ICC Fintech Collaboration Guidelines

May 2022

INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

PURPOSE AND SCOPE

The trade finance industry is witnessing an unprecedented drive towards digitalisation. There is an increasing momentum across the trade finance ecosystem to utilise technology and widen collaboration in order to swiftly address the limitations of paper-based trade finance. Technologies including Distributed Ledger Technology (DLT) (encompassing Blockchain), Machine Learning, Artificial Intelligence, Application Programming Interfaces (APIs) as well as technology agnostic digital networks are witnessing increasing interest from financial institutions and corporates alike.

Following this industry trend, it is evident that digitalisation of trade finance will require an increasing number of players in the industry to connect with each other and use services/information/data provided by third parties (Fintechs). At present most players in the industry have their own set of standards to conduct due diligence, exchange trade information and on-board third-party vendors. These standards are rarely consistent and continue to evolve. This makes it difficult for third parties to expediently commercialise their solutions.

This paper aims to bring together a set of common standards that parties in the trade finance digital ecosystem can use to connect with each other digitally. It is a living document which will be expanded over time. These standards capture the common areas of consideration for third-party collaboration and seek to bring about a degree of standardisation in such engagements to ensure a faster, efficient and more effective collaboration between service providers and users. Trade finance is subject to many regulatory constraints which require fulfilment by internal departments of banks (compliance, legal, risk, security, etc.), mainly due to evolutions around GDPR, regulatory requirements, audits, certifications companies, etc. Banks integrate such aspects, which was not the case 2-5 years previously. Banks have to handle those aspects with their clients.

There are three main themes of standards that are generally considered before or during a third-party engagement. These are:

1. Information Security (Infosec) Standards,
2. Commercial Standards, and,
3. Technology Standards.

The paper sets out the common considerations and standards used under each of these themes. It is important to note that these standards are for reference purposes only, and may not be considered as legal recommendations or advice, nor should they be seen as necessarily all-inclusive. Recipients of such third-party services should have regard for their particular circumstances and seek their own independent financial, legal, tax and other relevant advice.

Note: A glossary can be found towards the end of this document

STANDARDS

1. Information Security (Infosec) Standards

These standards apply to either the technology vendor or service provider; whomever is responsible for providing the platform and related services to the customers (*customer may be the financial services provider and/or corporate end users). See annex 1 for more information.

THEME	RECOMMENDED STANDARD	EXPLANATION
Data classification	• Classification of information or data based on type of information. For example—Public/Internal/Restricted/Highly Restricted/Classified/Confidential information etc. • Restricting access to data	Data classification is broadly defined as the process of organising data by relevant categories so that it may be used and protected more efficiently.
Data hosting	• Location of data services • Secure Data at Rest • Controls around Data transfer • Controls on data access • Regulatory requirements	Data hosting is the process of deploying and hosting a data centre on a third-party or external service provider's infrastructure. Assets must be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly, and assigned ownership by defined roles and responsibilities. Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems. Physical access to information assets and functions by users and support personnel shall be restricted. Be aware of regulatory environment and customer requirements with respect to hosting certain data/information, for example—FATCA.
Data Management	• Data loss prevention • Security patch management • Data reversibility and deletion procedures • Data retention standard subject to local regulations	Data loss prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. Security patch management is the ongoing process of applying updates that help resolve code vulnerabilities or errors for applications across your system. Policies and procedures shall be established with supporting business processes and technical measures implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means. Data retention policies should take into consideration any regulatory requirements on how long any particular clarification of data must be retained.

THEME	RECOMMENDED STANDARD	EXPLANATION
		Process should be in place to allow full reversibility of the data to the client and to ensure complete deletion of the data at the Service Provider side, once reversibility is complete. A timing of the actual deletion date should be agreed between the vendor and the bank.
Cyber security	• Level of backup • Network penetration tests • Preventive, detective and recovery controls • Periodicity of reviews to meet evolving threats • Disaster recovery in different locations	Data related to electronic commerce (e-commerce) that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorised disclosure, or modification in such a manner to prevent contract dispute and compromise of data. Production data shall not be replicated or used in non-production environments. Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements. This should be time-based (or occurence) and/or contractually binding. In the case of Personal Accounts, such should be time-based «explicit consent” **Example of Cyber Security Standards** SWIFT has launched the Customer Security Program (CSP) to drive industry wide collaboration in the battle against cyber threats. This includes a set of core security controls. This is one example of an industry standard when it comes to cyber security. ICC has not checked nor verified if these standards are directly applicable to your business. This has been included as example only. https://www.swift.com/myswift/customer-security-programme-csp Related-processes should exist with Fintechs for them to identify and communicate to their clients.
Application Security	• Managing the development process of applications • User Testing • Authentication/Identification of users	Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards and adhere to applicable legal, statutory, or regulatory compliance obligations.

THEME	RECOMMENDED STANDARD	EXPLANATION
		A list of such legal, statutory or regulatory compliance requirements shall be documented and presented to inform customers. Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed. Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.
Malware Identification and remediation activities	• Anti-malware programs that are installed locally or cloud based • Capability to rapidly patch vulnerabilities within agreed timelines and based on priorities • Applications developed for Mobile Devices	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organisationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.
Intrusion Prevention	• Implementation of File integrity (host) and network intrusion detection (IDS) tools	Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory, or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviours and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach.
Access Control (Conditional access)	• Management of user ids and passwords • Segregation of duties • Removal of access controls when no longer required (Such can include, but not limited to, user ids and passwords) • Restrict, access to information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.). • Log, and monitor access of user level activity	Access control is a security technique that regulates who or what can view or use resources in a computing environment. Access to, and use of, audit tools that interact with the organisation's information systems shall be appropriately segmented and restricted to prevent compromise and misuse of log data. User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring

THEME	RECOMMENDED STANDARD	EXPLANATION
	• Auditability—who had done what, date, time stamp, build should be able to audited by internal and external auditors	appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organisationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. User log to include the capability to identify users log in times and activities performed. Such logs should be 'readily' available, in a reasonable machine readable format and/or be convertible to human readable format.
Regulatory	• Compliance with Data Privacy laws, for example GDPR and Singapore PDPA • Engagement with regulators on where the data is hosted. There will be country regulations around hosting data on cloud, sharing data across borders and access of data on demand • Regulatory engagement with use of third-party channels for communicating with customers. Is this regarded as a new distribution channel? • KYC/on-boarding requirements of the third party • Programming Language—interoperability • Transparency, sanctions, AML screening • Cross border licences • Fintech should be prepared to share subcontracter details	Data compliance is the practice of ensuring that sensitive data is organised and managed in such a way as to enable organisations to meet enterprise business rules along with legal and governmental regulations.

2. Commercial Standards

DOMAIN	RECOMMENDED STANDARD	RATIONALE
Risk Management	**Business policies—**in addition to data and technology related policies, service providers should have appropriate business policies. Examples include: • AML/Terrorism and Sanctions policies; anti-bribery and corruption, fraud, environmental/social governance • Dividends • Operational risk control • Where the Fintech has majority shareholdings, including by government or major corporates/banks, this should be declared to manage potential anti-trust or conflicts of interest • Employee policies. Including: ◦ Incentives, if applicable ◦ Ensure roles are clearly segregated ◦ Any background verification requirements ◦ Meeting local statutory requirements on employing workforce ◦ Any sub-contracting ◦ Documented exit policies upon employee termination ◦ Health and safety Further—if the service provider is established by Banks, then additional policies may need to be in place: • Antitrust • Conflicts of Interest	Supplier demonstrates appropriate governance and management of risks.
Risk Management—Business Continuity	**There are two aspects of Business Continuity Planning (BCP):** 1. Consider adequate BCP and relevant policies are employed by the service provider (technology provider) and 2. Appropriate planning and fall-back measures in place at the receiver's end (e.g. FI or Corporate). **Key areas of consideration for BCP policy includes:** • Impact analysis for disruption in critical service areas • Recovery plan/ Redundancy • Established tolerable disruption periods • Regular Review of BCP plans • The Fintech should declare where are their BCP locations and no. of critical employees available at recovery site.	

<table>
<tr><th>DOMAIN</th><th>RECOMMENDED STANDARD</th><th>RATIONALE</th></tr>
<tr><td><strong>Liability</strong></td><td>
<p><strong>Responsibilities and Liabilities</strong></p>
<p>Establish clear liabilities between the parties.
Examples of liabilities and possible limitations provided below:</p>
<table>
<tr><th></th><th>% of contract value or nominal value (whichever is greater)</th><th>Supplier indemnify the Customer</th><th>Unlimited</th></tr>
<tr><td>Fraud</td><td></td><td></td><td>✓</td></tr>
<tr><td>Wilful default</td><td></td><td></td><td>✓</td></tr>
<tr><td>Wilful abandonment</td><td></td><td></td><td>✓</td></tr>
<tr><td>Intellectual Property Rights (IPR) breach</td><td></td><td>✓</td><td></td></tr>
<tr><td>General supplier liability</td><td>✓</td><td></td><td></td></tr>
<tr><td>Data loss</td><td>✓</td><td></td><td></td></tr>
</table>
<ul>
<li>“Force Majeure”, the Fintech would need to clarify what happens in that case and what is covered, or any impact (e.g. termination of the agreement over a certain period if it lasts)</li>
</ul>
</td><td>Clearly establish which party is liable in the event of various breaches or losses.</td></tr>
<tr><td><strong>Insurance</strong></td><td>
<p><strong>Insurance Policies</strong></p>
<p>Agree insurance policies which service provider shall maintain.
Examples:</p>
<ul>
<li>Professional indemnity</li>
<li>Public liability</li>
<li>General product liability</li>
<li>Employee fraud</li>
<li>Employer liability</li>
<li>Property damage</li>
<li>Data protection</li>
</ul>
<p>In general: parties should be comfortable with the standing and reputation of the insurer.</p>
<p>Other issues to consider with regard to insurance policies:</p>
<ul>
<li>Assignability or issued to bearer. Need to be able to claim on it by Bank’s own initiatives</li>
<li>Parties should pay close attention to amount of insurance coverage, ensuring it is commensurate with the risk relating to the underlying activity</li>
<li>In some instances: pilot(s) or “proof of concepts” may be undertaken which are free of charge. However, in these instances, insurance policies may still be procured in the event of various damages and/or losses incurred as a result of the pilot/proof of concept.</li>
</ul>
</td><td>Ensure appropriate insurance policies are in place in the event of a claim.</td></tr>
</table>

DOMAIN	RECOMMENDED STANDARD	RATIONALE
Intellectual Property (IP)	**Intellectual Property ownership** • Appropriately define 'Intellectual Property' created under the arrangement between the technology provider and service provider; and which party owns this. Listing specific examples of this material may assist. • Ensure IP is considered 'confidential' in the legal framework.	Establish ownership at commence-ment of arrangement to avoid future disputes.
Data sharing principles (non-technology)	**Standards for FI/Corporates sharing data with Fintechs/ Suppliers. Key principles should be agreed:** • Client consent is obtained for any sharing of data, may be included in banks' terms and conditions • Data may only be used for the purposes described • Regulators may request access to data • Alternative models may be agreed whereby network/ solution provider has no data, customers and banks maintain ownership of their own data and no other parties can access this data (i.e. within a node, view hashes only) • The provider of the data (i.e. Bank) remains custodian of that Data • Custodian of data retains the right to delete or send/migrate data, and request proof of this • Transactional data is shared only, unless otherwise specified/ agreed • Warranties provided to comply with GDPR • Technology/Service provider can share information with banks at a portfolio level, where this relates to platform/product usage, provided it is masked	Establish transparent principles for general acceptance (although data sharing may depend on specific circumstances of arrangements).
Fintech/ supplier on-boarding requirements	• During on-boarding there may be questions pertaining to supplier credit worthiness/financial stability/reputation, adverse news, sanctions etc. • Risks resulting from sub-contracting to be appropriately managed. This includes risks associated with new outsourcing, as well as inadequate cooperation or communication between the contractors and sub-contractors • Technology/Service provides required to disclose both subcontracting arrangements, including their jurisdiction(s)	Typical information requested upon entering into relationship with a bank. Enables bank to consider different licenses.
Global Regulatory Environment	**Key global and national regulatory programmes for consideration:** • The General Data Protection Regulation (GDPR)—EU Law • Regulatory reporting obligation of Fintech/supplier • Contracts may involve cross-geography parties and service provision. The Bank and Service/Technology provider to agree on the legally binding law and the appropriate court which can enforce the law defined in the service contract in case of a contract breach or dispute • Appropriate Tax clause (possible VAT, withholding tax, etc.) • Fintechs should share regulatory notification of approval of compliance.	Outline typical considerations for banks, which Fintechs/ Suppliers should be aware of.

DOMAIN	RECOMMENDED STANDARD	RATIONALE
	• Where cross border implementation is required, fintech should provide implementation plan and any considerations and difference in services to be expected	
Auditability	Depending on the contractual relationship, Bank´s right to audit the Fintech/Service provider if applicable, or to be prepared to be obligated to provide the data for the purpose of the bank's reporting requirments	
Use of brand/ logo, etc.	Depending on the contractual relationship, following scenarios should be considered: • The use of brand/logo etc. of the bank by the Fintech/service provider in a white label setup • The use of brand/logo etc. of the Fintech/service provider by the bank • The use of a joint brand/logo etc.	
Costs and revenues	The split of costs/ revenues between bank and the Fintech/ service provider if applicable	

3. Technology Standards

Technology standards can vary according to the underlying use case and purpose of the engagement. Also, consideration is to be provided to the fact that this is an area that will continue to evolve and therefore may vary at times. Therefore, instead of providing clear standards, below are the recommended considerations, in the form of FAQ's that encompass relevant technology areas.

DOMAIN	RECOMMENDED CONSIDERATION
Technical Support & Maintenance	• Describe how your solution provides clear event statuses that can be shared in an easy and clear manner with customers and support teams. • Describe your support management offering (localisation, language understood, hours covered, etc.). • Describe escalation support management (level 1, level 2, etc.). • What job scheduling tools does the product support for offline/batch processing? e.g. TWS, Autosys etc. • Describe how your solution manages application interdependencies, e.g. realtime sanction checking. • Does your solution have the automated capability to identify and notify support staff in case of irregular volume of data? • Describe how your solution support client's ability to set thresholds and indicators for determining the application's health? Describe this for all elements of the solution. • Describe how your solution exposes indicators of application health. • Describe how your application implements targeted logging to support incident resolution and/or process monitoring. • Describe the monitoring and alerting tools/utilities that your solution supports or integrates with. • Describe how performance of your product in the Bank's production environment could be monitored. State any tools provided by yourselves for monitoring performance or recommendations for other FinTechs tools that work with your product(s) e.g. Wily/AppDynamics. • Are there aspects of the data/configuration underpinning the product that are not available to support teams under incident resolution circumstances? Please describe all instances. • Client will wish to run analytics tools in the production environment to health check the state of the application. What real-time analytics tooling does it support? • Confirm that robust disaster recovery capabilities are in place, and are tested regularly. • Fintech should describe its intended framework to support ongoing review and monitoring and guidelines for termination. • Commitment on SLA levels and share framework of the different SLA for different severity issues. (i.e Turn around time to provide fixes for different levels). • Fintech should comment on whether its solution has an automatic audit log which tracks each user's actions, allowing easy identification of where an issue may have occurred.

DOMAIN	RECOMMENDED CONSIDERATION
Software Installation (Deployment)	• Who is taking responsibility in the deployment strategy? ◦ Only Client ◦ Only Service Provider ◦ Both Explain the strategy and options for each point. • In case client is responsible (fully or partially) for the deployment strategy of the solution, explain how this has to be done for both cases: ◦ In case of integration with a client appropriate CI/CD pipeline ◦ In case of no integration with a client CI/CD pipeline. Explain the tools coming with your solution. • What deployment can be applied: ◦ non disruptive and the entire system ◦ non disruptive and gradual (i.e. during the transition to a newer version the current version is still partially in use) ◦ disruptive and the entire system ◦ disruptive and gradual ◦ ready for A/B testing ◦ For each of the options supported explain how. • In case multiple cloud providers are supported, explain the impact of shifting to another cloud provider. • For joint implementations, Fintech should share expectation of what percentage of testing is meant to be done by the bank or which other efforts the bank is expected to perform.
Infrastructure	• Provide a diagram that gives an overview of the infrastructure used by each component: ◦ machines ◦ servers ◦ firewalls ◦ load balancers ◦ appliances (e.g. HSM, etc.) ◦ edge infrastructure (beacon, sensors, etc.) ◦ network zones ◦ datacentres • Which cloud provider(s) do you support? ◦ for IaaS ◦ for PaaS ◦ for SaaS ◦ Which cloud regions and availability zones do you support for each of the options above? ◦ What is your experience with each of those providers (special requirements, restrictions, etc.)? ◦ Is your solution portable between providers?» • Explain sizing for infrastructure (e.g. type and number of servers, storage, bandwidth, etc.) and the influencing factors (e.g. number of users, number of requests, peak volume, etc.) to respond to our non-functional requirements (see further). • What are the requirements for the underlying infrastructure to guarantee the required Recovery Point Objective (RPO) en Recovery Time Objective (RTO)? • In case of (X)aaS, where do backups reside? • What are the used availability zones and regions?

DOMAIN	RECOMMENDED CONSIDERATION
Architectural Fit	• Describe how the product is designed to be fault tolerant, how does your solution manage failures? Are all processes restartable from point of failure and if so how do you achieve this. Do you include failure testing as a part of your product testing? • Data analytics and visualisation applications are designed purely for end user consumption and not data extraction purposes; describe how your solution complies to this statement. • Describe how you audit the usage of the Business Intelligence functionality such that usage statistics can be obtained. • Describe the test automation tools (automated testing tools plus test data generation mechanisms) that your solution supports. • All aspects of an application and its run time must be configured through code that is managed in version control'—please describe how your solution achieves and supports this rule. • Provide details of how you manage product enhancement requests. • Describe how your product supports customisation and how this is done and managed. Please pay attention to how customisation is managed in context of your product, its upgrades and the roadmaps of technologies it has dependencies upon. • Describe how your solution manages application and state data. Is the solution built and run in an immutable fashion? i.e. no state is stored on application instances. • «Provide details on the application performance with supplied volumetric data. You should include suitable reference performance benchmark for your product processes. • Examples; Throughput TPS, average, spikes, peaks, data volumes, server loads, application and network latency and diversity, application contention, data layer performance, user interface performance, API performance.» • Describe how your solution supports workload management—fluctuating workloads peak batch load processing times and parallel user access. • Provide details of the product coverage, are there any regional or global restrictions? • «Describe how your solution is OS and browser independent? The UI must be capable of running on Windows, MacOS, Android, iOS, Linux and be full HTML5 compliant and browser reactive. • Confirm that the product does not rely on Silverlight, ActiveX, Flash and client-side Java. Please provide any information on additional components that have to be installed/downloaded on the desktop/browser.» • «Explain how your solution complies with the Disability Discrimination Act? • How do you test for compliance with the regulation? • How does the solution accommodate changes to the regulation?» • List the features/aspects of the solution interface that are device specific. Which devices are supported? Please provide the roadmap for future support. • Please describe your UI architecture, including separation of logical layers e.g. business logic and UI layer. Also provide information on how you take device constraints e.g. bandwidth, into account when serving content. • Provide information on the solution's compatibility with standard plug-ins and peripherals e.g. standard Microsoft Office plug-ins. • Are there constraints on plugging the user interfaces of your solution into the client's web analytics tools. • How many previous versions of application, operating systems and middleware technology do you support? • What is your change management process for new releases?

DOMAIN	RECOMMENDED CONSIDERATION
	• Describe environment management to qualify release delivery and involvement of users (pre-production solution, users test, go-no-go by client…). • Describe user information and training linked to application evolution. • How do you distribute software to us and do you have samples of comprehensive release notes? • Describe the capabilities of the system to support new technologies like Blockchain or APIs and any examples of successful implementation. • Does your solution leverage existing standards such as SWIFT MT standards, etc.? • Describe how your solution will adopt new standards being developed or considered to support the broader industry such as ISO20022? • How quickly do you support new o/s, platforms? • Is a dedicated architecture delivered to, or provided to the receiver? In case data of one client is hosted along with other client's data in a mutualised environment/ public cloud, precise how it is segregated and secured. • If needed, can a specific filtering be implemented to ensure the service delivered to a client's users is only accessible from specific premises? (using for example internet IP filtering, VPN, etc.) • Guidelines on testing results to determine whether or not product can move from UAT to Production should be shared with Bank. • Guidelines on which kind of certain data the bank can make a request should be shared. Will the banks be able to request anonymous reports on the industry or will this be automatically published? • Guidelines to what extent the product will be customisable to each bank or client? eg. in terms of financing, will it be able to support different bank mandates?
Application Design	• What are the main architectural principles your solution adheres to? Provide the software component diagram of the solution and explain the solution design principles applied (e.g. layered architecture). In case of mobile device support, don't forget the components on the mobile device. • Describe for each component the functionalities or capabilities they implement and identify the components used for integration with the outside world. • Where and how is what kind of logic implemented and why did you choose to implement it like that? ◦ presentation logic ◦ integration logic (data transformations, protocol transformations, etc.) ◦ process logic ◦ business logic ◦ data logic • Explain what design choices have been made to facilitate future changes of your solution (modularity, complexity, dependencies, separation of concerns, etc.). • Indicate the components that belong to the core of the system and cannot be replaced by a solution from a third party. • To better understand the application and see if it covers the client needs: ◦ provide the logical data model used ◦ provide the definitions of each entity type and relation type (the logical data model can be different and larger than the canonical data model) • Which components are designed to increase availability? Explain how availability is leveraged in: ◦ data store components (e.g. distributed)

DOMAIN	RECOMMENDED CONSIDERATION
	◦ processing components (e.g. multiple/distributed instances) • What options are taken in relation to the CAP-theorem? ◦ Consistency: the system focusses on keeping information consistent and is responding to every request correctly. ◦ Availability: the system focusses on acceptable response times and does not focus on the correctness of the response. ◦ Partition tolerance: the system focusses on staying operational and can handle intermittent network outages. • If the CAP-theorem is not applicable, explain why. • Provide the data model diagram used to interface or communicate with your solutions. • Provide the definitions for each entity type. • What are the different touchpoints for your solution: ◦ Web ◦ Mobile app ◦ Desktop app ◦ Others • Explain to what extent the solution can be used in a Service Oriented Architecture (SOA): ◦ What functionalities are exposed by the service(s) of your solution that can be called in a SOA (e.g. status of an internal process). ◦ What functionalities do you expect from client's services or a third party solution. • Explain to what extent the solution is based on an event-driven architecture (EDA): • What events do you publish with which content at what frequency (e.g. events from internal business processes, notifications, data events, etc.)? • What events do you expect to receive from the client, with which content at what frequency? • What are the main architectural principles your solution adheres to? Provide the software component diagram of the solution and explain the solution design principles applied (e.g. layered architecture). In case of mobile device support, don't forget the components on the mobile device. Detailed descriptions and diagrams can be provided as appendix. • Provide an insight in the technologies (platforms, middleware, frameworks and protocols) used by the solution. Even for SaaS solutions this information is useful in relation to risk mitigation. • Provide an architecture diagram, giving the complete view on the technology stacks used for the realisation of each component mentioned in the component diagram. List out all technologies: ◦ operating systems ◦ middleware platforms ◦ Storage ◦ DB technology ◦ structured ◦ unstructured ◦ data lake ◦ distributed ◦ content management technology ◦ integration technology ◦ queueing (MOM)

DOMAIN	RECOMMENDED CONSIDERATION
	◦ Service Bus (ESB) ◦ DB integration technology ◦ Process Engine (BPMS) ◦ Event Broker ◦ Streaming technology ◦ Scheduler ◦ Export Translate Load (ETL) ◦ execution ◦ web server ◦ application server ◦ rules engine (BRMS) ◦ process engine (BPMS) ◦ browsers (IE, Chrome, Edge, Safari, Firefox, etc.) ◦ run-time libraries (.Net, JRE, etc.) ◦ other • Indicate where in the stack a given technology can be replaced by an alternative technology.
Technology overview	• What are the main architectural principles your solution adheres to? Provide the software component diagram of the solution and explain the solution design principles applied (e.g. layered architecture). In case of mobile device support, don’t forget the components on the mobile device. • Explain for the components, where this is applicable in your solution, what languages are used to extend, configure and develop. • If edge computing is involved please take it into account. • Can you stay compliant with client standards: ◦ front-end: HTML5, CSS3, Javascript ◦ language: Java, Python» • Indicate the components that belong to the core of the system and cannot be replaced by a solution from a third party (e.g. a solution that client already owns). • To better understand the application and see if it covers the client needs: ◦ provide the logical data model used ◦ provide the definitions of each entity type and relation type (the logical data model can be different and larger than the canonical data model)» • What part of the solution is based on products of third parties e.g. components delivered by other FinTechs (solutions, processes, data, etc.)? • Which of the modules of your solution could be replaced by third party solutions or client in-house solutions? How can this be done?» • For all technology items involved, how fast do you follow FinTech releases and standard evolutions? ◦ Operating systems ◦ all middleware involved ◦ all frameworks involved ◦ all third-party components involved ◦ For all of these involved items, what is the current supported version ◦ Illustrate your pace of innovation in this area Indicate for each technology topic above how all of this is documented (e.g. in off-line documents, on a public or shielded help or support website, etc.)

DOMAIN	RECOMMENDED CONSIDERATION
Security & Access	• Describe how your solution supports both RBAC and ABAC access control methods. • Explain how the product differentiates between user types e.g. admin users and regular users. • Explain how the product makes a distinction between user types and their entitlements. • Explain how users are managed so that they can only view their entitled data? • Describe the entitlement functions and explain how they can be customised. • Explain how functions are explicitly assigned or blocked. • How are user privileges/roles persisted; e.g. on the server, cookie/URL parameter? • Explain how your product performs user authentication and single sign-on. • The system must control access to data and operations. Please explain how this achieved in the context of APIs and other back-end processing? • Is all data on authenticated data stores? Please explain how the authentication to the data stores takes place i.e. individual user accounts or system accounts? • For system accounts, please explain the password cycle process and controls i.e. how the solution caters for regularly expiring system passwords and makes use of products such as Cyberark. • Explain how the product supports multiple logins? • Describe how user security is maintained in the product. Please list all the technologies including versions involved in user security and maintenance e.g. Struts. • Explain the standard hardening guide available for the product. • Can your administration team access to the users database? • Is there any remote access that you can propose to the client? • Does the solution can be interface with a strong authentication mechanism (multifactor authentication) for the privileged users (Administrators of your solution)? • Describe how communication between components of the system are secured (HTTPS, MQ , JDBC/ODBC etc.). Are there any elements of inter-component communication that are not secured? • Have any security assessments been completed on the system by third party assessors to identify vulnerabilities i.e. Pen Tests? If so, can you tell us when they were completed, on which version of your system(s) and share the results with us. • The solution must support anti-virus and anti-malware protection. Please explain the product’s capability in this regard. • Explain how the proposed solution is protected from cyber security attack. Where it is expected that client will be responsible, please clearly indicate this. • Describe the solution’s security features including compatibility with third-party security and encryption software? • Explain how security is included in the development and testing processes for the product. • Is your product’s source code passed through a source code screening tool for security vulnerabilities as part of your change management pipeline? If yes, please state what product/s are used. • Explain how issues such as the OWASP top 10 and SANs 25 are addressed in the development of your product’s source code?

DOMAIN	RECOMMENDED CONSIDERATION
	• What type of data is required to undertake the testing of your product (i.e. production, synthetic data or sanitised data)? • Upon discovery of vulnerabilities within the solution, the client security team would raise this with your company; Describe your approach including responsible disclosure policies or procedures. • There is a requirement for client to review the source code integrated within the solution's applications, explain how the delivery of this source code would be facilitated. • At times client may require data to be secured at the message level (MLS) rather than just the transport level (TLS). Explain how the application would support encryption and/or signing of messages end to end. • Describe the Application's support for n-tier DMZ topologies where the presentation layer, application layer and database layer are segmented by firewall zones. • Explain how the application maintains session state between the client and the host or user and host. • Explain how locally cached data is protected from tampering. • Explain how the application supports dual/tiered authorisations for sensitive operations. • Data displayed on-screen, in printed material and in audit logs may need to be hidden due to confidentiality—explain how the application could be configured to obfuscate specific data. • Explain how the application can be configured to integrate with a network-based antivirus product. • Does your solution support scheduled extracts of bank user data and their role entitlements for access recertification? • Do you separate Internet traffic from telecom traffic in your network? • Is your internal IT network (LAN offices) connected to your client hosting network (customers network)? If yes, how do you prevent viruses originated from your internal IT network to attack your client hosting network? • Do you have a procedure to apply patches in emergency on your security infrastructure if ever a critical vulnerability is announced? • Can you provide your Security Assurance Plan and the Quality Assurance Plan? • Describe how you react or resist against a Distributed Denial Of Service attack.
Certifications	• List the provider certifications for the intended service. • Can you certify all hosting datacenters comply with regulations (HVAC etc.), and precise which regulations are followed (country)? • Is the service relying on systems or processes certified with standard security norms (example EAL x or ISO y)? • Describe the measures you put in place to ensure: ◦ application code quality ◦ data quality.
Mail services—Orchestration services	• Describe mail services architecture and management rules (notification process, acknowledge in application, email address handling, attached file handling, encryption service). • If provided, describe the automated platform (workflow, provisioning, monitoring…) that need to interact with client's equipment/services).

DOMAIN	RECOMMENDED CONSIDERATION
File Transfer	• Describe the solution available in case files have to be uploaded to your internet website. • What mechanism is implemented to ensure consistency and integrity of the file is respected? • In case of mismatch between original file and the one present on Internet site, what information is available on your side as an audit track? • Describe the solution available in case information has to be exchanged automatically between a provider and a client (ex: automatic feeding of a ressource).

Glossary of Terms

ABBREVIATION OR TERM	MEANING
ABAC	Attribute based access control
AML	Anti Money Laundering
AppDynamics	Application Performance Monitory tool
Autosys	Job Scheduling software
BI	Business Intelligence
CAP-theorem	Consistency, Availability and Partition tolerance
CI/CD	Continuous integration (CI) and continuous delivery (CD)
CSP	SWIFT's Customer Security Program
Cyberark	Cyber threat prevention software
DDoS	distributed denial-of-service
DLP	Data Loss Prevention
EDA	Event Driven Architecture
FATCA	Foreign Account Tax Compliance Act
GDPR	General Data Protection Regulation
HSM	Hardware Security Module
IaaS	Infrastructure as a Service
ISO 20022	Industry standard for trade and payments
KYC	Know Your Client
OWASP	Open Web Application Security Project
PaaS	Platform as a Service
R&R's	Roles and Responsibilities
RBAC	Role based access control
RPO	Recovery Point Objective
SaaS	Software as a Service
SANS	SysAdmin, Audit, Network, and Security
Secure data at rest	Protect data that is not in use or is not traveling to system endpoints
SOA	Service Oriented Architecture
SWIFT MT	SWIFT Message Types e.g. MT7xx
Throughput TPS	Throughput Transactions Per Second
TRO	Recovery Time Objective
TWS	Tivoli Work Scheduler (IBM) Job scheduling software
VPN	Virtual Private Network
Wily	Application Performance Monitory tool (IBM)

ANNEX 1
Additional Information Security (Infosec) Standards

The vendor and/or «data processor» informs its «client» about the organisational measures taken by them and the technical security measures with regard to its service or product in such a way that the client itself is able to make an assessment as to whether they are sufficient, given the intended use of the service or product by the client and with that possible processing of personal data. «Data processor» expresses this in a Code of Conduct (or SoC/ISO).

The data processor has published a «Statement» or has included such in the processor agreement.

The «Statement» includes at least:

- the information security management chosen by the data processor system, the security standard (s) or standard;
- the—if applicable—certification(s) of the data processor;
- whether and which (sub) data processors are used by the data processor;
  - in which way the personal data of the client can be deleted;
  - the retention period, if there is a deviation from a destruction period of 3 months;
- the contact details of the contact person for data protection within the organisation of the data processor; or the data processor uses this «statement» along with standard «industry Standard» or approved «Code of Conduct» by applicable industry; clauses for processing, as part of the (processor) agreement.
- the data processor keeps track, in its contract administration, whether the Standard clauses for processing operations apply.
- the data processor keeps track, in its contract administration, whether (an)other processor agreement or standard clauses apply.
- The data processor informs its client about the processes and procedures it has designed with which the client can respond to the rights of data subjects.
- The data processor informs its client about the possibilities in regard to «data-subjects» for exercising their rights; including but not limited to: the right to be informed, the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object and rights in relation to automated decision making and profiling.
- If the data processor detects a data breach, the data processor will inform the client of this as quickly as possible, so that the controller can comply with their legal obligation within 72 hours of being aware of it and where applicable, to report the breach to the local Data Protection Authority (DPA) and/or the data subjects involved. The choice of reporting to the local DPA, remains the responsibility of the controller.
- The data processor will support the client or the controller with, if desired, the reporting process.
- In the event of a data breach, the data processor provides the required information and at least:
  - a description of the incident, nature of the infringement, nature of the personal data or categories of data subjects involved, estimation of the number of data subjects involved and possible databases involved, indication when an incident occurred (example: what happened?);

- contact details of the contact person (where can the controller go with questions?);
- possible consequences (what can happen, where should the controller, or the data subject, be aware, point out the possibilities of identity fraud such as details such as social security numbers, login and password details, passport copies may have ended up in the wrong hands);
- measures taken (what has the data processor done to prevent, limit or prevent this damage in the future?);
- measures to be taken by the controller or data subjects involved (what can data subjects do themselves, for example «keep an eye on mail, change passwords»);
- the data processor keeps the client informed of any further developments.

The data processor regularly tests and evaluates its data protection policy and takes security measures and adjusts them where necessary.

The data processor regularly tests and evaluates its information security management system and adjusts such where necessary.

Review and supervision

1. Where standards are used, independent supervisors of such, and governing bodies addressed or appointed in such, act as supervisors, where applicable.
2. The data-processor is responsible for supervising the review process for compliance with the statement by data processor.
3. Where standards or codes of conducts are used or referred to, the data processor shall be reviewed by independent auditors.

ABOUT THE INTERNATIONAL CHAMBER OF COMMERCE (ICC)

The International Chamber of Commerce (ICC) is the institutional representative of more than 45 million companies in over 100 countries. ICC's core mission is to make business work for everyone, every day, everywhere. Through a unique mix of advocacy, solutions and standard setting, we promote international trade, responsible business conduct and a global approach to regulation, in addition to providing market-leading dispute resolution services. Our members include many of the world's leading companies, SMEs, business associations and local chambers of commerce.

ICC INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

33-43 avenue du Président Wilson, 75116 Paris, France
T +33 (0)1 49 53 28 28 E icc@iccwbo.org
www.iccwbo.org @iccwbo