Meeting Minutes: IRS (Public Sector)

Date: 07/12/2018

Time: 2:30pm to 3:20pm EDT

Attendance:

Mary C Petrosky = Acting section manager of the ESS team for the IRS. Both Syed and Janice work for her
Syed Abbas = Technical Lead for the ESS team. They cater to the needs of the customers that use their platform. They are on the business side, not the technical side.
Janice Foulk = She was on the original call in 2016 with Joe Cosentino. Business side of the house (ESS). This could possibly act as an discovery call before the technical one.
Joe Cosentino = Senior Leadership/Business Partner, Sprezzatura
Shane Johnson = Management Analyst, Sprezzatura
Nitin Sahai = Enterprise Cloud Architect, Sprezzatura
Thomas Holliday = Senior Manager/Microtask Lead, Sprezzatura

Interview Agenda Items/Questions:

General:

- What is your role in your organization?
    - Mr. Syed M. Abbas stated role at IRS is Management/Program Analyst.
    - Website: https://www.irs.gov/
- How many APIs do you build each year? How many are for external consumption? How many for Internal consumption? What are the security concerns for internal versus external consumption? Firewall relaxation process and procedures.
    - IRS MEF (Modernized E-File) program was developed 10 year ago. APIs are developed as SOAP service and are secured using certificate based authentication. The IRS team promotes proper testing of SOAP clients to ensure, prior to live processing, that API consumers/clients transmit in the correct format and meet the IRS electronic filing specifications.
    - Developed ten years ago, they offer 20 APIs (as SOAP). They use GSA approved certificates based security, and use a token system for their calls.
    - There were conversations about if their architecture may need to apply rest services with their SOAP service, but they do not see that happening anytime soon.
    - They do not have that many internal facing APIs, so the team can and will do both.
    - Their use cases would be base off of external facing APIs. They also have a test team that uses their APIs before they go out.
    - They already do their own internal testing before they allow the APIs out to the external environment.
- Do you utilize external industry publications such as Gartner?
    - SOAP services implementations follow Gartner and other industry standard specifications. Though, they did state that they were not sure and this is more of a development question.

Prioritizing APIs to Build:

- How do you prioritize the APIs you're building? Do you use an Agile Backlog, or other method? Do you evaluate based on Level of Effort and ROI, or use other metrics? Do you prioritize APIs as to their eventual utilization across the enterprise versus a single project?
    - The IRS prioritizes APIs typically based upon customer requirements. There are around 20 plus APIs currently exposed to providers/partners like Intuit Turbo Tax, etc. What's needed to be exposed to the external party is tax return information. Their most used API is 'send transmission.' The second most used API is 'get acknowledgement.'
    - The IRS does not have a formal process to apply enhancements to current APIs (includes topic areas such as versioning strategy, API industry transfer). Said a different way, they do not currently have a formalized process when someone asks for an enhancement or a change with their APIs. They do not do a lot of changes because their APIs are ten years old and very mature. If there is an issue, they will pursue a large change. Aside from that, they do not veer from their strategy.
- How much of your API backlog is defined by a Consumer's request? How much do you attempt to anticipate the needs of Consumers and build APIs speculatively? Should speculative API development be more or less constrained by defined governance specifications?
    - At this point, the IRS does not have any new API designs in the pipeline.
    - The IRS does not have an upcoming backlog of APIs. They must process for this, utilizing external and testing environments. The processors have two weeks to test before it is sent out.
- How do you make choices between building Experience layer APIs vs Process layer vs System layer APIs? Experience layer APIs vs Process layer development could conceivably be performed by different development team – how will the governance model be enforced when there is a multi-team development environment?
    - Internal communications are done via system call and they do not have an API for that.
    - The IRS has many internal systems (like E-File/MEF, sequels). They do downstream workflow with processing and processors.
    - What is the onboarding process for IT companies/new customers?
        - They need to file (I.e. put in the E-File, ETIN number, e-pin number), and then they verify who they are, and what they want to do, and then they receive a certificate saying they can possibly do a test on their test environment.
    - Do you manage your API lifecycle and pipeline?
        - Yes, they do. They follow a traditional waterfall process with their pipeline.
    - Is their one team handling the development for the APIs?
        - Yes, one team and one contractor vendor.
- Do you allow Experience layer requirements to drive build prioritization on Process and System layer APIs? If not, why not? Or is the option of the building of "mocked" lower level API implementations (Process and System)?
    - The IRS follows a top-down approach, which starts with WSDL, and is then followed by/with implementation.
- If you have APIs/services on legacy platforms, how do you decide when port those over to a new platform? Additionally, how these legacy applications will be "ported" – re-hosted, re-factored, re-built?
    - The IRS issues APIs once a year around January.
    - Do you have your own turbo tax tool?

        - Yes they have their own set of tools that are home grown to make sure those APIs are functioning as designed.
        - They have a calendar. The first testing is in November and the last is in January and customers can come In and test their API
        - Do they all have to cut over in January? No they don't force that on vendors
        - They shut their systems down for about ten days before a switch so they and the vendor are ready for the switch over.
        - Making it an all or nothing deal.
        - Testing in November. Product is open between January to Dec.

Standards to Which to Build

- Do you have multiple, unrelated teams, delivering APIs into the same environment? If so, what lessons have you learned about configuration management across the environment/teams? What level of maturity are your Agile, CI/CD, Dev/Ops capabilities?
    - Dev GitHub to Ansible to Environment.
- Does your organization maintain formal standards for: API Contracts, Naming Conventions; Version Control, Branching, and Merging; Testing Requirements; Exception Handling; Logging; Security? Would you be able to share any documentation? How is this documentation presented – web pages, WIKIs, Playbook SharePoint sites etc.?
    - Maintain Playbook.
- Do you experience a need to keep documentation and configuration control minimal/light? How do you ensure you're minimizing paperwork/bureaucracy and maximizing code delivery? Again Agile, CI/CD, Dev/Ops capability levels.
    - Via API reference architecture and Governance docs.
- How do you enforce standards across multiple development teams?
    - Not addressed specifically with this question.

Consumer Experience

- How many customers external to your organization consume your APIs?
    - Not addressed specifically with this question.
- What have you learned about development, testing, deployment that you apply to maximizing consumer experience?
    - APIs abuse topic:
        - When they publish their APIs they put a guideline out on how to use their APIs, but they cant control customers and how they use the API so they begin to abuse the power (e.g. they call those APIs too many times). Sometimes they have to call and tell them about their misuse even though they did not have bad intentions. They thought about putting controls or restrictions on their APIs, but they have not done this to date.

Closing Questions

- Are there any internal documents (not published on your Webpage) that you could share that would show how you apply governance internally?
    - The IRS has several publications available. They are mostly created in-house by their own employees. They also have documentation available that was developed by contractors in the past.

    - Th IRS has some guides that they only give to their trusted partners. They have a company called PIGTA that chooses who they can give privileged information to rather than to distribute to a wide audience.
    - Not with their team. She can send over the public side but not the trusted partner side.
    - They check all of the information before they publish anything. They have a page on IRS.gov where they have that documentation. They check before the post on that page.
- To whom do you look to for API governance best practices, with who else should we speak?
    - Response provided is that this would be a question for a Developer.
- May we please circle back with any follow-up questions (Yes/No)?
    - No response provided to this particular question.

Additional Reference Information and Analysis

Microtask Requirement

As the VA Lighthouse (now API Platform) Product Owner seeking the appropriate Governance model, I would like to understand, with the intention to adopt, best practices from the private and public sector, specifically for prioritizing APIs to build, standards to which to build APIs, and making the APIs usable by external consumers. We would like the primary research performed to gather best practices around:

- Characteristics of effective models in the public and private sector, and who is successfully using them. Including the utilization of leading edge API development enabling technologies (CI/CD, Dev/OPS, Micro service, Containers etc.).
- Lessons learned from these organizations (both what is working and what isn't)
- Highlight strengths and weaknesses of selected governance models.

Interview Analysis

Two Tiers of Technical Documentation - The IRS maintains two different tiers of technical documentation for security reasons. The first tier is publicly exposed via the EFS website. This is scrubbed of all specific information that could enable a cyber attack. The second tier of technical documentation is only available once a third party clears the onboarding security review and becomes a "Trusted Partner." It has technical details necessary for actually enabling the interface.

> Analysis: VA could consider which APIs carry a similar security risk and then provide documentation through an analogous process.

Trusted Partner Process - IRS processes 3rd parties through a security vetting process prior to granting them "Trusted Partner" status and allowing them to connect to the APIs.

> Analysis: VA may want to consider this, especially for APIs that allow Creation, Update, Delete responsibilities.

Third Parties Cannot Be Trusted to Use API's as Intended - IRS has observed that partners don't use API's as designed. The example they cited was exceeding the number of planned calls per second due to implementation errors on the side of the third party.

> Analysis: VA could address this both through SLA and and API Management tool. The SLA would define limits on calls to an API. A modern API Management tool could then make this easily configurable, such that the SLA could be operationalized and issues addressed without touching the code base.

Vendor Testing/Release Tempo and Process - IRS fully tests all APIs prior to exposing them to vendors. They then call vendors into a single test environment to validate their own systems gains the APIs. They allow vendors to do this for a two month period before a hard cut-over in production.

> Analysis: - Somewhat counterintuitively, it may be better to minimize interaction with vendors during the testing phase in order to ensure they only have to interact with a stable API. The IRS model of a hard

cutover will not work for VA, who receives claims continuously and who has requirements around establishing the date of claim.