Seven Tips for Passing a CJIS Audit

By Clinton Pownall

Cybersecurity has become a top concern for all law enforcement agencies because of the constant threat of intrusion from hackers and other bad actors—both domestic and international. CJIS, which is used by law enforcement and related agencies on the local, state, and federal levels, has been identified as a critically important resource for protection.

As part of its protection efforts, the FBI requires all users of CJIS data to pass a demanding CJIS technical audit every three years. While it isn't uncommon to hear law enforcement agencies recognize the challenges of passing a CJIS audit, the rigor of the audit helps protect us all.

Even the largest law enforcement organizations—those with dedicated IT staff—may find it difficult to pass the onsite CJIS technical audits, without which organizations can't access CJIS information—which would severely limit a department's ability to function. For small organizations, which lack a dedicated IT department, the challenge is even greater.

25 COMPUTER BUSINESS
CONSULTANTS, INC.
1996-2021
computerbusiness.com
407-654-5600

Seven Tips for Passing the Three-Year Challenge

As someone who has long worked with organizations to help them prepare for and pass CJIS audits, here are some tips that may be of value in preparing for these audits.

Tip #1: Ensure CJIS Literacy. For departments with internal IT organizations, ensure that the group makes CJIS compliance part of their day-by-day decision-making process. For smaller organizations, which might rely on a third-party managed services provider, make sure they are CJIS literate and keep compliance as an essential priority.

Tip #2: Demand CJIS Certification of IT Providers. Whenever engaging with third-party consultants to work on CJIS-related systems, demand that they are CJIS certified to do so. I recently worked with one Police Chief who found that his outside vendor not only wasn't CJIS certified, but that he couldn't pass a background check. Protecting CJIS data is mission critical on not just a local, but a national level. Access to the data must be tightly protected.

Tip #3: Once in Compliance, Stay in Compliance. Sounds logical enough. However, the same discernment that goes into passing a CJIS technical audit needs to continue. During the three years between audits, a lot can change: New applications, hacking techniques, communication tools, remote access utilities, security protocols, and cloud-based services. Each change or addition to a department's IT infrastructure must be evaluated in terms of CJIS compliance. The best way to pass your next audit is to remain in compliance from the previous audit.

Tip #4: Document, Document, Document. A major component of a CJIS audit is documenting your compliance. You might have all of the required protections and authentications in place, but unless you can document precisely what was implemented, and in most cases how it was implemented, you may find yourself failing the audit. For example, during the most recent audit cycle, the Federal Information Security Management Act (FISMA) required that U.S. government agencies (and participants in CJIS) had to use the Federal Information Processing Standard (FIPS) publication 140-2 for validating cryptography modules. When working with one police department, it turned out that the wireless service provider they were using couldn't provide FIPS documentation. We solved the problem—prior to the audit—by shifting to a wireless carrier who could provide FIPS documentation.

Tip #5: Prepare a War Room Prior to the Audit. Prior to an audit, each law enforcement department should receive a questionnaire outlining what will be covered in the upcoming audit. This is a good time to create a multi-disciplinary task force to go through each point and verify that the requirement has been fulfilled . . . and that you have proper documentation to prove it was done and done correctly. This kind of proactive approach helps remove surprises, and helps ensure safe passage through the audit process. If you don't have a dedicated IT group to bring into such meetings, include your third-party managed services provider, and if you don't have one of those . . . it would be a good idea to find one, quickly.

Tip #6: Share with Neighboring Law Enforcement Agencies. Reach out to other law enforcement agencies to work together for CJIS compliance. Neighboring departments should already be coordinating efforts in other areas. Create a united war room where you can bring fresh perspectives into how others are meeting CJIS requirements. Agencies recognize that passing a CJIS audit isn't a competition (although I know many small departments that take great pride in passing their CJIS audits that larger departments failed.)

Tip #7: Learn from Those Who Have Just Been Audited. This might sound like a high school kid asking a friend in first period about the math test they won't have to take until fifth period, but this is just another form of research. Don't be afraid to reach out to colleagues in other organizations and even the auditors themselves. Everyone recognizes law enforcement is a team effort. What was it like? What are they looking for? What were sticking points for you? Conversations like this can help make sure that your early planning didn't overlook points that will be in the audit. Those who have just passed an audit will be especially eager to share their experience. One of my clients recalled "I've had agencies contact me after the audit asking for our policy, since our policy was accepted by CJIS. It's nice to have agencies that are several times larger than we are asking us for our policy because they knew that we passed."

25 COMPUTER BUSINESS CONSULTANTS, INC. 1996-2021

Call Us

407-654-5600

computerbusiness.com

When you pass your CJIS audit, take pride in the fact your department has done its best to keep our entire national information infrastructure secure. Even the smallest force receives national critical information from the FBI, the Department of Homeland Security, and the full alphabet soup of other agencies. All of this must be secured.

Hackers and other bad actors are adept at finding one open window from which they can travel far and wide through connected networks. CJIS audits help ensure that all of us batten down the hatches to reduce the risk of intrusion.