Date of Approval: 07/01/2025 Questionnaire Number: 2192

Basic Information/Executive Summary

What is the name of your project (system, database, pilot, product, survey, social media site, etc.)?

Authorization Framework Cloud

Acronym:

AZF Cloud

Business Unit

Information Technology

Preparer

For Official Use Only

Subject Matter Expert

For Official Use Only

Program Manager

For Official Use Only

Designated Executive Representative

For Official Use Only

Executive Sponsor

For Official Use Only

Executive Summary: Provide a clear and concise description of your project and how it will allow the IRS to achieve its mission.

The Authorization Framework will be implemented as an AWS (Amazon Web Services) Cloud Service that provides centralized Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) authorizations to IRS applications. This service will be external to the applications and existing authentication systems. AZF (Authorization Framework) is, in and of itself, not an application, but a COTS (Commercial of the Shelf) implementation that authorizes requestors (services) to either be permitted or denied access to protected resources within applications. There are no actual users, other than those who configure and integrate the COTS with government developed applications. Authorization Framework (AZF) Cloud is used for IRS enterprise-wide common authorization service and to satisfy authorization security requirements, it is owned by Information Technology (IT) Business Unit (BU).

Personally Identifiable Information (PII)

Will this project use, collect, receive, display, store, maintain, or disseminate any type of Sensitive but Unclassified (SBU), Personally Identifiable Information (PII), or Federal Tax Information (FTI)?

Yes

Please explain in detail how this project uses sensitive data from inception to destruction (data lifecycle).

AZF stores PII (SADI UUID only) in the attribute datastore. This data is used as part of the authorization transaction verification. Any other PII is not stored but is used in a transient manner for these transactions. PII may be present in the AZF audit logs but is obfuscated.

Please select all types of Sensitive but Unclassified data (SBU)/Personally Identifiable Information (PII)/Federal Tax Information (FTI) that this project uses.

Address

Email Address

Employer Identification Number

Federal Tax Information (FTI)

Internet Protocol Address (IP Address)

Name

Social Security Number (including masked or last four digits)

Universal Unique Identifier (UUID)

Cite the authority for collecting SBU/PII/FTI (including SSN if relevant).

PII for federal tax administration - generally IRC Sections 6001 6011 or 6012

SSN for tax returns and return information - IRC section 6109

Product Information (Questions)

- 1 Is this PCLIA a result of a specific initiative or a process improvement? Yes
- 1.1 What is the name of the Business Unit (BU) or Agency initiative?

 IRS Modernization Program and the Treasury Department's overarching new Enterprise Architecture Framework.
- 2 What type of project is this (system, project, application, database, pilot/proof of concept/prototype, power platform/visualization tool)?

System

3 What Tier designation has been applied to your system?

2

4 Is this a new system?

No

4.1 Is there a previous Privacy and Civil Liberties Impact Assessment (PCLIA) for this project?

Yes

4.11 What is the previous PCLIA number?

4.12 What is the previous PCLIA title (system name)? Authorization Framework Cloud (AZF-Cloud) 1171

4.2 You have indicated this is not a new system; explain what has or will change and why. (Expiring PCLIA, changes to the PII or use of the PII, etc.)

AZF Cloud will be migrating all existing clients from Enterprise Container Platform On-Prem (ECP On-prem) to Integrated Enterprise Portal (IEP) Cloud Production to align to the IRS Modernization Program and the Treasury Department's overarching new Enterprise Architecture Framework. Existing Clients include Secure Access Digital Identity (SADI), Automated Lien System Extranet (ALS-E), Clean Energy (CE), Business Tax Account (BTA), Income Verification Express Service - Form-Based Process (IVES-FBP), eServices Consent & eService Terms of Service (eServices TOS). AZF is also supporting new clients, including Tax(payer) Delinquent Account (TDA), Digital and Mobile Adaptive Forms (DMAF) & Tax Professional (TaxPro).

5 Is this system considered a child system/application to another (parent) system?

6 Indicate what OneSDLC State is the system in (Allocation, Readiness, Execution) or indicate if you go through Information Technology's (IT) Technical Insertion Process and what stage you have progressed to.

Execution

7 Is this a change resulting from the OneSDLC process?

No

8 Please provide the full name and acronym of the governance board or Executive Steering Committee (ESC) this system reports to.

Authentication, Authorization, and Access - Executive Governance Board (A3 EGB)

9 If the system is on the As-Built-Architecture (ABA), what is the ABA ID number of the system? If this PCLIA covers multiple applications shown on the ABA, please indicate the ABA ID number(s) for each application covered separated by a comma. If the system is not in the ABA, then contact the ABA (https://ea.web.irs.gov/aba/index.html) for assistance.

211215

10 If this system discloses any PII to any third party outside the IRS, does the system have a process in place to account for such disclosures in compliance with IRC 6103(p)(3)(A) or Subsection c of the Privacy Act?

No

10.1 You have indicated that you do not have an "accounting of disclosures" process is in place; please indicate a projected completion date or explain the steps taken to develop your accounting of disclosures process. Note: The Office of Disclosure should be contacted to develop this system's accounting of disclosures process.

Not applicable because the system does not disclose any PII to any third party outside the IRS.

11 Does your project/system involve any use of artificial intelligence (AI), including virtual assistant, chat bot, and robotic process automation, as defined in Executive Order 13960 and 14110?

No

12 Does this system use cloud computing?

Yes

12.1 Please identify the Cloud Service Provider (CSP), FedRAMP Package ID, and date of FedRAMP authorization.

AWS Gov Cloud - Accenture FR # F1603047866 - 06/21/2016

12.2 Does the CSP allow auditing?

Yes

12.21 Who has access to the CSP audit data (IRS or 3rd party)? IRS

12.3 Please indicate the background check level required for the CSP (None, Low, Moderate or High).

Moderate

13 Does this system/application interact with the public?

No

14 Describe the business process allowing an individual to access or correct their information. (Due Process)

AZF is an Enterprise solution for business applications and does not meet the standard user-application use cases because there are no real "users". There are no actual direct individual users of AZF Cloud. Only AZF Cloud developers connect directly to the COTS Admin GUI of the application to configure and integrate the COTS product with client application policies and requirements

15 Is this system owned and/or operated by a contractor?

16 Identify what role(s) the IRS and/or the contractor(s) performs; indicate what access level (to this system's PII data) each role is entitled to. (Include details about completion status and level of access of the contractor's background investigation was approved for.)

Roles: Developer Access Level: No access in the production environment. In the DEV environment, developers have READ-WRITE access.

17 The Privacy Act of 1974 (5 USC § 552a(e)(3)) requires each agency that maintains a system of records, to inform each individual requested to supply information about himself or herself. Please provide the Privacy Act Statement presented by your system or indicate a Privacy Act Statement is not used and individuals are not given the opportunity to consent to the collection of their PII.

Not Applicable, AZF Cloud does not have any news.

18 How many records in the system are attributable to IRS Employees? Enter "Under 50,000", "50,000 to 100,000", "More than 100,000" or "Not Applicable".

Not Applicable

19 How many records in the system are attributable to contractors? Enter "Under 5,000", "5,000 to 10,000", "More than 10,000" or "Not Applicable".

Not Applicable

20 How many records in the system are attributable to members of the public? Enter "Under 100,000", "100,000 to 1,000,000", "More than 1,000,000" or "Not applicable". Not Applicable

21 Identify any "other" records categories not attributable to the categories listed above; identify the category and the number of corresponding records, to the nearest 10,000; if no other categories exist, enter "Not Applicable".

Not Applicable

22 How is access to SBU/PII determined and by whom?

AZF Cloud Application Team does not have access to any client PROD SBU or PII. Treasury Inspector General for Tax Administration/Enterprise Security Audit

Trails (TIGTA/ESAT) has access to this info within Splunk audit logs. Authorization Service: AZF Cloud provides Authorization decisions based on individual client requirements, including what SBU/PII is accessed and by whom. Generally, specific PIPs containing attributes which may be SBU or PII are required to make the authorization decisions. Attribute Service: AZF Cloud client applications which are onboarded to this service may access their own data only. Details around where the information clients submit to our service is accessed or by whom is determined by the client application.

23 Is there a data dictionary on file for this system? Note: Selecting "Yes" indicates an upload to the Attachment Section is required.

No

- 24 Explain any privacy and civil liberties risks related to privacy controls.

 None
- 25 Please upload all privacy risk finding documents identified for the system (Audit trail, RAFT, POA&M, Breach Plan, etc.); click "yes" to confirm upload(s) are complete.
- 26 Describe this system's audit trail in detail. Provide supporting documents. See audit worksheet attached.
- 27 Does this system use or plan to use SBU data in a non-production environment?

Interfaces

Interface Type

IRS Systems, file, or database

Agency Name

AZF Cloud to ESAT Audit Records

Incoming/Outgoing

Outgoing (Sending)

Transfer Method

Application to Application (A2A)

Interface Type

IRS Systems, file, or database

Agency Name

Automated Lien System (ALS) request to AZF Cloud

Incoming/Outgoing

Incoming (Receiving)

Transfer Method

Application to Application (A2A)

Interface Type

IRS Systems, file, or database

Agency Name

eServices request to AZF Cloud

Incoming/Outgoing

Incoming (Receiving)

Transfer Method

Application to Application (A2A)

Interface Type

IRS Systems, file, or database

Agency Name

SADI request to AZF Cloud

Incoming/Outgoing

Incoming (Receiving)

Transfer Method

Application to Application (A2A)

Interface Type

IRS Systems, file, or database

Agency Name

AZF Cloud to Electronic Signature Storage and Retrieval (ESSAR)

for Signature Validation

Incoming/Outgoing

Outgoing (Sending)

Transfer Method

Application to Application (A2A)

Interface Type

IRS Systems, file, or database

Agency Name

Income Verification Express Service (IVES) request to AZF Cloud

Incoming/Outgoing

Incoming (Receiving)

Transfer Method

Application to Application (A2A)

Interface Type

IRS Systems, file, or database

Agency Name

AZF Cloud request to Enterprise Data Platform (EDP)

Incoming/Outgoing

Outgoing (Sending)

Transfer Method

Application to Application (A2A)

Interface Type

IRS Systems, file, or database

Agency Name

Clean Energy (CE) request to AZF Cloud

Incoming/Outgoing

Incoming (Receiving)

Transfer Method

Application to Application (A2A)

Interface Type

IRS Systems, file, or database

Agency Name

AZF Cloud send request to ALS DB

Incoming/Outgoing

Outgoing (Sending)

Transfer Method

Application to Application (A2A)

Interface Type

IRS Systems, file, or database

Agency Name

Business Taxpayer Account (BTA) request to AZF Cloud

Incoming/Outgoing

Incoming (Receiving)

Transfer Method

Application to Application (A2A)

Systems of Records Notices (SORNs)

SORN Number & Name

IRS 24.030 - Customer Account Data Engine Individual Master File

Describe the IRS use and relevance of this SORN.

By electronic filing provider name or Taxpayer Identification Number (TIN) (e.g., Social Security Number (SSN), Employer Identification Number (EIN), or other similar number assigned by the IRS)

SORN Number & Name

IRS 34.037 - Audit Trail and Security Records

Describe the IRS use and relevance of this SORN.

By name, Social Security Number (SSN), or the standard employee identification number (SEID) of employee, contractor, or other individual who has been granted access to IRS information, or to IRS equipment and resources, and by incident number. Also, by name, SSN or Taxpayer Identification Number (TIN) of entities whose records were accessed.

SORN Number & Name

Treasury .015 - General Information Technology Access Account Records

Describe the IRS use and relevance of this SORN.

Records may be retrieved by an identification number assigned by computer, by facility, by business affiliation, email address, or by the name of the individual, or other employee data fields previously identified in this System of Records Notice.

Records Retention

What is the Record Schedule System?

General Record Schedule (GRS)

What is the retention series title?

3.1: General Technology Management Records

What is the GRS/RCS Item Number?

030

What type of Records is this for?

Electronic

Please provide a brief description of the chosen GRS or RCS item. Configuration and change management records. Records created and retained for asset management, performance and capacity management, system management, configuration and change management, and planning, follow-up, and impact assessment of operational networks and systems.

What is the disposition schedule?

Temporary. Destroy 5 years after system is superseded by a new iteration, or is terminated, defunded, or no longer needed for agency/IT administrative purposes, but longer retention is authorized if required for business use.

What is the Record Schedule System?

General Record Schedule (GRS)

What is the retention series title?

3.2: Information Systems Security Records

What is the GRS/RCS Item Number?

010

What type of Records is this for?

Electronic

Please provide a brief description of the chosen GRS or RCS item. Systems and data security records. These are records related to maintaining the security of information technology (IT) systems and data. Records outline official procedures for securing and maintaining IT infrastructure and relate to the specific systems for which they were written. This series also includes analysis of security policies, processes, and guidelines, as well as system risk management and vulnerability analyses.

What is the disposition schedule?

Temporary. Destroy 1 year(s) after system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system.

What is the Record Schedule System?

General Record Schedule (GRS)

What is the retention series title?

3.1: General Technology Management Records

What is the GRS/RCS Item Number?

011

What type of Records is this for?

Electronic

Please provide a brief description of the chosen GRS or RCS item. System development records. These records relate to the development of information technology (IT) systems and software applications through their initial stages up until hand-off to production which includes planning, requirements analysis, design, verification and testing, procurement, and installation. Records include case files containing documentation of planning, decision making, designing, programming, testing, evaluation, and problem solving

What is the disposition schedule?

Temporary. Destroy 5 years after system is superseded by a new iteration, or is terminated, defunded, or no longer needed for agency/IT administrative purposes, but longer retention is authorized if required for business use.

Data Locations

What type of site is this? System

What is the name of the System?

Authorization Framework Cloud

What is the sensitivity of the System?

Sensitive But Unclassified (SBU)

Please provide a brief description of the System.

Authorization Framework Cloud (AZF Cloud) provides a common platform to ensure a consistent approach for access control decisions across the Enterprise. Utilizing a Service-Oriented Architecture (SOA), AZF Cloud provides a platform that integrates with authorization infrastructure and applications. It reduces dependency on individual COTS products and provides standards-based implementations as well as providing a consistent approach for increased security and reduced integration time with applications.

What are the incoming connections to this System?

Incoming connections to the system are through the IEP Cloud Enterprise API Gateway from clients requesting our service, including Secure Access Digital Identity (SADI), eServices, Automated Lien System (ALS), Clean Energy (CE), Business Tax Account (BTA) & Income Verification Express Service (IVES)

What are the outgoing connections from this System?

There are no outgoing connections from the system for current AZF Cloud client support.