

Sprezzatura

Management Consulting, LLC



VA Microtask - API Governance Executive Summary

PO Box 535 McLean, VA 22101
T: (888) 529-8965
F: (888) 647-0542

A low-angle, upward-looking photograph of a modern skyscraper with a glass facade. The building's structure, including dark metal beams and glass panels, is visible against a clear blue sky. The perspective creates a sense of height and architectural scale.

Contents

- **Deliverables**
- **Review of Process**
- **Research & Analysis Specifics**
- **Recommendations to VA**
- **Team Retrospective**



Deliverables

WHAT WE'RE DELIVERING

- Presentation of Findings (this brief) - PowerPoint-style summary and analysis of our findings targeted at VA executives. It highlights strengths and weaknesses of selected governance models and provides actionable recommendations for governance improvements.
- Narrative of Findings - In addition to the executive presentation, we are providing a narrative summary of research and analysis. This will be in markdown format shareable on GitHub.
- Primary Research Results - We are providing written summaries of all the primary research that backs our findings. This will be provided in markdown format, as well.
- Sprint Retrospective - Separate from presenting our research and analysis, this will critique our efforts and provide VA with lessons learned that may be applied to further research and Microtaskings.

Process Outline Highlights

- Interviews Scheduled/Conducted
 - Contacted 30+ Organizations
 - Conducted 9 interviews
 - Focused on 6 best public and private
- Elements Focused On During Interviews
 - General Business Information
 - API Prioritization
 - Standards
 - Consumer Experience
 - Best Practices/Data Share





Research and Analysis Specifics

Prioritizing Which API's to Build

- **Strength**: A Dedicated User Permission API
 - Analysis: VA already has multiple permission schemes for its publicly facing API's. VA could potentially focus on building or acquiring its own dedicated User Permissions API and exposing that early in its API Platform Program to speed adoption of subsequent API's
- **Strength**: Building API's Above Cerner, Epic and other Provider EHRM API
 - Analysis: We recommend that any API Governance initiative includes a liaison with Veterans Health Administration on forward looking policy questions concerning health data sharing beyond what is maintained within Veteran VistA and Cerner records.



Research and Analysis Specifics

Implementation Patterns

- **Weakness**: Heavy Handed Enterprise Architecture Kills Momentum
 - Analysis: Recommends embedding enterprise level architects in individual teams to provide guidance and not forcing a SOA architecture through a gateway review.
- **Strength**: Defined Partner “Trusting” Process (IRS)
 - Analysis: VA should consider an enterprise level process for trusting partners, especially for API's that allow Create, Update, and Delete to VA data sources.
- **Strength**: Lightweight Whitelisting Process (GSA)
 - Analysis: We recommend that the API platform governance team create tiered templates for lightweight whitelisting and heavyweight whitelisting. These could then be presented as “out of the box” solutions for specific business line requirements.



Research and Analysis Specifics

Implementation Patterns

- **Strength**: Robust Testing Prior to Engaging Third Parties
 - Analysis: Consider minimizing interaction with vendors during the testing phase in order to ensure consumers only have interaction with a stable API.
- **Strength**: When Third Party Testing Is Required, Engage Motivated Consumers
 - Analysis: We recommend that the VA require its contracted developers to be responsible for Reference Implementation testing of their own API'S prior to any final testing with a consumer.
- **Strength**: Provisioning of an Enterprise CI/CD Platform and Associated Training
 - Analysis: We recommend including a developer education and documentation component beyond stanard VIP documentation requirements. Also consider acquiring CI/CD support in a way that doesn't favor a specific developer.



Research and Analysis Specifics

Implementation Patterns

- **Strength**: Not Forcing OAuth2 in Test Environment
 - Analysis: Recommend simplifying the security requirements in the exposed test environment to support easy experimentation with an API.
- **Weakness**: Ancillary Tool Requirements to an API Gateway Tool Increases Licensing Cost
 - Analysis: There's no clear answer on what API tools or platforms to acquire for large federal agencies based on the VA and FS' experience. Early governance could focus on making a decision for a gateway tool factoring in lifestyle cost considerations.
- **Strength**: Purposeful Division of Team on Github to Enforce Architectural Goals
 - Analysis: VA could consider amending VIP and the Rational schema/Compliance epics to encourage API's and Microservices.



Research and Analysis Specifics

Implementation Patterns .

- **Weakness**: Reliance on Non- Cloud Based Legacy Systems Decreases API Availability
 - Analysis: As VA initiates its own Cloud migration initiative it may be worth factoring in the API pipeline when considering prioritization of legacy system migration.
- **Weakness**: Even with Mature Governance, Third Parties Cannot Be Trusted to Use API's as Intended
 - Analysis: VA could address this both through thorough SLA's enforced through an API Management tool.



Research and Analysis Specifics

Consumer/Developer Experience

- **Strength**: Dedicated Evangelism Function (GSA)
 - Analysis: We recommend that evangelism be explicitly addressed in future API Governance initiatives. This evangelism should include external outreach as well as internal outreach to VA development teams.
- **Strength**: Two Tiers of Technical Documentation (IRS)
 - Analysis: VA could consider which API's carry a similar security risk and then provide documentation through an analogous process.
- **Strength**: Use of Peer Review To Ensure a Positive Developer Experience.
 - Analysis: Recommend identifying a small cadre of developers available for this type of review. These outside developers be engaged only when VA feels it has fully mature documentation based on a best practice.



Research and Analysis Specifics

Consumer/Developer Experience

- **Strength**: Copying Best Practices
 - Analysis: We Recommend that prior to any new contracts for API development being written, that a review of some API Developer webpages be performed in order to identify common denominator elements. These can be published in Playbooks, Design Patterns, and required in future contracts.
- **Weakness**: Communicating System Outages in Multilayered Orchestration
 - Analysis: VA could follow a similar maturation path as 1upHealth to provide consumers of its API's visibility into the overall system health. This would include a dashboard webpage and periodic test calls in production.
- **Strength** Designate a Customer Success Engineer.
 - :Analysis: We recommend VA acquire services for such in either a PMO contract or a API development contract.



Research and Analysis Specifics

Consumer/Developer Experience

- **Strength**: Verify Third Party Applications Functions As Expected Prior to Whitelisting
 - Analysis: VA builds and exposes more API's to be consumed by third party applications, it will likely become increasingly difficult to verify those third party apps function as expected for Veterans and other users. As part of its governance model, VA should consider how much governance it wants to place over 3rd party apps prior to them being whitelisted in production.



Recommendations to VA

- **Apply Governance Resources Early to Development of a Partner Trusting Process and Associated Permissions API** - We believe that applying governance early to the partner trusting process and linking that to a permissions API will enable third party developers to interface easily with VA produced API's.
- **Apply More Effort to CI/CD Pipeline Governance and Support** - We recommend that VA provide a single cloud native CI/CD pipeline that any of these teams could use. This initiative would include internal evangelism and training of developers.
- **Apply Governance to the Developer Experience via a Customer Success Engineer or Product Owner** - We recommend staffing a dedicated position of Customer Success Engineer or Product Owner. This position would be responsible for guaranteeing a developer friendly experience for 3rd parties interfacing with VA API's. This position would differ from the Project Manager for an API initiative.



Team Retrospective

- **Research & Analysis Process (primary areas of Lessons Learned)**
 - The four week window provided to complete the microtask was as good timeframe. Our approach to the micro task was focused, but definitely not dedicated resources. Flexibility was key.
 - Collaborative approach, flexibility for interactions, as well as timeframe for deliverables (putting quality over rigid timeframes) were all very helpful in the timely completion of this microtask.
 - Difficult to respond to other available microtasks while working on the current microtask (resource constraints and dollar constraints). Also (relational), difficult to perform work on multiple microtasks at the same time. Challenge of the microtask model. Should add more time to respond to the microtask RFIs (14 days versus 7 days would be helpful).



Team Retrospective (con't)

- **Research & Analysis Process (primary areas of Lessons Learned)**
 - Level of effort of the total team combined may go beyond the awarded \$10K dollar amount for this microtask. Recommend reviewing the dollar amounts associated with individual microtasks to determine the breadth and depth of reasonable scope of work for that particular dollar amount.
 - Appreciated the nimbleness and flexibility, and the streamlined nature of the process (including the RFI/proposal process, the open door policy to ask questions of the government, the flexible time frame offered for working on and completion of the deliverables). Truly, an Agile approach.
 - Responding to the microtask worked well. Good to respond in a public forum through the draft RFI process. Good thing to having sharing online (including others that responded to the microtask; seeing things out on GitHub shared).
 - Maximized the value of each call with the interviewees. Opportunity to do things better (I.e. get interview questions to those being interviewed ahead of time to aid in the call structure and interview process). Establish expectations for follow-up at the end of each call, including opening the door for direct interaction with VA personnel associated with the particular microtask.



sprezzmc.com