Key Questions for a Successful Security Walkthrough

A large part of many security audit methodologies are walkthroughs, where the auditing party will ask to speak to various members of the staff that can answer questions about various elements of the company's security and/or privacy posture. This process is one we find to be extremely helpful for both of the parties involved, as the auditor gets some first-hand insight into the company while the staff is exposed to new considerations about their security posture.

That said, occasionally we see clients worry a bit about preparing properly ahead of time, wondering what sort of questions they might receive over the process, and what types of answers work best for the questions. Well, by and large, the auditing party often will aim to ensure that questions are easily answerable for the invited parties and willing to break the question down further where needed, but it can pay to have an idea ahead of time of what common topics and great answers look like – after all, the quality of responses at this stage affects the quality of the information available to the auditors and, in turn, the quality of the final suggestions and report itself.

To that end, let's take a dive into our common question types and what solid answers look like!

Agendas

The questions you may see during a walkthrough process can vary depending on the type of audit it's being conducted for, as different standards have different criteria that require checking. For the sake of our guide here we'll be focusing on questions seen in an ISO 27001 Audit, as its wide coverage and depth of questions make for a solid baseline of expectations.

It's worth noting that, before the walkthroughs commence, many auditing organizations will give walkthrough "agendas" in advance, with the intention to inform the audited party of some idea of the topics to be discussed and to better help select the staff to attend that walkthrough call. I would highly recommend leafing through these agendas to that end – for best walkthrough results, we would like to see that between all the staff on a walkthrough call that at least one person can speak to each topic.

This often requires different staff members depending on the topic; for instance, of the 13 walkthrough calls and agendas we deliver for ISO 27001, topics vary from organizational context to human resources to cryptography to disaster recovery and beyond. Over the course of the walkthrough process, you can usually count on receiving questions touching on most of the operational and administrative aspects of the business, including roles like leadership, IT administrators, security staff, human resource representatives, and customer service and/or sales representatives.

By this point, you might have an idea of the topics of the calls and whom to invite to each. If not, don't worry; at that event, I'd suggest pulling a representative from each of the roles we just described, and preparing the sections to come!

Question Types

The types of questions you might see on a walkthrough can deviate somewhat depending on the auditor, but the trick is that each question is designed to create an answer for each agenda/standard topic. This means questions can have many form factors: some will be straightforward yes-or-no questions, some will offer a number of options, some will be entirely open-ended, and some will have follow-up questions. But regardless of the form of the question, the design is for the asker to be able to answer to each topic of the agenda/standard on behalf of the audited company, and so ultimately the questions will take the approximate form of the standard's topics.

To that end, we can judge somewhat what the likely focus of the questions will be. But what might the form factor of the questions look like? Let's look at a few of the most common types:

Yes-or-No

These questions are, on paper, the simplest concept. Many questions asked by auditors will be designed as open-ended only if an open-ended answer is needed, so if the question can be answered with a yes or no that's usually the best response! If the auditor needs more information, they can ask follow-up questions afterward.

Example: "Do you have an Information Security Policy in effect as of now?" or "Do you perform data backups? If so, is it on a quarterly or greater basis? Are these backups automated?"

Multiple Choice

These questions are characterized by the auditor asking about a topic and following with some options to choose from, often with the explanation to pick what is closest to the truth. These questions are often given when compliance with a topic is on more of a sliding scale than black-and-white, or when answering a question open-ended would be otherwise tricky. Much like multiple choice questions, the best answers are usually in the options given, maybe with a slight explanation for any deviance you might have from the option you picked if relevant.
Example: “Where do you store your logs? Do you keep them all on-premises, in the cloud, or in some sort of combination?” or “Which of your cloud platforms do you keep security logs on for, between AWS, Google Workspace, Dropbox, and Salesforce?”

Open-Ended

These questions can seem like the trickiest, but typically they’re left open-ended because the answers can vary so much from business to business and require a finer analysis to assess compliance. Answers here do not need to always be long or perfect – a brief sentence or two that could answer a question can often give all the information needed. If more information is required or if the question is hard to answer at first, you often will see the asker give further definitions or follow-ups to the questions, so don’t worry too much about having to concoct a perfect answer all at once.
Example: “What does your employee offboarding process look like?” or “What are the different levels of document classification you have in place? This is thinking things like public, internal, only, confidential…”.

Good Answers

With an idea of the call’s structure, topics, and question types in mind one last concern that can linger is what exactly good answers to the walkthroughs might look like. While with a smart auditor, many questions can be answered in many different ways to a similarly good outcome, there are certain methods to answering that can help increase the speed or efficiency of the walkthrough process. We discussed what good answers look like for each question type in their respective sections in the prior section, but let’s take a quick look at general answering principles that we find to be best practice.

- Concision – Like we touched on in the suggestions for each question type, often the best answer to a question can be the simplest: yes-or-no to a yes-or-no question, or a straightforward sentence for an open-ended question. Many folks are compelled to give the most detailed answer they can, and while that’s appreciated, it’s usually safe to trust that the auditor will ask for any additional detail they’ll require. This is also good practice for answering questions in genuine audits – we don’t want to open doors for further questioning by mistake!

- Objectivity –It's often tempting to give what sounds to be the "right" answers in walkthroughs. But remember that the walkthrough process has the goal of informing the organization's path to improvement, not to deduct points or get people in trouble. If a backup on a critical system has only been performed once or sporadically, don't feel pressured to claim that the backup process is robust and routine – tell us like it is, to the best of your ability.
- Honesty –When we speak of honesty in this context, I mostly mean in terms of speaking to what you know and what you do not. If at some point in the questions you don't fully understand the question or feel certain about the answer to the question, that's OK! Let the walkthrough auditor know and they can give further context to the question or tell you what to look for. Questions can be followed up on later wherever needed, so if a solid answer needs more time or information, that works just fine!

Now, in the end, these principles can help the walkthrough process, but try not to worry about crafting and providing perfect answers on the fly. Of course, we all hope to get good quality information for a good quality assessment. But remember that with walkthroughs the askers and the answers are on the same team with the same goal, so a solid auditing party will help you craft the answers they need. Walkthroughs can often turn out to be a fun process in practice and serve a great purpose in gathering information for the improvement of your organization's security at large. If you have more questions about walkthroughs or would like to speak with us about scheduling one, please contact us at info@cyberdatapros.com – we'd be happy to discuss!