U.S General Service Administration (GSA)

GSA IL: Software Pilots

CIO IL 24-01
GSA IT
cto@gsa.gov

Purpose:

This Order establishes the proposal and review process all software pilots must follow. It is designed to ensure pilots are safe, secure, and comply with applicable laws, regulations, and policies.

Background:

OMB M-16-12, Category Management Policy, Improving the Acquisition and Management of Common Information Technology: Software Licensing, dated June 2, 2016, directed agencies to develop processes and guidelines to manage software consistent with OMB policies and guidance, including OMB circular A-130 and the Federal Acquisition Regulation, considering such factors as performance, security, privacy, accessibility, interoperability, and the ability to share or re-use software. This Order updates an existing GSA Order with respect to software pilots.

Applicability:

This Order applies to all GSA employees as they perform their duties. The following are exceptions:

1. The Office of Inspector General (OIG), given its independence under the Inspector General Reform Act of 2008 (5 U.S.C. §§ 401-424).
2. The Civilian Board of Contract Appeals, due to its independent authorities.

Cancellation:

This Order supersedes Section 6(c)(2) of CIO 2160.1G (June 27, 2024).

Summary of Changes:

This Order completely replaces the existing section of the IT Standards Profile that relates to pilots (section 6(c)(2) only).

Roles and Responsibilities:

1. This Order requires The Chief Technology Officer (CTO) to establish a Technology Standards Pilot Committee (TSPC).

2. The CTO shall lead the TSCP. The TSCP shall be responsible for reviewing and approving or rejecting all pilot proposals.

Signature

*/S/*________________________ 9/24/2024___________

David Shive
Chief Information Officer
Office of GSA IT

[Date]

1. Conducting Pilots

When the feasibility or applicability of new information technology is not known or not yet proven, a pilot project can be conducted to explore its use and build a case to become an IT Standard.

- If software is not already approved for use, a pilot must be conducted if it is intended to address new user or business requirements.
- A pilot need not be conducted for new software that addresses pre-existing requirements for which there is already a solution in place, or where existing software gains new features resulting from a change implemented by the vendor.
- Exploratory pilots may be conducted to evaluate emerging technology for which there is no current business requirement.

All new technology software pilots, including hardware with software/firmware components, and those leveraging cloud services, must be conducted in close coordination with the Office of the Chief Technology Officer (OCTO) and the Technology Standards Pilot Committee (TSPC) established herein. Pilot requests should be initiated through the IT Service Desk, which will be reviewed by the TSPC. The process and requirements for pilots shall be as follows:

2. The Technology Standards Pilot Committee

2.1. Pilot proposals shall be reviewed by the Technology Standards Pilot Committee (TSPC), which shall be established and led by the Chief Technology Officer (CTO). The TSPC will evaluate all pilot proposals, set each pilot's limitations as appropriate to the specific technology being piloted, and determine what type of security review is required. The committee will determine whether or not, and with what restrictions, the pilot may proceed. If the pilot proposal is denied, the committee shall provide the reason(s) for the denial.

2.2. In evaluating a pilot proposal, the TSPC shall consider the following factors and apply limitations as necessary:

- Total amount of money that can be spent on the technology during the pilot, including expected labor costs.
- Duration of the pilot.
- Redundancy with other existing technology.
- Likelihood the technology will adequately address the business problem.
- Risks posed by piloting the technology.

- Whether, if successful, the technology's procurement for long-term use would be permitted under procurement rules, regulations, and laws.
- Appropriate security requirements as determined by the TSCP.
- If use of any federal data is authorized for use during the pilot and the risk acceptance/mitigation is sufficient.
- Identify key GSA IT teams or individuals with whom the piloting team must coordinate.
- Any additional reporting required of the proposing team beyond those outlined below in Section 7 below.
- Any additional restrictions required to ensure the safe, secure, compliant, and appropriate piloting of the technology.
- For cloud services, if not FedRAMP authorized, ability to fund FedRAMP sponsorship for the requested technology.

3. Piloting Teams' Responsibilities

3.1. Teams seeking to pilot software must submit a written pilot proposal.

3.2. With their proposal teams must, where applicable:

- Identify the specific hardware and/or software that will be evaluated.
- Propose a budget and timeline, including any associated cloud or infrastructure support costs.
- Identify all key business objective(s) sought through the use of the technology, and show that if successful, the technology will sufficiently meet all intended requirements at implementation.
- Identify which individuals/users will use the pilot technology, and limit them to the minimum number required to evaluate it. These users must be identified in advance of the pilot; however, through mutual agreement between the TSCP and proposing team, the user group can be modified during evaluation as needed.
- Create success metrics by which the pilot will be evaluated.
- Address all additional applicable TSPC consideration factors identified in Section 6(a) above.
- Identify any software (e.g. cloud sandboxes), hardware, or other technical resources required to conduct the pilot.
- Complete a thorough market research and competitive analysis driven by clearly defined and documented requirements that explains the research procedures undertaken and stands up to expert scrutiny. The analysis must identify which vendor or vendors

have been selected for the pilot, and the justification for their inclusion in the pilot. All applicable acquisition regulations must be followed.
- Consult with OCISO C-SCRM team to ensure the piloted technology complies within the secure cyber supply chain risk management framework.
- Include a risk management plan approved by the TSCP to mitigate or accept any risks stemming from their use of Controlled Unclassified Information (CUI), Personally Identifiable Information (PII), any other federal data, and any integration with GSA production systems if applicable
- Anything else required by the TSPC in order to evaluate the proposal.

3.2 While conducting the pilot, piloting teams must:

- Keep the CTO team apprised of key milestones, as mutually agreed upon at the project's outset.
- Alert the CTO team, Office of Digital Infrastructure Technologies POC, and appropriate Information System Security Manager (ISSM) of any potential security risks, either theoretical or realized, once identified. Incidents shall be immediately reported to the GSA Incident Response Team through the GSA IT Service Desk.
- Propose any changes to the TSCP to the pilot's scope before deviating from the approved scope.

3.3. At the conclusion of the pilot, piloting teams must provide the TSPC with a pilot close-out document detailing the following:

- Where applicable, a report of the pilot's findings/outcomes that includes a comprehensive analysis of alternatives comparing the piloted technologies, existing solutions, and the consequences of implementing none of the evaluated solutions.
- A determination of whether or not the requester believes that a piloted technology is an acceptable solution to the stated business problem, including the timeframe for which the technology is expected to remain suitable.
- Evidence that all costs have been identified and budgeted within the requesting office and as required by other affected offices, to include out-year operations and maintenance.
- A proposed path to attain full security, Section 508, and records management approval, if sought.

- A statement, developed with the IT security team, identifying any security risks or blockers the piloted technology would present in the event full approval is sought. For SaaS pilots where the proposed software would require FedRAMP authorization, the piloting team is encouraged to engage with the vendor to determine if they intend to pursue FedRAMP; however, the piloting team may not commit to sponsoring the technology without the explicit approval of the CIO and CISO.

4. Exploratory Pilots

4.1. Where neither a new business requirement exists nor an existing solution is in place, an Exploratory Pilot may be proposed. Exploratory pilots:

- Are appropriate for conducting research into emerging technologies for which there is not a current stated need, but a need is expected in the future.
- Must follow the same approval process.
- Need not produce the same close-out documentation (although the nature of the required close-out must be defined in the proposal phase).
- Because they are not being measured against a requirement, by definition do not provide sufficient analysis of alternatives documentation for full approval.

5. AI Pilots

5.1. If the piloted technology uses AI, it must also be approved by the AI Safety Team via the process defined in the Use of Artificial Intelligence at GSA, Section 2.2 “New or Proposed AI Use Cases.”

6. Additional Policies

6.1. All pilots must comply with GSA IT Security Policy, IT Rules of Behavior, the Order for the Use of Artificial Intelligence at GSA, Section 508 requirements, and Records Management requirements.

7. Exceptions

7.1. Exceptions to this policy, in whole or in part, may be granted by the CTO on a case by case basis. Requests for exceptions shall be sent to cto@gsa.gov.