Commission de Surveillance du Secteur Financier

LIST OF ANNEXES TO BE PROVIDED WITH THE BANKING LICENSE APPLICATION FILE

This is a standard, non-exhaustive list. Other documents may be requested after a detailed review of the application file.

- Signed ECB licensing privacy statement(s) from the future bank.
- Draft statutes / articles of association of the future bank reflecting bank status and statutory objectives.
- Documents to assess suitability of the authorised management and board members of the future bank as set out in the CSSF prudential appointment procedure published on the CSSF website:
    1. Copy of passport(s) or ID card(s),
    2. Criminal records extract(s),
    3. Declaration of honour for natural persons (please check for latest version using the following link and complete with care before signing (https://www.cssf.lu/en/document/declaration-of-honour-for-natural-persons/),
    4. Only for board members and authorised managers of significant institutions: Fit and Proper declaration for natural persons (please check for latest version using the following link and complete with care before signing https://www.cssf.lu/en/document/fit-and-proper-declaration-for-natural-persons-significant-institutions/),
    5. Comprehensive and detailed individual CV,
    6. Individual and collective suitability assessments from the future bank,
    7. Signed ECB privacy statement.
- Documents to assess suitability of the qualifying shareholder(s) that are natural persons*:*
    1. Copy of passport(s) or ID card(s),
    2. Criminal records extract(s),
    3. Declaration of honour for natural persons: (please check for latest version using the following link and complete with care before signing (https://www.cssf.lu/en/document/declaration-of-honour-for-natural-persons/),
    4. Comprehensive and detailed individual CV,
    5. Signed ECB privacy statement.
- Documents to assess suitability of qualifying shareholder(s) that are legal persons:
    1. Audited financial statements for the last 3 years,
    2. Declaration of honour for legal persons (please check for latest version using the following link and complete with care before signing https://www.cssf.lu/en/document/declaration-of-honour-for-legal-persons/),
    3. Certificate of registration,
    4. Statutes / articles of incorporation,
    5. Ratings (if available),
    6. Criminal records extract (if available),
    7. If the legal person is a regulated entity, certificate of good standing from the relevant supervisory authority,
    8. Suitability documents of those effectively directing the business. See above “Documents to assess suitability of the qualifying shareholder(s) that are natural persons”
    9. Shareholders’ agreement(s),
    10. Signed ECB privacy statement.
- Other relevant shareholder information:
    1. Shareholding structure chart, identifying key shareholders and ultimate beneficial owners,
    2. Complete group structure chart, highlighting participations in supervised (identify authority) and other entities with financial activities,
    3. Letter of comfort from reference shareholder (template provided by the CSSF),
    4. Declaration of origin of funds of key shareholders and ultimate beneficial owner.
- 3- year business plan including:
    1. Presentation of a business plan (balance sheet, income statement, regulatory requirements statement) covering at least 3 years of forecasts (in electronic format) and including core ratios (capital ratio, LCR, NSFR, leverage ratio, RWAs),
    2. Business plan shall include all relevant business drivers (number of clients, interest rates by product type, fee structure, etc.),

3. If credit risk is a relevant source of the overall risk of the bank, then provide a breakdown of the loan portfolio in terms of total exposures, allowances and NPL forecasts (i.e. LGD and PD estimates),
4. Elaboration of a stress scenario including lower growth perspectives, longer implementation phase and deteriorated economic circumstances (balance sheet, income statement and regulatory requirements statement),
5. Evolution of number of employees over years 1-3 to implement business strategy.

- Draft FGDL (deposit guarantee scheme) membership letter (article 10-1 LFS) https://www.cssf.lu/en/document/declaration-of-membership-of-the-fonds-de-garantie-des-depots-luxembourgfgdl/.
- Acceptance letter from external audit firm & name of partner in charge (article 10 LFS).
- Other key policies/plans:

1. Remuneration policy.
2. Anti-money laundering policy.
3. Recovery plan.

- IT requirements:

1. IT organisation and strategy

a. Provide a summarised description of the IT organisation (organisational chart, number of staff, key IT and information security roles and responsibilities) and the selected IT strategy (in-house or partial/full IT outsourcing).

b. In case of outsourcing, please:

- Specify the outsourced IT activities and provide the information about the external provider(s) (in particular: company name, belonging to the group of the entity seeking authorisation, location/address, supervision by a supervisory authority, support PFS).
- Specify which IT systems will remain in Luxembourg under your responsibility (i.e. not outsourced)
- Confirm that a contract and/or SLA is signed between both parties and that this contract/SLA is in line with best practices and addresses the following points/requirements:
  - description of services provided by your contractor,
  - description of your responsibilities and of your contractor,
  - integration of your needs in your contractor's BCP/DRP and backups arrangements,
  - conditions for revocation/termination of contract and transfer to another service provider or hand over to you,
  - management of the outsourcing relationship (e.g. regular reporting / meetings between your contractor and you, incident management process, KPI, etc.)
  - conditions for sub-contracting for your contractor (e.g. your prior authorisation)
  - data confidentiality and security
  - possibility for your internal and external auditors and for your supervisor (i.e. the CSSF) to perform an audit on site
- Specify who will be in charge of this outsourcing within the entity seeking authorisation.
- Describe the controls implemented to ensure the quality of service and compliance with applicable regulatory requirements.

c. In any case, the entity seeking authorisation must confirm that it will be responsible and actively involved in the management of the access rights (for instance validation of access rights requests and periodic access recertification, in accordance with “need to know” and “least privilege” principles) as well as the change management process of IT systems (i.e. changes to the IT environment impacting the data of the entity should be approved by the entity).

d. Clarify if the accounting system is located in Luxembourg or abroad. In case the accounting system is located abroad, in order to mitigate the risk of not being able to independently draw up a balance sheet and a profit and loss account, please clarify whether a copy of the basic accounting documents (including in principle the general ledger and the journal) will be available in Luxembourg.

2. Description of the IT systems

e. Specify the “business” IT systems supporting the “business” activities provided (e.g. software for fund administration, transfer agent, accounting of domiciled companies, reconciliation, portfolio management, customer relationship management, Intranet, Website – consultative or transactional) and the “support” IT systems used for the organisation and administration of the entity seeking authorisation (e.g. the internal accounting and CSSF reporting systems, e-mail servers, internal files servers and access management tools like Active Directory).

f. Provide a summarised table indicating, for each application system listed at point e. above:

- a short description of the application
- indication if it contains confidential data (of which type)
- the vendor of the application (if not in-house developed)
- the primary (production) hosting location of the application,
- the secondary (disaster recovery) hosting location of the application,
- the entity in charge of the IT infrastructure
- the entity in charge of the IT operations
- the entity in charge of the IT application maintenance
- the entity responsible (owner) for the application (e.g. you, a group entity, a third party..)
- if the application is dedicated or shared with other entities of the group (if so, please list the other entities with which the systems are shared)

g. Specify if the entity seeking authorisation plans to use mobile devices (e.g. smartphones, tablets). In case of such usage, the entity shall describe the tools (e.g. Mobile/Enterprise Device Management tools) used to securely connect and control (including remote wipe, passcode lock, etc.) the mobile devices and confirm its compliance with the CSSF Annual Reports 2012 (chap. XI, section 2.4.), 2007 (chap. VIII, section 2.1) and 2005, (chap. VIII, section 2.2.1).

h. Specify what type of telephone line the entity seeking authorisation will use (i.e. classical PBAX or VoIP). In this case, the entity shall confirm its compliance with CSSF Annual Report 2013, Chap. XI, 2.3.

i. Describe whether the entity seeking authorisation will host and administer its IT systems (support and business) itself on its premises. If not, please provide information on the type of service (e.g. PaaS, SaaS, IaaS), the system’s location (with an external provider or a provider belonging to the same group as the entity, in Luxembourg or abroad), the system operator (in particular: company name, location/address, belonging to the group of the entity seeking authorisation, supervision by a supervisory authority, support PFS) and on any system sharing with other entities (belonging to the same group as the entity seeking authorisation or not).

j. In case of sub-outsourcing, the entity seeking authorisation shall ensure that the principles stated in the previous section, related to outsourcing, are respected by the entity which is contractually responsible for the information systems management and has to ensure that the process is under full control. Please provide all evidence that the process is effectively under control.

3. IT Logical Security

k. Describe the measures aiming at protecting the data in transit, either as part of your internal communications (i.e. on the network which is exclusively under your control) or external communications (e.g. through the Internet or leased lines). In particular, please specify:

- The redundancy of the lines, to ensure the service continuity.
- The network communication protocols (e.g. IPSec, SSL), including the symmetric (e.g. AES) and asymmetric (e.g. RSA) encryption algorithms, and the size of the corresponding keys.
- The controls in place to ensure that the implementation of the encryption technologies is not exposed to known vulnerabilities (e.g. SSL vulnerabilities like Heartbleed, Poodle, etc.).

l. In case of remote access, please specify:

- The persons who will use the external connections (e.g. employees, IT support, other entities belonging to the same group, external providers). In case you plan to authorise employees to remotely access the systems, please specify the number of people, the systems that are remotely

accessible (indicating if they contain confidential data or not), the business purpose of such access and confirm its compliance to the CSSF's requirements stated in the Annual Reports 2013 (chap. XI, section 2.7.) and 2007 (chap. VIII, section 2.1.).

- The technical means used to provide remote access (e.g. VPN, Citrix, etc.), the (strong) authentication methods used (e.g. tokens) and the security controls in place to prevent the data leakage (e.g. hard disk encryption, block of USB ports, block of copy/paste and printing, etc.).

m. Specify the implemented security measures to ensure data protection, including data leakage prevention and segregation of environments in case systems are shared.

n. Specify if data at rest is encrypted. Should data at rest be encrypted, please describe the encryption process providing the encryption protocol, the encryption algorithm and the key lengths. Please specify the location of these keys and of any potential copies (backups) as well as a list of persons having access to the encryption keys.

o. Describe the controls in place over access to the information systems used by the entity (e.g. respect of the "need to know" and "least privilege" principle, regular access recertification, opening/closure of communication lines, user authentication, intrusion detection, antivirus, logs).

p. In case the entity seeking authorisation provides Front end applications to its clients (e.g. Website, mobile application), please describe the functionalities of the applications, the security measures related to the underlying infrastructure, as well as the security mechanisms in place for the clients' connections.

q. Provide a summarised description of your patch management process.

4. IT Physical Security

r. Describe the physical security measures and controls (access controls and environmental security measures) in place at:

- the offices of the entity

- the IT room/data center of the entity, or if applicable, the outsourced entity.

5. Business Continuity

s. Describe the backup process (in particular: full or incremental, frequency, retention periods, location of the backups and access restriction to the backups). The entity seeking authorisation must confirm its compliance with the CSSF Annual Report 2012 (chap. XI, section 2.7.).

t. Specify the secondary office location in case of the activation of the BCP (Business Continuity Plan). The entity seeking authorisation must confirm its compliance or commit to comply with CSSF requirements stated in the CSSF Annual Report 2013 (chap. XI, section 2.5.1.). Please describe the DRP (Disaster Recovery Plan) strategy (i.e. secondary site or not) and the high availability measures implemented.

u. Confirm that the entity seeking authorisation has a permanent, direct and unconditional (read and write) access to the IT systems provided by outsourced entities that allows the entity to take its activities back in hand at any time.

v. Confirm that the backup solution, BCP and DRP are in line with the entity's requirements in terms of continuity.