



FusionFabric.cloud Application Security Assessment by Synopsys

Presented by FusionFabric.cloud Partner Team

Context

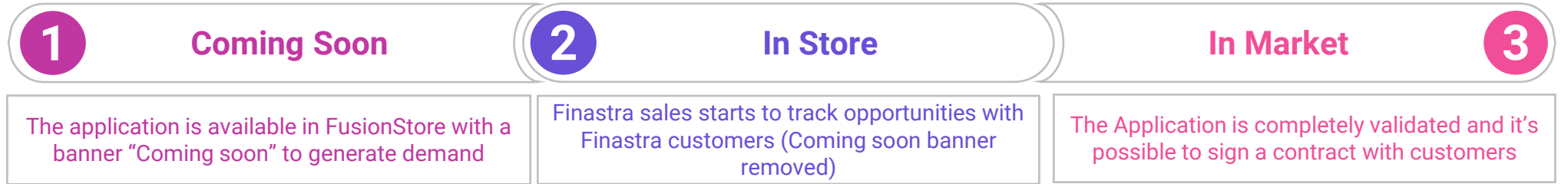
Finastra's Partner Team invites you to learn more about the security assessment process and to qualify your application for "In-Market" status which is the last step before contracting with a financial institution. For more information about FusionFabric.cloud App Validation Process, please check <https://developer.fusionfabric.cloud/documentation/platform-deep-dive/store-app-validation>

When a financial institution chooses an application for their use-case, the security evaluation guarantees that development organizations follow security rules or that certain provisions are in place to ensure data security.

The security review is performed by Finastra's global security partner, [Synopsys](#). All validation costs are pre-negotiated with Synopsys, and thus, the cost of a 3rd party security assessment and report is attractive, regardless of its connection to FusionFabric.cloud.

The next slide gives a quick overview of the security assessment process.

Progressive Onboarding Process In 3 Stages



1. Legal & Compliance

- ➔ Finastra Contract is signed
- ➔ First level of due diligence with a general questionnaire (refer) or TPRM (resell)

- ➔ Due diligence completed with all the additional documentation (no need for Resell apps)

2. Product review

- ➔ Application page is published in FusionStore (not necessary to have developed the application with the building blocks at this stage)

- ➔ Demo session to validate the technical integration with FusionFabric.cloud building blocks (API, SPI, Dataset)

3. Go to Market

- ➔ Provide documentation to support sales activities (App brief)
- ➔ Creation of relevant records in Finastra CRM system (NS Vendor record & SFDC Product)

4. Security assessment

- ➔ Ensure the fintech have deployed security best practice at different levels (governance, development, testing...)

Security Assessment Steps

1 Step 1



Once a client interest is confirmed, fintech organization will be contacted by FusionFabric.cloud Partner Team to sign the standard [3-way NDA](#) and start to fill the Security Questionnaire on Monday.com with the necessary evidences.

2 Step 2



Once fintech confirms the completion of questionnaire, FusionFabric.cloud Partner Team will notify Synopsys Team to start the pre-check and Synopsys team will list the missing evidence if they found any.

3 Step 3



Synopsys will produce a security assessment report based on the questionnaire answers and evidences. Finastra security team will later review the report to decide whether to approve it directly or give a CAP (Corrective Action Plan) for fintech to work on the key security issues identified. fintech organization is notified of the result with the Synopsys report attached and CAP letter, if any.

4 Step 4

(for app with CAP only)







Fintech will need to re-submit the evidence required from CAP to Synopsys for a retest. Finastra Security team will give the final approval or rejection based on the retest report

Security Assessment Task Owners

Step	Details	Task Owner
Questionnaire	Fill the form and attach all the necessary evidence (Monday.com)	Fintech
App Security review + report	Synopsis produce a detailed report on the Partner app to Finastra.	Synopsis
Review of security report and legal papers	Above Report is reviewed by Finastra to provide a positive or negative advice on the app based on the report	Finastra Legal and Due Diligence team
Final approval	<p>Application is approved or rejected. Partner is notified of the result.</p> <p>In case of rejection, Finastra will directly contact the partner to work on further improvements fixes needed to have the app passing the validation.</p>	Finastra FusionFabric.cloud Team

Before you start...

-  The target audience for this presentation is fintech organizations.
-  This questionnaire is designed to determine the security posture of the application development process employed to create the application, and the level of security controls built into the application.
-  For each “Yes” answer, please also submit the requested supporting artifacts/evidence of the control.
-  Do not leave any questions unanswered, and keep in mind that we do not expect perfect processes.



Security Questionnaire Categories

01

Impact on Financial
or Personal
Identifiable
Information (PII)

02

Governance

03

Construction

04

Verification

05

Deployment

IMPACT ON FINANCIAL OR PERSONAL IDENTIFIABLE INFORMATION (PII)

Question 1.a



Does the application provide **READ/VIEW ONLY access** to **financial data** on **FusionFabric.cloud**?

Severity : None

Evidence required : No

Mention if users have READ/VIEW ONLY access to financial data including but not limited to assets, liabilities, equity, income, expenses, etc.

Question 1.b



Does the application provide **READ/VIEW ONLY access** to **personally identifiable information (PII)** on **FusionFabric.cloud**?

Severity : None

Evidence required : No

Mention if users have READ/VIEW ONLY access to personally identifiable information such as an email address, a date of birth, a business phone number, a passport number, biometric data, and financial account numbers, etc.

Question 1.c



Does the application provide **WRITE/UPDATE access to financial data** or personally identifiable information (**PII**)?

Severity : None

Evidence required : No

Check if users have WRITE/UPDATE access to financial data or PII. If yes, mention the specific user roles (for example: admin, subscriber, guest) who have the rights to WRITE/UPDATE financial data or PII.

Question 1.d and 1.e



Does the application persist any personally identifiable information (**PII**)?
Does the application persist any non-anonymized **financial data**?

Severity : None

Evidence required : No

In reference to the above points d) and e) fintech organizations are required to scrutinize if an application stores or processes any PII or non-anonymized financial data. If yes, notifying about the purpose of storing such data and roles having access to this data would help to understand the security level of the information stored.

GOVERNANCE

Question 2.a



Have **regulatory compliance** considerations been incorporated into the application ?

Severity : None

Evidence required : Yes

If any of the regulatory policies are incorporated into the application, respective evidence should be provided. Some examples of such compliances are PCI, SOC1/2, CSA STAR, FFIEC, NYDFS, PSD2, Open Banking Standard etc.

Question 2.b



Have all developers completed **security awareness and secure coding trainings**?

Severity : None

Evidence required : Yes

Mention whether development team has undergone any security awareness, secure coding and any other application security related trainings. If yes, submit evidence(s) such as workshop certification, training material samples, a letter from the organization that provided the training, list of courses available internally etc.

Question 2.c



Do developers working on the application follow **secure program coding practices**, as part of a secure system development life cycle (S-SDLC), that meet industry standards ?

Severity : Critical

Evidence required : Yes

If the developers have followed the secured programming practices as a part of S-SDLC, answer to this question can be marked as “Yes” or organization needs to provide a compensating control of penetration testing report from the last year.

CONSTRUCTION

Question 3.a



Has the application been developed using a **secure architecture**, i.e., transport security, encryption, push vs pull mechanisms etc.?

Severity : None

Evidence required : No

Confirm if the application has been developed using a secure architecture considering various attributes like internal and external networks such as database servers/web servers. Security implementation of any web application varies based on its business and performance needs. Below is the reference link for high level secure architecture.

Reference : <https://www.synopsys.com/blogs/software-security/attributes-of-secure-web-application-architecture/>

Question 3.b



Have **security design reviews (SDR)** been conducted throughout the development process?

Severity : None

Evidence required : No

Notify if the security design reviews are conducted for an application taking into consideration various parameters such as authentication, authorization, session management, data and input validations etc.

Question 3.c



Has **Threat Modeling/ Threat Assessment and vulnerability analysis** been completed for this application?

Severity : None

Evidence required : Yes

As threat modelling helps in spotting design flaws and developing the secure application architecture, confirm if the threat modelling/ assessment and vulnerability analysis has been completed for an application with various types of testing such as tampering, spoofing etc. As evidence, share threat modelling report.

Reference: <https://www.synopsys.com/glossary/what-is-threat-modeling.html>

Question 3.d

Does application documentation provided include the following:



Question 3.d.i

Approved **High Level Diagram** been completed for the application?

Severity : Critical

Evidence required : Yes

Fintech needs to notify if the high-level diagram for an application has been completed and approved. As evidence, provide architecture diagram.

Question 3.d.ii



Description of **application processing details** and how application **data/information** will be **protected** in processing, transit and storage?

Severity : Critical

Evidence required : Yes

Fintech organization is required to provide the documentation with the description of application processing details and how application data/information will be protected while processing, transit and storage. The relevant information regarding encryption protocols, hashing algorithms can be added in the documentation if applicable.

Question 3.d.iii



Network diagrams?

Severity : Critical

Evidence required : Yes

If the answer to this question is yes, a network diagram would be required to share as evidence which elaborates what are the different components in the network are and how do they communicate with each other.



Question 3.d.iv

Data flow diagrams (DFD)?

Severity : Critical

Evidence required : Yes

If the answer to this question is yes, a DFD would be required to share as evidence which elaborates various entities, processes, data stores and data flow structure.



Question 3.d.v

Interconnectivity and calls (APIs, Exits) to external programs and systems?

Severity : Critical

Evidence required : Yes

If the answer to this question is yes, documentation with the relevant information needs to be submitted as evidence.

Question 3.e



Has **unit testing** of security features been performed for the application?

Severity : None

Evidence required : No

Notify answer to this question as “Yes” if the unit testing of security features has been done for an application considering various aspects such as XSS, SQL Injection etc.

Question 3.f



Does the design **separate user and administrative functions**?

Severity : None

Evidence required : Yes

In either case, fintech organization will require to provide the relevant explanation. If the answer to this question is marked as “Yes”, fintech will need to provide the list of administrative functions and explain how they are separated and restricted. If this is applicable, fintech organization would be required to provide documentation on how the admin and user roles separation is handled, list of admin functions and how the functionality is separated, etc.

Reference: <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models>

Question 3.g



Are all **entry points** to the application documented?

Severity : None

Evidence required : No

If all the entry points to an application are documented with necessary description and relevant diagrams wherever required, mark answer to this question as “Yes”.

Question 3.h



Are controls in place to **prevent the storing of passwords and encryption keys** in clear text within the application or associated files?

Severity : None

Evidence required : No

Fintech organization is required to confirm if the controls are in place to prevent the storing of passwords and encryption keys in clear text. Fintech organization can inform about the technique they are utilizing and mark answer to this question as “Yes”.

Question 3.i



Is **logging** enabled for all processing of the application?

Severity : None

Evidence required : No

If every process executed in the application is properly logged, answer to this question can be marked as “Yes”.

Question 3.j



Is **exception reporting/error handling** enabled for all processing of the application?

Severity : None

Evidence required : No

Fintech needs to check and confirm if the exception reporting has been enabled with proper error codes/ messages without disclosing any sensitive information for all the processes in the application.

Question 3.k

Are **application keys** managed with the following mechanism?

Question 3.k.i



Are keys stored in a **key vault** provided by a 3rd party e.g., HashiCorp Vault, AWS Secrets Manager, Microsoft Azure Key Vault, etc.?

Severity : None

Evidence required : No

If the keys are stored in 3rd party key vaults as mentioned in the question, the fintech organization needs to provide evidence such as the supporting documentation or code samples and mark the answer to this question as “Yes”.

Question 3.k.ii



Are **keys segregated** between test and **production environments**?

Severity : None

Evidence required : No

Verify if the encryptions keys are separately stored for test and production environments.

Question 3.k.iii



Is **access control** enforced to allow only specific services/instances to access the keys?

Severity : None

Evidence required : Yes

With evidence, fintech organization needs to confirm if the access control has been established so that only certain services can access the keys. Evidence can be provided in the form of document, code snippets, elaborating established key access controls like AWS, GCP, Azure services etc.

Question 3.k.iv



Is any **access to the keys logged**?

Severity : None

Evidence required : No

If someone accesses the keys, check and validate if the information is logged by the application with information such as entry point of the key, user ID, time at which keys were accessed etc.

Question 3.k.v



Is the **access to the keys monitored** by a security operations center?

Severity : None

Evidence required : No

When any type of access information (entry point, user ID, time etc.) about the key is logged, is it monitored by a security operations center? If yes, mention the same as answer to this question.

Question 3.l



Does the application **support secure deletion of data** needed to satisfy legal and regulatory requirements?

Severity : None

Evidence required : No

Under General Data Protection Regulation (GDPR), organizations must erase personal data under some cases such as if the data is no longer needed or if the processing of the original data is unlawful. Considering such scenarios, fintech organization is required to review and confirm if the application support secure deletion of the data when required.

Reference: <https://www.synopsys.com/blogs/software-security/eu-gdpr-data-security-standard/>

VERIFICATION

Question 4.a



Has an **independent code review** by a third party been performed for the application?

Severity : None

Evidence required : No

Fintech organizations can answer this as “Yes” if code review has been done by a third-party vendor has been done by considering various aspects such as design, functionality, performance, security etc.

Question 4.b



Security testing occurs at all post-design phases of the SDLC for the application, and its clients (if applicable, e.g., mobile app).

Severity : None

Evidence required : No

If the security testing (For example: XSS, SQL Injection, URL Manipulation, secure session management etc.) is planned at all post-design phases for the application and clients, mark this as “Yes”. Else fintech organization can mark this as “No”.

Question 4.c

Has the following **application security testing** been performed for this application in the last year?
[Note: If no answer in this section is marked as "YES", the validation would fail.]

Question 4.c.1



Has **Static Application Security Testing (SAST)** been performed?

Severity : Critical

Evidence required : Yes

If SAST has performed for the application, fintech organization shall provide an executive summary report as evidence and mark answer to this question as "Yes".

Reference: <https://www.synopsys.com/glossary/what-is-sast.html>

Question 4.c.2



Has **Dynamic Application Security Testing (DAST)** been performed?

Severity : Critical

Evidence required : Yes

If DAST has been performed for the application, fintech organization shall provide an executive summary report as evidence and mark answer to this question as "Yes".

Reference: <https://www.synopsys.com/glossary/what-is-dast.html>

Question 4.c.3



Has Interactive Application Security Testing (IAST) been performed?

Severity : Critical

Evidence required :Yes

If IAST has been performed for the application, fintech organization shall provide an executive summary report as evidence and mark answer to this question as "Yes".

Reference: [https://www.synopsys.com/glossary/what-is-iaast.html#:~:text=Comprehensive%20Software%20Analysis,Interactive%20Analysis%20\(IAST\)](https://www.synopsys.com/glossary/what-is-iaast.html#:~:text=Comprehensive%20Software%20Analysis,Interactive%20Analysis%20(IAST))

Question 4.c.4



Has Software Composition Analysis (SCA) been performed?

Severity : Critical

Evidence required : Yes

If SCA has been performed for the application, fintech organization shall provide an executive summary report as evidence and mark the answer to this question as "Yes".

Reference: <https://www.synopsys.com/glossary/what-is-software-composition-analysis.html>

Question 4.c.5



Have **penetration tests** been performed against your product?

Severity : Critical

Evidence required :Yes

If penetration tests have been performed for the application, fintech organization shall provide an executive summary report as evidence and mark answer to this question as "Yes".

Reference: <https://www.synopsys.com/glossary/what-is-penetration-testing.html>

Question 4.c.6



Do you have a **security bug bounty program**?

Severity : Critical

Evidence required : Yes

If any security bug bounty programs are conducted, fintech organization shall provide a reference link as evidence and mark answer to this question as "Yes".

Question 4.d

Have the following **security features/functions** been tested?

Question 4.d.i



Calls made to sub-processes or network interfaces **time out if completion codes are not returned within a reasonable time?**

Severity : None

Evidence required : No

If such a provision has been made so that application sub-process will timeout when completion codes/ expected response isn't retrieved within reasonable time, this question can be marked as "Yes".

Question 4.d.ii



Validity checking for all user inputs for syntactic and semantic correctness?

Severity : Critical

Evidence required : Yes

If the syntactic and semantic correctness validation has been implemented to check the validation of all the user inputs, the fintech organization needs to explain how it is achieved. Also, provide a screenshot of implementation that checks for valid inputs on the server-side, does not allow numbers in place for characters, etc. as evidence.

Question 4.d.iii



Request management - input validation issues are restricted by using parameterized SQL statements, input filtering, and input validation controls on all input parameters?

Severity : None

Evidence required :Yes

Fintech needs to provide information if input validation issues are restricted by using parameterized SQL statements, input filtering, and input validation controls on all input parameters. Also provide evidence such as a screenshot of input validation routine that utilizes whitelist regular expression checks, proof of usage of parameterized queries.

Question 4.d.iv



Correctness of arguments passed to operation system functions, if applicable.

Severity : None

Evidence required : No

If correctness of the various types of arguments passed to program functions are validated, this can be marked as "Yes".

Question 4.d.v



Return code checks from system calls, with logging of all codes and error number variables?

Severity : None

Evidence required : No

If the return codes by application calls are being checked and logged with all return codes, error number variables, this can be marked as "Yes".

Question 4.d.vi



Unauthorized access to the underlying operating system is prevented?

Severity : None

Evidence required : No

Based on the design and workflow of the application, if an application needs to interact with the underlying system, confirm if the unauthorized access is prevented to the system to ensure proper access control.

Question 4.d.vii



Unauthorized access to application resources is prevented?

Severity : None

Evidence required : No

If unauthorized access is prevented to the application resources such as program, server etc., this can be marked as "Yes".

Question 4.d.viii



Authentication controls in place to prevent cookie attack, credential theft and network eavesdropping?

Severity : None

Evidence required : No

If the necessary authentication controls are implemented for various scenarios mentioned in this question, this can be marked as "Yes".

Question 4.d.ix



Is **multifactor authentication** (MFA) required for remote users and privileged users (i.e. administrators)?

Severity : None

Evidence required : No

If there are two or more independent ways to identify remote and privileged users, this can be marked as "Yes". Some examples of MFA are codes received on users' smartphones, captcha tests, fingerprints or facial recognition.

Question 4.d.x & 4.d.xi



Are **strong passwords** required with minimum password length of 8 characters is required?
Are complex passwords required with minimum 3 of the following 4: numbers, capital letters, small letters, special characters?

Severity : None

Evidence required : No

As information technology services strongly encourage the use of strong passwords, fintech organization needs to notify about the password policies set for their application as mentioned in both the above points.

Question 4.d.xii



Authorization controls provide user accounts based on least privilege and enforce separation of privileges?

Severity : None

Evidence required : No

If the user accounts for the application are differentiated by various controls with least or full access privileges to perform certain actions in the application/ data, answer to this question can be marked as "Yes".

Question 4.d.xiii



Configuration management controls provide ACL access control and encrypt sensitive sections of the configuration files?

Severity : None

Evidence required : No

Scrutinize and confirm if the configuration management controls have been implemented in such a way that access to ACL can be controlled which specifies which users or system processes are granted access to specific functions and if sensitive sections of the configuration files can be encrypted so that unauthorized resources won't be able to identify the content of the configuration files.

Question 4.d.xiv



Session management controls prevent session hijacking, session replay and inability to log out successfully?

Severity : None

Evidence required : No

If session management controls are in place to prevent session hijacking, session replay, and inability to log out successfully, the answer to this question can be marked as “Yes”.

Question 4.d.xv



Are Denial of Service protections in place?

Severity : None

Evidence required : No

If the application is secured from Denial-of-Service (DoS) attacks, mark the answer to this as “Yes”.

Question 4.d.xvi



Unauthorized access or escalation of privileges are prevented?

Severity : None

Evidence required : No

Confirm if unauthorized access or escalation of privileges to systems within security perimeter is prevented.

Question 4.d.xvii



Privacy controls are in place to monitor access to data and maintain data integrity?

Severity : None

Evidence required : No

Answer as "Yes" if the information about access to the data is logged and monitored by an application and if data integrity is maintained.

DEPLOYMENT

Question 5.a



Have the **default accounts been changed or disabled** on services such as databases and web servers?

Severity : None

Evidence required : No

Confirm if the default accounts of the application are updated or disabled on services like databases and web servers.

Question 5.b



Have the **golden image** for servers, both physical and virtual, been **updated** with the latest patches and software versions?

Severity : None

Evidence required : No

If the golden image (clone/master/base image) for servers is updated with the most recent patches and software versions, this can be marked as “Yes”.

Question 5.c



Are the servers patched for critical security updates?

Severity : None

Evidence required : Yes

Fintech organization needs to review and confirm if the servers are patched for most recent critical security updates and relevant documentation/ screenshot proof should be provided for the same.

Question 5.d



Do you plan to whitelist all requests from your application to FusionFabric.cloud APIs?

Severity : None

Evidence required : Yes

If the fintech organization plans to whitelist all requests from their application to FusionFabric.cloud APIs, they would require to provide the IP addresses otherwise relevant explanation.

THE FUTURE OF FINANCE IS OPEN

Finastra is unlocking the power of finance for everyone by creating a platform for open innovation in the world of financial services.

