responsibility for data protection? *If so, please provide the name and contact information in the Comments session.*		
44	If sensitive data is processed, are additional measures taken to protect it according to GDPR requirements?		
45	Is personal data transferred or processed outside the EU/EEA? If yes, are appropriate legal safeguards in place ((e.g SCCs, adequacy decision)?		
46	If data is transferred outside the EU, have you obtained prior authorization from the relevant Data Protection Authority, where required?		
47	Do you have internal policies and procedures in place to ensure GDPR compliance?		
48	Do you have a Data Processing Agreement (DPA) in place with your clients?		
49	Do you ensure that any subprocessors or third parties you engage are also GDPR compliant?		
50	**In the last 24 months have you either reported an incident happening within your organization to the Commissioner of Data Protection or been subject to any action from the Commissioner?** *If yes, please provide further information in the Comments session.*		
51	Do you have in place technical and organisational measures to assist your clients with their obligations as a data controller/data processor in respect of data subject rights under GDPR?		
52	**Do you have a data retention and deletion policy?**		
Financial Stability & Reputation			
53	Is your company at loss during the last year?	No	
54	**Are you rated by any Rating company?** *If yes please provide your latest rating, its date and the Rating Company name in the Comments session.*	Yes	Last rating:_____ Rating issuance date:_____ Rating Company:_____
55	**Have you every filed for bankruptcy or experienced financial distress?**	No	
56	Are there any **ongoing legal or regulatory actions** against your company or any subsidiary of your company? *If yes provide detailed in the Comments session.*	No	
57	Do you have **insurance coverage** for cyber & operational risks (e.g. cyber incidents, professional liability, business interruption, etc.)? *If yes please provide details in the Comments session.*	Yes	Insurance type:_____ Insurance coverage:_____
58	Are you currently under any **Merger & Acquisition process**? *If yes please provide details in the Comments session.*	No	
59	**Do any of your clients contribute more than 10% of your total revenue**?	No	
Ethics & Corporate Responsibility			
60	Do you have a **Code of Conduct or Ethics Policy?**	Yes	
61	Do you have an **anti-bribery and anti-corruption policy?**	Yes	
62	Do you have a **Corporate Social Responsibility (CRS)** program?	Yes	
63	Do you have policies on **human rights, fair wages, diversity, and inclusion**?	Yes	
64	Do you have a policy on **forced labor, child labor, and modern slavery**?	Yes	
65	Do you ensure **health and safety standards** for your employees and contractors?	Yes	
66	Have you faced any **labor disputes, lawsuits, or regulatory violations** related to employee rights in the past five years? *If yes please provide detailes in the Comments session.*	No	
Environmental & Climate Risk			
67	Do you have a formal **climate and environmental risk policy** and measurable targets for improvement?	Yes	
68	Is climate and environmental risk integrated into your **corporate risk management framework** including both physical and transition risks?	Yes	
69	Have you conducted a **climate risk assessment** for your operations and supply chain?	Yes	
70	Do you comply with relevant **climate and environmental regulations** in your operating jurisdictions?	Yes	
71	Have you been subject to any **environmental violations, fines or penalties** in the past five years? *If yes please provide detailes in the Comments session.*	No	
72	Have you faced any supply chain disruptions due to **climate-related events** and what measures have you taken to address these risks? *If yes please provide detailes and measures in the Comments session.*	No	
73	Do you require suppliers and subcontractors to meet specific climate and environmental standards?	Yes	