IT Security Procedural Guide: Low Impact Software as a Service (LiSaaS) Solutions Authorization Process CIO-IT Security-16-75

Revision 7

November 7, 2024

Office of the Chief Information Security Officer

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		Initial Release – May 19, 2016		
N/A	Wilson/ Klemens/ Cozart-Amos	Initial Version of Low Impact SaaS Solutions in Procedural Guide format	Converting Document to a Procedural Guide	N/A
		Revision 1 – March 28, 2017		
1	Eaton/Desai/Klemens	Update to reflect current GSA practice/guidance.	Revise/edit steps required to achieve a LiSaaS ATO, correct guide number.	Section 6.1 throughout
		Revision 2 – June 27, 2017		
1	Feliksa/ Klemens	Update conditions for using the LiSaaS process.	Update conditions to align with GSA CIO Order 2100.1	Various
		Revision 3 – June 18, 2019		
1	Dean/ Klemens	Update to reflect ATO extension guidance	FedRAMP now a requirement for LiSaaS	Throughout
		Revision 4 – March 2, 2020		
1	Desai, Turnau, Klemens	Update to allow 3-year ATO for Very Low/Negligible Risk, Low impact systems. Addition of LiSaaS Solution Profile to determine suitability for LiSaaS and clarification of requirements.	Reflect change in GSA policy and guidance.	Various
		Revision 5 – December 30, 2022		
1	Ciano, Klemens	Updates included: ● Added sections for extensions/renewals. ● Added language requiring MFA. ● Updated user responsibilities.	Updated to reflect change in GSA process and guidance.	Throughout
2	McCormick	Edited for format, content, grammar, reference links.	Align to latest GSA guide formatting and style.	Throughout
		Revision 6 – October 2, 2023		
1	Klemens	Included the step of submitting a ServiceNow ticket to initiate the LiSaaS approval process.	Updated to align with the GSA LiSaaS approval process.	5-6
		Revision 7 – November 7, 2024		
1	Klemens, Peralta, Ciano, Normand	Updates included: ● Included additional criteria regarding very low/Negligible Risk LiSaaS Solutions. ● Added PTA requirement. ● Edited for format, content, grammar, reference links.	Updated to reflect change in GSA process and guidance.	Throughout

Approval

IT Security Procedural Guide: Low Impact Software as a Service (LiSaaS) Solutions Authorization Process, CIO-IT Security 16-75, Revision 7 is hereby approved for distribution.

DocuSigned by:
Bo Berlas
FD7479261615444F...

Bo Berlas
GSA Chief Information Security Officer

Contact: GSA Office of the Chief Information Security Officer (OCISO), Policy and Compliance Division, at ispcompliance@gsa.gov.

Table of Contents

NOTE: Hyperlinks in running text will be provided if they link to a location within this document (i.e., a different section or an appendix). Hyperlinks will be provided for external sources unless the hyperlink is to a web page or document listed in Section 1.3. For example, Google Forms, Google Docs, and websites will have links.

1 Introduction

General Services Administration (GSA) and Federal information security policies including the Office of Management and Budget (OMB) A-130, "Managing Information as a Strategic Resource," require security authorizations for all Federal Information Processing Standards (FIPS) 199 Low, Moderate, and High impact information systems, consistent with Federal assessment and authorization (A&A) processes and CIO-IT Security 06-30, "Managing Enterprise Cybersecurity Risk." Agencies are permitted to utilize commercial cloud service offerings[1] if appropriate security controls are implemented, tested, and reviewed as part of the agency's information security program and protected to the degree required by the Federal Information Security Modernization Act (FISMA) of 2014, FISMA implementing standards, and associated guidance. Cloud service offerings used by GSA are required to be included in FISMA reports.

Current information security requirements are not always practical for certain types of commercial sector cloud computing Software-as-a-Service (SaaS) solutions such as the Low Impact SaaS solutions listed below.

Low Risk LiSaaS Solutions

- Will not be utilized in a permanent capacity at GSA (implemented for a limited duration);
- Involve data already in the public domain or data that is non-sensitive and determined to be FIPS 199 low impact;
- Could cause limited harm to GSA regardless of the consequence of an attack or compromise;
- Have a cost for deployment not exceeding $100,000 annually; and
- Will not impact operations or business processes should they experience a disruption in service or the inability to access the service.

Additional Criteria for Very Low/Negligible Risk LiSaaS Solutions

- Shall have no integration with GSA business systems (exclusion enterprise single sign on [SSO] integrations for multi-factor authentication [MFA]);
- Operates as a stand alone solution;
- Involves data already available in the public domain or data that could be made publicly available, and;
- There are no availability concerns (e.g., should the solution become unavailable, there is no impact to the GSA).

SaaS offerings that adhere to factors listed above will be allowed to use the Low Impact SaaS (LiSaaS) authorization process described throughout this guide. The Office of the Chief Information Security Officer (OCISO) developed the LiSaaS authorization process to provide GSA Service and Staff Office (SSO) Authorizing Officials (AOs) the option of following a more streamlined A&A approach when implementing low-cost market-driven solutions meeting the stated criteria. AOs must consider the following items to ensure that the security controls and contractor practices are adequate before authorizing use and accepting residual risk.

- Federal and agency information security requirements;

[1] For further information on cloud computing, see NIST Special Publication (SP) 800-145, "The NIST Definition of Cloud Computing."

- Agency and organizational security needs;
- Project scope and the data involved to ensure they meet the conditions noted above; and
- Completion of the review activities identified in Section 3.

1.1 Purpose

This procedural guide defines the process necessary to perform security reviews of LiSaaS solutions used within GSA and receive an authorization to operate (ATO) for those solutions.

1.2 Policy

GSA Order CIO 2100.1, "GSA Information Technology (IT) Security Policy," Chapter 1, Section 11, Contractor Operations, states:

a. The appropriate security requirements of this Order must be included in task orders and contracts for all IT systems designed, developed, implemented, and operated by a contractor on behalf of GSA, including but not limited to systems operating in a Cloud Computing environment. In addition, GSA shall ensure that the contract allows GSA or its designated representative (i.e., third-party contractor) to review, monitor, test, and evaluate the proper implementation, operation, and maintenance of the security controls. This requirement includes, but is not limited to, documentation review, server configuration review, vulnerability scanning, code review, physical data center reviews, and operational process reviews and monitoring of Service Organization Control 2 and Statements on Standards for Attestation Engagements (SSAE) 18 reports.

1.3 References

Federal Laws, Standards, Regulations, and Publications:

- FIPS Pub 199, "Standards for Security Categorization of Federal Information and Information Systems"
- NIST SP 800-53, Revision 5, "Security and Privacy Controls for Federal Information Systems and Organizations"
- NIST SP 800-145, "The NIST Definition of Cloud Computing"
- Office of Management and Budget (OMB) Circular A-130, "Managing Information as a Strategic Resource"
- Public Law 113-283, "FISMA of 2014"

GSA Policies, Procedures, Guidance:

The GSA policies listed below are available on the GSA.gov Directives Library webpage.

- GSA Order CIO 2100.1, "GSA Information Technology (IT) Security Policy"
- GSA Order CIO 2103.2, "Controlled Unclassified Information (CUI) Policy"

The GSA CIO-IT Security Procedural Guides listed below are available on the GSA.gov IT Security Procedural Guides webpage.

- CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk

- CIO-IT Security-09-48: Security and Privacy Requirements for IT Acquisition Efforts

The forms/templates below are available on the GSA IT Security Forms and Aids webpage.

- SaaS Solution Profile Template
- LiSaaS Attestation Letter Template
- LiSaaS Solution Review Checklist Template
- FIPS 199 Security Categorization Template
- LiSaaS ATO Letter Template

2 Roles and Responsibilities

There are many roles associated with implementing an effective security program for LiSaaS solutions. Roles and responsibilities for agency management officials and others with significant IT Security responsibilities are fully defined in GSA CIO 2100.1. The following sections provide a listing of the key roles and high-level description of the responsibilities involved in authorizing the operation of LiSaaS solutions.

2.1 GSA Chief Information Officer (CIO)

Responsibilities include the following:

- Developing and maintaining an agency-wide GSA IT Security Program.
- Ensuring the agency effectively implements and maintains information security policies and guidelines.
- Issuing the ATO of the LiSaaS solution for use within GSA. Only the GSA CIO can issue ATOs for LiSaaS solutions.
- Ensuring all LiSaaS solutions have a current ATO.

2.2 Chief Information Security Officer (CISO)

Responsibilities include the following:

- Implementing and overseeing GSA's IT Security Program by developing and publishing security policies and IT security procedural guides that are consistent with CIO Order 2100.1.
- Managing the Office of the CISO which implements the GSA IT Security Program.
- Ensuring that IT acquisitions align with GSA information security requirements.
- Concurring on LiSaaS ATOs.

2.3 Authorizing Official (AO)

The AO is responsible for implementing or integrating with LiSaaS solutions only after they have been authorized to operate by the CIO.

2.4 OCISO Division Directors

Responsibilities include the following:

- Monitoring adherence and proper implementation of GSA’s IT Security Policy and reporting the results to the CISO.
- Reviewing LiSaaS ATO documents when appropriate.

2.5 Information Systems Security Manager (ISSM)

Responsibilities include the following:

- Providing guidance, advice, and assistance to ISSOs on IT security issues, the IT Security Program, and security policies.
- Ensuring A&A support documentation is developed and maintained for the life of the system.
- Ensuring LiSaaS requirements have been met and recommending LiSaaS ATOs where appropriate.

2.6 Information Systems Security Officer (ISSO)

Responsibilities include the following:

- Ensuring the LiSaaS solution is operated, used, maintained, and disposed of in accordance with documented security policies and procedures.
- Ensuring necessary LiSaaS security requirements are in place and operating as intended.
- Advising System Owners of risks to their LiSaaS solutions and obtaining assistance from the ISSM, if necessary, in assessing risk.
- Completing the LiSaaS Checklist.
- Coordinating with System Owners in completing and maintaining the LiSaaS solution deliverables/evidence and ATO.
- Working with the System Owner and Data Owner to ensure a Privacy Threshold Assessment (PTA) IAW GSA Order CIO 1878.3 CHGE 3 is conducted to ascertain that no Personally Identifiable Information (PII) is within the solution.

2.7 System Owners

Responsibilities include the following:

- Ensuring LiSaaS solutions and the data the solutions process meet the requirements of the GSA LiSaaS authorization process, and any additional guidelines established by GSA.
- Obtaining a written LiSaaS ATO prior to operational usage of a LiSaaS solution, including LiSaaS solutions purchased via government credit card.
- Developing and maintaining the LiSaaS solution deliverables and evidence with the solution provider.
- Coordinating with the ISSM, ISSO, Data Owners, and LiSaaS solution provider to ensure compliance with the LiSaaS process.
- Working with the Data Owner and the ISSO to ensure a PTA IAW GSA Order CIO 1878.3 CHGE 3 is conducted to ascertain that no PII is within the solution.
- Monitoring and controlling the data types residing in and processed by the system after initial system categorization (e.g. ensuring that all data in the system stays “low impact/very low impact”).
- If any data type other than low/very low impact data is discovered in a LiSaaS System, the System Owner must immediately report the incident to the LiSaaS ISSO/ISSM.

2.8 Data Owner

Responsibilities include the following:

- Obtaining a written LiSaaS ATO prior to operational usage of a LiSaaS solution, including LiSaaS solutions purchased via government credit card.
- Coordinating with the System Owner, ISSM, ISSO, and LiSaaS solution provider to ensure compliance with the LiSaaS process.
- Working with the System Owner and ISSO to ensure a PTA IAW GSA Order CIO 1878.3 CHGE 3 is conducted to ascertain that no PII is within the solution.

2.9 Contracting Officer (CO) and Contracting Officer's Representative (COR)

Responsibilities include the following:

- Ensuring that new LiSaaS solicitations qualified to use the process defined in this guide include the security requirements from Section 4 of CIO-IT Security-09-48, "Security and Privacy Requirements for IT Acquisition Efforts."

3 Requesting Security Review for LiSaaS Solutions

3.1 Requesting a LiSaaS Software Review

LiSaaS solutions that are not already approved for use at GSA under the LiSaaS authorization process must be submitted via a Software Review Request using GSA's ServiceNow Service Catalog. To submit a ticket, use the link below and on the page presented type "Software Review Request" in the Search Bar, when the selection window opens click on "Software Review Request" as shown in Figure 3-1.

GSA Service Catalog -> All Categories

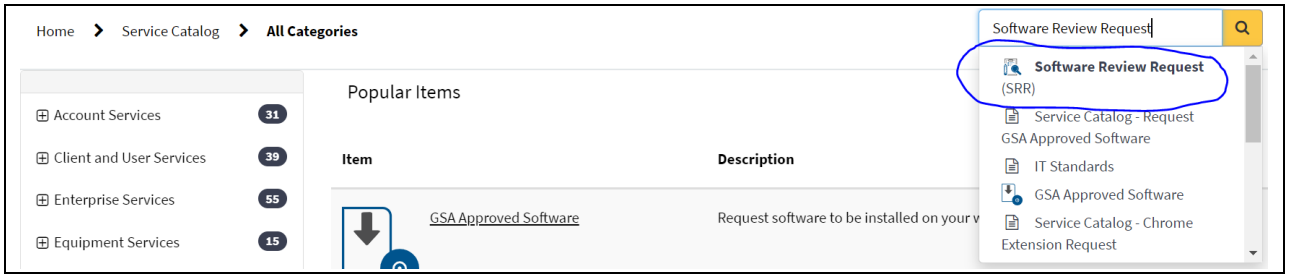

Figure 3-1: Selecting Software Review Request in ServiceNow

Complete the Software Review Request, ensuring that "Software as a Service (SaaS)" is chosen for the Service model as shown in Figure 3-2, then submit the ticket.

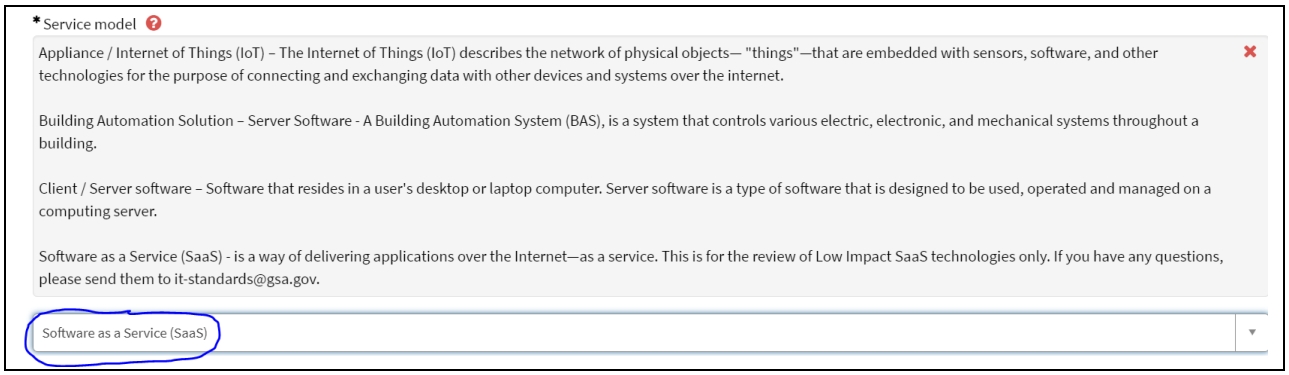

Figure 3-2: Selecting Software as a Service for Service Model

The ServiceNow ticket will be routed to the appropriate personnel to determine if the LiSaaS Solutions Authorization Process should be followed. If the LiSaaS approval process should be followed, follow the steps in Section 3.2 for a security review of the LiSaaS solution.

3.2 Security Review Requirements for LiSaaS Solutions

The LiSaaS solution provider must be able to satisfy the requirements and provide the deliverables listed below, including demonstrating how the requirements are met and verified. The requirements must be satisfied within three months of the start of the ATO process. If the vendor fails to meet this timeframe, GSA will discontinue engagement with the vendor on the LiSaaS ATO process.

In the absence of actual artifacts/deliverables for items 3 through 7 on the list below, a LiSaaS Attestation Letter may be submitted by the ISSO or ISSM. The letter of attestation must indicate how the requirements were verified. Acceptable verification methods are an in-person meeting or a web-enabled call during which the solution provider demonstrates they are meeting the required review activities to the satisfaction of the reviewer. Under this circumstance, in support of receiving an ATO per Section 4, the signed attestation letter provides the documentation and validation of requirements for items 3 through 7 below.

Vendors in collaboration with GSA must complete the following actions to inform the ATO process:

1. Completion of the LiSaaS Solution Profile Template by the GSA Requestor/SaaS vendor. This profile provides a summary of the service function and purpose provided by the LiSaaS solution. It includes the who, what, when, where, and how of the solution, including the following information and capabilities, as applicable. Instructions are contained in the template.
    a. LiSaaS Solution Name.
    b. FIPS 199 Security Categorization Template – documenting data description and sensitivity.
    c. Authentication and Authorization Capability.
    d. Completion of a PTA to verify that no PII is within the solution.
    e. MFA Capability (must be fully implemented).
        i. Provide information on user types intended to use the LiSaaS.
            (a) Internal GSA users – @gsa.gov.
            (b) External GSA customers.
                (1) Other federal agencies/@.gov and @.mil,
                (2) Vendors/@*.com, or
                (3) Public customers/@gmail.com, etc.
            (c) For each user type, provide the anticipated number of users.
        ii. For each user type, specify if a GSA provided identity provider or enterprise SSO platform can be configured for the LiSaaS solution. GSA allows Security Assertion Markup Language (SAML) or OpenID Connect as integration protocols for a SaaS product to integrate with a GSA-provided identity provider or enterprise SSO solution.
        iii. Specify the choices provided for each user type to use MFA.
    f. Role-based Access Control Capability.
    g. Audit Logging Capability.
    h. Encryption in Transit Capability (must be fully implemented).
    i. Encryption in Storage Capability (must be fully implemented).
    j. Connection Type(s).

2. Completion of the LiSaaS Solution Review Checklist Template by the assigned ISSO. The LiSaaS checklist will go into specific detail regarding the actual GSA implementation of the LiSaaS. The ISSO will use this checklist to verify that all information provided in the LiSaaS Solution Profile is accurate and that all security measures have been correctly documented and implemented.

3. Document how system and security parameters deferred to customers are implemented. Do not use the vendor-supplied defaults for system passwords and other security parameters. GSA security policies and best practices should be used to the greatest extent possible.

4. Submit the latest web application vulnerability scan results (e.g., NetSparker, Acunetix, Burp Suite Pro).

5. Submit the latest operating system (OS) vulnerability scan results (e.g., Tenable Nessus, Qualys, nCircle, McAfee Vulnerability Manager). Reference NIST SP 800-53 Control RA-5: Vulnerability Monitoring and Scanning.

    a. Vendors that are Payment Card Industry Data Security Standard (PCI DSS) compliant or have TrustedSite Certification or the Trust Guard Seal may provide the results of their latest PCI DSS Compliant, TrustedSite Certification, or TrustGuard quarterly scan.
    b. Vendors that do not meet the PCI DSS, TrustedSite, or TrustGuard standards listed, must provide their most recent OS vulnerability scan results.

6. Document an acceptable flaw remediation process. Vendors must be able to identify and remediate information system flaws in a timely manner (i.e., the process must describe how often scans are completed and how vulnerabilities are remediated). Reference NIST 800-53 Control SI-2: Flaw Remediation.

7. Provide the results of a Service Organization Control (SOC) 2/Statements on Standards for Attestation Engagements (SSAE) 18 audit report and/or have one of the following vendor certifications: SysTrust, WebTrust, ISO/IEC 27001, or PCI DSS Compliance. The SOC 2/SSAE is not a form of security certification, but it does provide independent third-party attestation of the provider's general operating environment and supporting processes. Vendors may also provide evidence of PCI security assessments, self-testing, and records from other external audits and assessors to supplement the SOC 2/SSAE audit report or vendor certifications.

8. Vendors are strongly encouraged to present as much information as possible to allow an adequate understanding of the application's security posture and a determination of risk. Although the basic requirement is the SOC 2/SSAE audit report or one of the vendor certifications, the GSA AO and the CISO will take a holistic view of the application based on all documentation presented to determine the overall risk of the application as well as any residual risks that may need to be accepted when considering the application for use. If the documentation presented does not provide an adequate understanding of the systems security posture, and/or is deemed insufficient to make a risk determination, additional information will be required.

4 LiSaaS ATO Process

LiSaaS solutions must not have any Critical/Very High or High vulnerabilities identified in their scans before an ATO can be granted.

4.1 Initial ATO

The ATO package must include documentation and validation of the requirements identified in Section 3, and consists of:

- LiSaaS Solution Profile
- LiSaaS Checklist
- FIPS 199 Security Categorization
- Latest vulnerability scan results (e.g., web, OS, container), as applicable
- LiSaaS Attestation Letter, if applicable
- LiSaaS ATO Letter
- Privacy Threshold Assessment (PTA)

The ATO package will be coordinated by the ISSO with the ISSM and OCISO. The ISSM reviews the package, and then the CISO and the GSA AO sign the LiSaaS ATO letter. The ATO shall be valid for:

- No more than one year if the application is determined to be Low Risk based on the evidence provided.
- Up to three years if the application is determined to be a commodity ancillary service that presents Very Low/Negligible Risk based on the evidence provided (see criteria listed in the “Introduction” section of this document) .

Any application granted a one-year LiSaaS ATO must obtain a FedRAMP Tailored (at a minimum) authorization within one year of its ATO. If, within three months of receiving its one-year ATO, progress toward a FedRAMP Tailored authorization has not been observed, GSA will start to cease engagement with the vendor and pursue alternative solutions. For detailed requirements of FedRAMP Tailored Li-SaaS, download the FedRAMP Tailored Authorization Toolkit available on the FedRAMP Baselines webpage.

Note: In all cases, an ATO is valid only if the application license has not expired.

4.2 LiSaaS ATO Extensions

Extensions to LiSaaS ATOs will only be granted in special circumstances, and must be approved by the GSA CISO, and the corresponding AO. Extensions may be granted under the following circumstances:

- The business line requires additional time, not to exceed 3 months, to transition off the current LiSaaS solution, or to transition to another solution that will take its place. This course of action does not require new documentation from the vendor/system owner.

- The vendor will complete their FedRAMP package within 3 months of the current expiration date and needs the additional time to finish the FedRAMP package. This course of action does not require new documentation from the vendor/system owner.

4.3 LiSaaS ATO Renewals

LiSaaS ATO renewals will be treated the same as a new LiSaaS ATO, and will require new documentation, scans, etc. from the vendor/system owner as referenced in Section 3. Renewals for LiSaaS ATOs may be granted when the business line needs additional time to:

- Finish testing the usability of the product.

- Complete the FedRAMP package (requiring more than 3 months).
- Move off the product (requiring more than 3 months).

5 Failure to Meet/Maintain LiSaaS ATO Requirements

If at any time, the vendor is either unwilling or unable to meet any of the requirements specified in this guide, the ATO shall be terminated upon approval of the AO. It is the responsibility of the assigned ISSO and GSA system owner to ensure the requirements continue to be met. Significant changes regarding the LiSaaS solution shall be reported to the ISSM, who with the ISSO, manages the ATO package.

Questions? Contact the OCISO Policy and Compliance Division at ispcompliance@gsa.gov.