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

Revision 4

March 2, 2020

Office of the Chief Information Security Officer

VERSION HISTORY/CHANGE RECORDS

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

Approval

IT Security Procedural Guide: Security Reviews for Low Impact Software as a Service (SaaS) Solutions, CIO-IT Security 16-75, Revision 4 is hereby approved for distribution.

X DocuSigned by:
Bo Berlas
FD717926161544F...

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 this guide are provided as follows:

- Section 4 References - This section contains hyperlinks to Federal Regulations/Guidance and to GSA webpages containing GSA policies, guides, and forms.

- In running text - Hyperlinks 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 webpage or document listed in Section 1.4. For example, Google Forms, Google Docs, and websites will have links.

Note: It may be necessary to copy and paste hyperlinks in this document (Right-Click, Select Copy Hyperlink) directly into a web browser rather than using Ctrl-Click to access them within the document.

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 GSA IT Security Procedural Guide, CIO-IT Security 06-30, "*Managing Enterprise Risk.*" Agencies are permitted to utilize commercial cloud service offerings as long as 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. Furthermore, these services are required to be included in FISMA reports with regard to Cloud Services.

Current information security requirements as noted above are not always practical for certain types of commercial sector cloud computing Software as a Service (SaaS) solutions that (1) are implemented for a limited duration; (2) involve data already in the public domain or data that is non-sensitive and could be considered FIPS 199 low impact; (3) could cause limited harm to GSA regardless of the consequence of an attack or compromise; (4) the dollar cost for such deployments do not exceed $100,000 annually; and (5) a disruption in service or the inability to access the service will not have an impact to operations or business process. SaaS offerings that adhere to Factors 1-5 will be allowed to use this process. Suitability will be determined through completion of a SaaS Solution Profile.

Note: For further general knowledge on cloud computing see NIST Special Publication (SP) 800-145, "*The NIST Definition of Cloud Computing*."

In such cases, the Office of the Chief Information Security Officer (OCISO) recognizes the need for added flexibility to allow GSA Service/Staff Office Authorizing Officials (AOs) the option to implement such low cost market driven solutions following a more streamlined assessment and authorization approach. AOs must consider the following items to assure the security controls and practices of the contractor are adequate before authorizing use and accepting residual risk.

- Federal and agency information security requirements;
- Agency and organizational security needs;
- Data involved and project scope to assure it meets the conditions noted above;
- Completion of the review activities identified in Section 6.

2 Purpose

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

3 Policy

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

a. *GSA System Program Managers and Contracting Officers shall ensure that the appropriate security requirements of this Order are 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 (SOC) 2/Statements on Standards for Attestation Engagements (SSAE) 18 reports.*

4 References

Note: GSA updates its IT security policies and procedural guides on independent cycles which may introduce conflicting guidance until revised guides are developed. In addition, many of the references listed are updated by external organizations which can lead to inconsistencies with GSA policies and guides. When conflicts or inconsistencies are noticed, please contact ispcompliance@gsa.gov for guidance.

Federal Laws, Regulations, and Guidance:

- NIST SP 800-53, Revision 4, "*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, "*Federal Information Security Modernization Act of 2014*"

GSA Guidance:

- GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy*"
- GSA Order CIO 2103.1, "*Controlled Unclassified Information (CUI) Policy*"

The guidance documents below are available on the GSA IT Security Procedural Guides InSite page.

- CIO-IT Security-06-30, "*Managing Enterprise 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 InSite page.

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

5 Roles and Responsibilities

There are many roles and responsibilities associated with implementing an effective security program for Low Impact SaaS 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 high level description and summary of the key roles involved in authorizing the operation of Low Impact SaaS solutions.

5.1 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.
- Issues the authorization of the LiSaaS solution for use within GSA. Only the GSA CIO can issue authorizations to operate for SaaS under this process.
- Ensuring all LiSaaS solutions have a current ATO.

5.2 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 GSA CIO 2100.1.
- Managing the CIO 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.

5.3 Authorizing Official (AO)

Responsibilities include the following:

- Implementing or integrating with SaaS solutions only after they have been authorized to operate by the CIO.

5.4 Office of the CISO Division Directors (OCISO)

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 where appropriate.

5.5 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.

5.6 Information Systems Security Officer (ISSO)

Responsibilities include the following:

- Ensuring the LiSaaS solution is operated, used, maintained, and disposed of IAW documented security policies and procedures. 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.
- Coordinating with System Owners in completing and maintaining the LiSaaS deliverables/evidence, initial ATO, and ongoing maintenance of the ATO.

5.7 System Owners

Responsibilities include the following:

- Ensuring LiSaaS solutions and the data the solutions process meet the requirements of GSA LiSaaS authorization process and any additional guidelines established by GSA.
- Obtaining a written LiSaaS Authorization to Operate (ATO) prior to operational usage of the LiSaaS solution; this includes LiSaaS solutions purchased via government credit card.
- Developing and maintaining the LiSaaS deliverables and evidence with the solution provider.
- Coordinating with the ISSM, ISSO, Data Owners and SaaS provider to ensure compliance with the LiSaaS process.

5.8 Contracting Officers (CO) and Contracting Officer's Representative (COR)

Responsibilities include the following:

- Ensuring new SaaS solicitations that qualify to use the process defined in this guide include the security acquisition language from Section 4 of GSA CIO-IT Security-09-48, "*Security and Privacy Requirements for IT Acquisitions*."

6 Security Reviews for Low Impact Software as a Service (SaaS) Solutions

6.1 Required Review Activities

The LiSaaS solution provider must be able to satisfy the requirements below and demonstrate how the requirements are provided and verified. The vendor must commit to satisfying the requirements listed below, including deliverables, within 3 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 (2)-(6) in the list of required review activities below, a letter of attestation may be submitted by the OCISO IST Director or a member of a review team assigned by the Director such as an 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, per Section 6.2, the signed attestation letter provides the documentation and validation of requirements for items (2)-(6) below.

(1) Completion of the SaaS Solution Profile Template. 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. Data Description and Sensitivity
   c. Authentication and Authorization Capability
   d. Multi-Factor Authentication Capability
   e. Role-based Access Control Capability
   f. Audit Logging Capability
   g. Encryption in Transit Capability
   h. Encryption in Storage Capability
   i. Connection Type(s)

(2) 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.

(3) Submit latest web application vulnerability scanning results (e.g., NetSparker, Acunetix, Burp Suite Pro, etc.). The OCISO can assist with web application scans if vendor(s) do not have an in house web application scanning capability.

(4) Submit latest operating system (OS) vulnerability scan results (e.g., Tenable Nessus, Qualys, nCircle, McAfee Vulnerability Manager, etc.). Reference NIST SP 800-53 control RA-5 - Vulnerability Scanning.

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

(5) Verify that the vendor has 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.

(6) Vendor shall either provide the results of their 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 (American Institute of Certified Public Accountants (AICPA)-sponsored), ISO/IEC 27001, or PCI DSS Compliance. The SSAE/SOC 2 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 SSAE/SOC 2 audit report or vendor certifications. 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 for the SSAE/SOC 2 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 of the 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.

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

6.2 Security Authorization

The ATO package must include documentation and validation of the requirements identified in Section 6.1 and a FIPS 199 Security Categorization Template. The ATO package will be coordinated by the ISSO with the ISSM and OCISO. The ISSO Support Division (IST) Director reviews the package, and then the CISO and the GSA AO sign a 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.

If not already FedRAMP authorized, any application granted a one year ATO must obtain a FedRAMP tailored 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 a FEDRAMP Tailored authorization visit the FEDRAMP Tailored for Low-Impact Software-as-a-Service (LI-SaaS) page.

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

6.3 Ongoing Maintenance

The LiSaaS ATO will be contingent on annual validation of the requirements identified in Section 6.1, including:

- The latest SSAE/SOC 2 audit report, vendor certification, or PCI DSS compliance;
- Annual web application vulnerability scan results;
- Most recent quarterly operating system vulnerability scan results or proof of compliance with PCI DSS, McAfee Secure Seal, or TrustGuard standards/seals;
- Annual recertification that GSA is still using the service.

Note: If an attestation letter was used to validate any of the requirements listed above for the existing ATO, then a new attestation letter or the artifact/deliverables listed must be provided.

If at any time, the vendor is either unwilling or unable to meet any of the requirements, the ATO shall be terminated upon approval of the AO. It is the responsibility of the assigned ISSO to ensure the requirements continue to be met. Significant changes shall be reported to the ISSM, who with the ISSO, manages the ATO package.

A LiSaaS Solution Review Checklist Template is available on the GSA IT Security Forms InSite webpage.

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