10 Ways to Lose Your FedRAMP ATO

Project Hosts™
Security Compliant Clouds

✉ www.projecthosts.com

🌐 info@projecthosts.com

10 Ways to Lose Your ATO

The Federal Risk and Authorization Management Program (FedRAMP) is among the most important cloud compliances for independent software vendors (ISVs). Without a FedRAMP ATO (Authority to Operate), ISVs are barred from selling to the federal government — one of the largest cloud computing markets in the United States. Earning an ATO is hard enough. But maintaining it? That's a challenge in and of itself. **In this eBook, we explore 10 easy ways to lose a FedRAMP ATO that every ISV must avoid.**

1. Failing an annual FedRAMP Audit

FedRAMP compliance isn't a one-and-done deal. It's an ongoing effort that must be maintained through continuous monitoring, testing and remediation.

What could cause you to fail your annual audit? Maybe the auditor is not satisfied with the way that you've remediated vulnerabilities that have arisen during the last year. Maybe this year's auditor has a stricter interpretation than last year's auditor on what is required for a particular control implementation. Maybe a service that your solution depends on has lost its FedRAMP authorization. There are a million possible causes.

If you do one audit per year, it's easy to inadvertently fall out of compliance while you're busy focusing on core business objectives. If you do, it's only a matter of time before you fail an annual audit.

2. Not providing timely and accurate POA&M reporting to your agency sponsor

ISVs are required to submit a monthly Plan of Action and Milestones (POA&M), a document that identifies known weaknesses and security vulnerabilities, as well as activities that will correct them.

Hackers are constantly finding new vulnerabilities in operating systems, databases, middleware, web servers, and other resources. For example, dozens (or hundreds) of new Microsoft vulnerabilities are made public every month on "patch Tuesday." Linux is similar — not to mention databases, middleware, etc. Depending on its severity, each vulnerability has to be remediated in 30, 90 or 180 days. Putting together the comprehensive list of new vulnerabilities along with how you plan to remediate them is a daunting task every month.

But you better not be late in reporting your POA&M — or miss anything — or have unconvincing remediation plans. Lacking timeliness, consistency and completeness in your POA&M reporting to an agency is a surefire way to kiss your ATO goodbye.

3. Missing POA&M remediation timelines

In your POA&M, you're signing up to definite remediation timelines for every vulnerability. Fixing some vulnerabilities will require you to patch an Operating System, database or other software with a patch provided by the developer. Other vulnerabilities will require you to make code changes to your own software. Still, others may require more substantive changes — even to your overall architecture.

Each change must be tested in a test environment and rescanned successfully before it is deployed in production. Sometimes it may seem impossible to remediate certain vulnerabilities within the required timeframes. But missing a deadline? That's a recipe for deauthorization.

4. Not providing supplementary evidence in a timely manner

From time to time, agency sponsors may request supplementary evidence of a remediation or control implementation. Reports from scanning tools are the usual evidence required to ensure a remediation has been completed, but sometimes an agency will request other evidence like screenshots of a technical configuration, or signed statements by an ISV executive (e.g. attesting no use of Kaspersky or other U.S.-sanctioned software).

Other times evidence will be required for implementation of a control that is above and beyond the FedRAMP baseline. Each agency has the option of requiring additional controls (e.g. the NIST PM family, Appendix J privacy controls, etc.). If an agency requests supplemental evidence, you have to act quickly to prove you've remedied the vulnerability or implemented the additional control. If you don't, your ATO is at risk.

5. Inadequately justifying/ documenting new interconnections

All authorized applications are subject to an "authorization boundary," which illustrates an ISV's internal components and external connections.1 An interconnection refers to any "direct connection of two or more IT systems for the purpose of sharing data" and other resources.

According to FedRAMP, for each interconnection of a FedRAMP authorized system, there must be an Interconnection Security agreement signed by both parties. So, if your system interconnects with Microsoft, AWS, Google or some other resource, FedRAMP requires you to get someone from that company to sign your Interconnection Security agreement and approve annual updates. Good luck with that. So, how do you achieve compliance?

Even with an Interconnection agreement, Federal Information cannot be transferred to any non-FedRAMP system. This is particularly challenging due to the fact that FedRAMP has clarified its interpretation of Federal Information to include a wide range of metadata. As a result of this clarification, a number of SaaS solutions over the last few years have lost their ATOs due to using non-FedRAMP cloud services for authentication, log correlation or vulnerability management. Others have lost ATOs by sending usage data back to corporate systems (e.g. billing) — data that has now become Federal Information.

Interconnections have become a hot button for the FedRAMP PMO and many agencies. There are a myriad of ways for interconnections to cause you to slip up and lose your ATO.

6. Not implementing changes to security requirements or controls quickly enough

As the cyber landscape changes, so do interpretations by the FedRAMP PMO about what is required to implement a control. When FedRAMP changes its security requirement and control interpretations, ISVs are expected to stay in lockstep.

Smart phone-based multifactor authentication (MFA) used to be acceptable to FedRAMP. Now only FIPS-compliant smart-card-based MFA is acceptable. Auditors used to focus on verifying that every external connection of your cloud service was encrypted, but did not typically verify encryption of every internal connection behind the DMZ of your cloud solution. Due to new FedRAMP guidance, internal encryption of all traffic (including internal DNS calls) must be enforced.

Changes like these that happen after your authorization could not only require updates to your code, but in some cases an overhaul to your cloud offering. These overhauls must be performed in a timely manner, or you could lose your ATO.

7. Failing to upgrade documentation to FedRAMP Rev 5 by the deadline

FedRAMP models its framework off NIST (National Institute of Standards and Technology) guidelines. Stimulated by the recent release of NIST 800-53 Rev 5, FedRAMP will soon release its own new version of its security baseline, called FedRAMP Rev 5.

Each ISV will have a set amount of time to implement the new Rev 5 controls and upgrade its documentation. If they don't, the ISV's cloud offering will be considered non-compliant and could lose its ATO.

8. Failing to implement CMMC, Ghastly Wealth and other DoD requirements

FedRAMP is just one of several compliances at the federal level. If you're an ISV selling to the Department of Defense (DoD), you're also required to comply with Ghastly Wealth and Cybersecurity Maturity Model Certification (CMMC) requirements.

The difficulty with CMMC is that it is required for DOD cloud services, but the DOD has not yet defined how a company can prove compliance with CMMC. When the definitive guidance comes out, significant changes and even new audits may be required in a relatively short time frame.

Ghastly Wealth requires DOD cloud services with public facing sites to use commercial publicly available trusted certificates. But if those cloud services require security of DOD Impact Level 4 or 5 and are connected to the DOD's private network by way of a "BCAP," then it is very difficult to convince DOD IT personnel to allow use of those kinds of certificates.

In addition to these, there are many other specific DOD requirements that are in flux. If your ATO is with a DOD agency, and you are not completely on top of the latest implementation guidance for these additional requirements, you are at risk of losing your ATO.

9. Getting hacked

This one's obvious: If you get hacked, no more ATO. Why? Because FedRAMP controls are designed to prevent that from happening in the first place. If you suffer a breach, that's a clear sign you haven't met your security requirements.

10. Responding to a security incident in an unprepared fashion

That said, not every security incident is a hack or a breach. Many can be rectified if you're quick on your feet and contain the risk in an organized manner. But if you're slow, unprepared and let an incident go from bad to worse? That's an indication you aren't ready to secure federal data.

The Project Hosts solution

Project Hosts offers ISVs a simpler way to achieve and maintain a FedRAMP ATO. By connecting your application to our pre-audited platform-as-a-service offering and complementary SaaS-level managed services, you offload 100% of the compliance burden to us. That means you can focus less on compliance and more on providing the best cloud solution possible to your Federal agency customers. We continuously monitor, document and maintain your cloud compliance from top to bottom.

Ready to take the pain out of FedRAMP compliance? Contact our team today.

Source

https://www.fedramp.gov/assets/resources/documents/CSP_A_FedRAMP_Authorization_Boundary_Guidance.pdf