Pratum

An IT Manager's Guide to a Successful Audit

Written by Dave Nelson, CISSP

About the Author

Dave Nelson, CISSP
President at Pratum

Dave is a Certified Information Systems Security Professional (CISSP) with 20 years of experience and a Fellow with the Information Systems Security Association (ISSA). He has lead technology organizations in both the public and private sector. Prior to founding Pratum, he most recently was the Chief Information Security Officer for a leading health informatics company. He also managed an information security group for a top 5 U.S. banking organization, was the CIO for a higher education institution and served as the information security officer for one of the largest municipal governments on the east coast. Dave received his Bachelor of Science degree with a major in Computer Information Systems from Excelsior College. He has also taught and developed information technology curriculum at the post-secondary level, is a published author and speaker at national conferences.

www.pratum.com

Table of Contents

[PART 1]

Introduction to IT Audits

The audit process is one of the most misunderstood and loathed processes in the IT world. A lot of this comes from the fact that the process is not embraced by IT management as an opportunity for a partnership. Once managers realize they can utilize the audit process to highlight some of their own business concerns and objectives, the audit process becomes less adversarial and more about building relationships.

This white paper will provide an overview of the audit process and how IT management can insert themselves into this process to benefit from the exercise. It's important to remember your attitude will set the tone for the engagement. You will get out of the process as much as you choose to put into it. This is a great opportunity to partner with someone who has an objective view of your organization and who in most cases will not be a "yes-person" because they are not trying to sell you products or services as they assess your organization.

IT's Involvement within an Organization

Information Technology departments are typically involved in almost every aspect of a business today. This is great in some respects and not so great in others. IT managers are finding it easier to transition into corporate leadership positions because their IT work exposes them to multiple areas of the company. This also means that whenever a business unit (BU) is audited, IT will be involved to some degree. Even if the audit focus is only on the BU process, the BU probably uses technology at some point in that process. Finance uses an electronic accounting system to store POs, Accounts Receivable/Payable, Payroll, etc.

Auditors will want to know how access to each of these components is restricted, how often access rights are reviewed, etc. Even though IT isn't the focus of the audit, they are still involved in the audit. It's important for IT managers to have a seat at the table during the audit scoping phase, which we'll talk about later.

When IT systems and processes are the focus of the audit, the roles and responsibilities are much easier to ascertain. The auditors are looking at your standard operating procedures. How do you limit access to systems? Is there segregation of duties? How is change management handled? An audit requires that process be documented. Two questions typically arise during an audit. First, how well is the process followed? Second, is the work documented and available to use as evidence that the process was followed?

Common Audit Types

There are various reasons that an audit engagement could occur, but we will focus on three main areas: **Compliance, System Discrepancy and Process Assessment.** These are the audits in which IT would most frequently be engaged. While the phases and objectives of an audit remain the same in general terms, it is important to understand how the audit's focus may change the scope, groups impacted, timelines or other specific details for each audit.

Compliance Audits

Compliance audits may be one of the easiest to work through. Typically, these audits have clearly defined objectives and criteria for achieving a satisfactory rating. The subjective nature of the audit process is limited by the specifics laid out in the regulations. Compliance audits can be broken down into two categories: regulatory and industry. Regulatory audits are the result of legislation being passed and may carry civil and/or criminal penalties for non-compliance. Industry audits, however, are based on standards of one's industry. The biggest risk to your organization is that it may lose the ability to be considered certified or to offer a specific product or service.

Some regulations such as HIPAA are more ambiguous in their requirements and have greater room for interpretation than say the Federal Information Systems Management Act (FISMA). FISMA uses the very literal National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 as its guidelines. It's important to note that except for FISMA, most of the regulations you may encounter are designed to regulate a business practice. The sections that address data security and privacy are only components to the overarching legislative functions.

Most Common Regulatory Compliance Audits

SOX

In 2005, Section 404 of the Sarbanes Oxley Act (SOX) pretty much turned the business world on its edge. All publicly traded companies had to add a section to their annual SEC filing stating that the company's executive management personally attest to the financial statements being filed. This also included an attestation that there be a framework in place to manage controls over financial systems, and that the controls were tested and are deemed effective. The fire drills have subsided, however there is now a focused effort on yearly testing for SOX 404 Compliance.

HIPAA/HITECH

The beginnings of HIPAA focused on the ability of health care payers (insurance companies, Medicare/Medicaid) and payees (hospitals, school systems, physicians) being able to share information electronically. Until then there was no standard

code for a specific diagnosis, method of care, prescription, etc. Once people started thinking about sharing such sensitive data more easily, an emphasis on information security and privacy was added. Most HIPAA audits are internal and focus on how well you meet the compliance objectives. External audits have become more prevalent as enforcement measures were enacted in 2008. In 2009, additional security and enforcement actions were signed into law under the HITECH Act.

FISMA

FISMA standards are the bane of existence for any IT manager supporting the federal government. The NIST SP800-53 standard is one of the most detailed and stringent standards available. A huge benefit, however, is that SP800-53A Guide for Assessing the Security Controls in Federal Information Systems has been published as well. This is the guide for auditing systems against FISMA. It's like having the answers to the exams at the beginning of the course.

PCI

Compliance to industry imposed regulations isn't a new concept. Industry groups have long offered certification for suppliers of goods or services that meet a certain standard. The Payment Card Industry (PCI) Data Security Standard (DSS) is now one of the most prevalent set of requirements IT systems are audited against.

System Discrepancy Audits

System discrepancy audits are sometimes the hardest because they arise out of the fact that things simply don't add up. If the mismatch isn't easily detected, a discrepancy audit is called for. Herein lies the problem. Where do you start? Is the problem in the application? Is it the database? Is it in the data collection tool? Was it simply human error? Could all of the data be collected and stored properly but the reporting system be the culprit? Who knows? Hopefully your systems administrators and business analysts can review the details and provide some intelligent hypothesis on where to begin. That's all it is though…an educated guess. Until you start testing controls and components, you don't know where you stand. You just hope to catch that loose string that allows you to unravel the tangled mess.

Discrepancy audits usually yield one of two results. The first is that a control was weak and allowed someone to exploit the system, either intentionally or unintentionally. This one is a little easier for executives to understand and deal with. You shore up the process or control to prevent a repeat and move on. The second result is that all controls appear to be effective and working properly, however, the discrepancy still occurred. Wow…what do we do now? This is probably going to point to an inside attack from someone with authorized access. Hang on because the ride has just begun at that point.

Process Audits

Process audits are usually very straight forward. You have a body of standards such as NIST, ISO or your own information security policy that your organization has agreed to adopt and utilize to manage your information security and privacy. On a regular interval, you will need to show evidence that the organization utilizes processes and procedures that are in alignment with this body of standards. If the process audit is in relation to a body of standards there are two phases. The first is to **map your process or procedures to the standard controls**. The second is to the **test the control for efficiency, or how well it works.**

If this is simply a process audit there is no need to map these back to any external criteria. The audit will simply be a review of the current effectiveness and efficiency of the control.

Four Reasons to Not Combine Your Audits

Sometimes internal auditors will try to combine audits because they think it will save them time in the fieldwork and reporting process. Auditors are no different than any other profession; everyone looks for efficiencies. However, that approach isn't advised in this instance for several reasons. **First** this creates confusion when trying to identify the objectives and outcome for the audit. Without a specific focus, the audit engagement continues to grow in size, time needed to complete, and resources impacted. The larger your audit, the greater the chance the outcomes will not be meaningful.

Second, sometimes inexperienced auditors don't see how the specific audit relates to your business model. Testing scenarios for compliance may look very different than those for a process improvement. Testing scenarios should be carefully chosen to reflect the focus of the audit. When you combine audits you typically must choose multiple testing scenarios, so you lose the very efficiency you were trying to gain.

Third, reporting becomes a mess when you try to combine the various opinion letters and recommendations. You may have trouble mapping these to regulatory requirements or to remediation plans.

And lastly, you need a "W" in the win column. If all your audits are combined into one big engagement chances are there's going to be something that you need to improve on. This could cause you a less than satisfactory rating. If this is your only audit for the year, executives will only see your 0-1 record and may begin to judge your competency. If, however, you break things down into smaller chunks you may end up with a 3-1 record, which is a much better reflection of your execution of business objectives.

Understanding and Working with Auditors

Not all audits are equal. There are different reasons to audit, so it would be reasonable to assume that audits would be initiated by various groups. We've reviewed a little about how the type of audit can impact you, now let's look at how the auditor can impact you. Ronald Reagan was famous for using the quote "Trust but Verify" when dealing with Soviet Union in the 1980's. This can also be an approach to take with auditors. In general, auditors aren't "out to get you", however, you should always question the motives of the individuals and strive to understand the details of your audit engagement.

You need to ask questions like, "Who do they work for?", "What impact does the audit result have on them?", "Do they have experience in this field?" These types of questions will help you assess the best way to approach and communicate with your audit team. You both have a stake in a successful engagement regardless of whether you "work" for the same company. Your motives for success might be vastly different, but this in no way diminishes the fact that you both need to score a win. An auditor is typically considered successful if they routinely find gaps and provide solid opinions on how an organization can improve. A department is considered to have successfully passed an audit if they have no significant or material gaps that need to be remediated. Acknowledging that we are not perfect, and that we may have room to improve, allows for both the auditor and entity being audited to have a successful engagement.

The first myth that needs to be debunked is that auditors are trolls who live under a bridge and only come out to make your life miserable. Nothing could be further from the truth. In my experience auditors are quite often friendly individuals who have a wealth of knowledge they're dying to share. All you have to do is ask. They typically have seen many different technologies used in companies of all sizes and in various industries. As an IT manager, that knowledge is invaluable. Tap into it.

Many IT auditors today were at one time very skilled technically. So much that the technology now "bores" them and they are interested in helping improve processes used around the technology. Many IT auditors have become Certified Information System Auditors (CISA) by the Information Systems Audit and Control Association (ISACA). The CISA credential requires 5 years of experience and continuing education. As with all professions and certifications, there are those who slipped through the cracks and shouldn't be practicing, but those are few and far between in the IT audit ranks.

Another myth about auditors is that they have no interest in your operational goals and objectives. They want to lock down your organization no matter the cost. While this might be true of some external auditors, think about it for a second. Auditors are just as informed about your company's performance and its impact on their jobs as you are. Typically, bonuses are paid to everyone based on the company's performance. Auditors don't get exempted from this. They are just as concerned about your organization succeeding as you are. They simply have a different perspective of the impacts that gaps in your organization may create for the company. Once you learn to respect that perspective and work with it, your life will become much easier.

Occasionally I hear discussions were auditors are described as "by the book", a "Boy Scout", someone who is inflexible and can't be reasoned with. The only time I've ever seen this is when the IT manager is exhibiting similar characteristics. Then it's usually a matter of pride on both sides, nobody is willing to back down. Almost every audit I've been involved with has resulted in some sort of negotiation as to what is going to be reported as a gap, its criticality, timeline for remediation - the list goes on and on.

Internal Auditors

Internal auditors are probably the easiest to work with because they are your peers. You work for the same company, have the same ultimate boss, understand the company's culture, etc. They're one of the gang. You are able to build a relationship with these individuals because they are available to you. You probably work with them at least on a yearly basis, if not more often. It's like any other relationship. As you spend more time with them you begin to understand their thought process, motivating factors, and communication style. They in turn are learning the same about you and your team. Things get easier with every engagement.

Internal auditors typically have some sort of independent or dotted line reporting structure to the board of directors or other executive management. This helps to ensure a level of objectivity in the audit process. They have a reasonable level of assurance that they won't be retaliated against for finding gaps in a process with fewer levels of management oversight. Don't look at this as if everything they know goes straight to the top, it doesn't. In fact, the board typically only sees the most critical of issues in their reports. This reporting structure is designed to support the integrity of the audit process and not to make sure the head honchos know all of your shortcomings.

Since internal auditors work for your company, their motives are usually somewhat impacted by what's in the company's best interest. Auditors, attorneys, information security professionals, just about everyone struggles with this. How do I balance

what I think is best versus what is best for the company? It is difficult to find the equilibrium, but we all must do it.

External Auditor

If your company doesn't have an internal audit group or you are hoping to add a little bit of independent validity to the audit outcome, a company might hire an external audit firm. While this is typically seen as a good opportunity to get an independent validation, be careful. (Side Note: If you are doing due diligence and have been provided an audit report on a company prepared by an audit firm retained by the same company, you should understand the risk. Obviously, there are criminal or civil penalties for false or misleading statements, but when something can go either way…it's going to go in the direction the money flows. After all, this is an audit firm that is in business to…make money.)

You can still have a level of rapport with your external auditors, but I'd probably be less forthcoming about all of my secrets than with my own internal auditors. Their motives are shared between keeping your business and their obligations, legally and professionally. They also have their own corporate reputation to worry about.

Typically external auditors have very little interest in what happens to your company as a result of this audit. Notice I didn't say they don't care, there just isn't much at stake for them. They are simply there to report on how well you comply with the stated controls. This can be the most dangerous audit to navigate. You typically have very little leverage with these auditors during negotiations so you'll have to win them over with your charm. Find some common ground with external auditors. Something that makes a human connection. Heck…take them to lunch. Even if they must pay for their own meal to avoid a conflict of interest, it's harder to have a real disdain for someone with whom you've shared a meal.

Be very careful what information you provide to external auditors. Don't ever hide information, give half the story, or mislead them. Always think of the Miranda Rights. "You have the right to remain silent. Anything you say can and will be used against you…" Do you remember growing up and your little brother or sister just wouldn't stop rambling on to your mom when you both got caught doing something you shouldn't have? Your mom learned things she would not have otherwise found out about if they would have just stopped talking. Give auditors what they ask for, but don't offer up every piece of information you can find. This subject will be discussed further in the scoping and fieldwork section of a later post.

Communicating Throughout the Audit Process

How you view your audit team will directly impact your ability to communicate and partner with them. If you view this relationship as adversarial, you've got a long road ahead of you.

Communication channels must be established quickly. Both teams need to know the protocol for whom to communicate with and how. One of the biggest concerns commonly addressed by management is poor communications. Finding ways to improve this over the short term certainly won't hurt.

Assigning a single point of contact for each audit helps the transition into and out of the audit run much smoother. It also helps alleviate some of the pressures commonly associated with an audit.

Everything in an audit has to be documented. Purpose, scope, testing scenarios, test evidence, opinions, reports, everything. Get used to the fact that agreements, assertions, and other items which are typically ok in verbal form for day to day operations may not suffice in an audit.

Attitude is Paramount

Your attitude toward auditors will set the tone for the engagement. Try viewing them as a group who is trying to help you become a better organization. With this approach, you immediately want to learn from their experiences, want to hear their insight, want to mine as much knowledge from them as possible. This is the basis for a great audit engagement.

When someone sees the opportunity to build a relationship with you, they typically take a different approach to their interaction. "You work with me…I'll work with you." We're all the same at some basic level. We want to be liked and respected. Keeping things on an even keel with professional courtesy and respect will enhance your experience.

When your staff members see you take this approach they will begin to emulate it. They will try to work with the auditors and find solutions that benefit both parties. If, however, you close your office door and mock the auditors or their work, your team will also exhibit this behavior and it will be hard to hide. Their approach to the engagement will be evident and your true colors will be discovered by the auditor.

Communication Channels

Communication channels must be established quickly. Both teams need to know the protocol for whom to communicate with and how. Will there be weekly meetings? Who should attend? Will minutes be taken and shared? When do we escalate issues? It's often best to take care of things at the lowest levels. This is where most of the knowledge is and it just makes sense. Give people the benefit of the doubt when following up. Perhaps they just missed an email or voicemail. Maybe they forgot. Usually people aren't trying to dodge you. This isn't an excuse for repeated communication gaffs or a lack of professional courtesy. Just don't be too quick to judge if they've only missed one phone call.

Get every request from the audit team in writing. It is inevitable that there will be miscommunication. These are two teams who don't regularly work together. They are forced to complete a high visibility project in an extremely short timeframe. Getting requests in writing minimizes the chances of miscommunication. You also need to enforce with your team that they aren't to make assumptions as to what has been requested. If they don't understand, or have suggestions that may yield better results, have them take this to your point of contact for review with the audit team.

Single Point of Contact

Assigning a single point of contact helps ensure consistent communications and processes. The audit timeline is typically very short. Auditors have a "production" schedule just like the rest of us. They want to get in and get out as quickly as possible. Delays in your audit means possible impacts down the road. Learning how to communicate with a large group of people or trying to interpret how each individual processes information is time consuming. You don't have this luxury during the audit process. Giving the audit team a single point of contact gives them some reasonable assurance that your team will be available when needed.

By identifying a single point of contact from your team, you can minimize the operational impacts. This will be accomplished by reducing the number of duplicate requests and having an experienced staff member scope and review test scenarios before they are given to your team. There is nothing worse than spending hours gathering evidence for an auditor and then being told after a 5-minute review that the data isn't what they needed. Sometimes auditors are just a little overzealous as well. They want to find that big issue that's going to look great to a performance or promotion review board. They'll take as much access to your team as you'll give them. While you don't want to hinder this access, you certainly need to control it. The single point of contact ensures questions are being directed only to those who have the answers.

Get it in Writing

Auditors want to see everything in writing. Having a policy or procedure your team follows can only be validated if it is written down. Using undocumented controls or procedures isn't a bad thing. You won't be cited for using them unless they contradict your existing documentation. In most cases, you'll be cited for not having a written, repeatable process. Management may have to get involved in this case as not everything can be written down. You may have some wiggle room if you can show that a written procedure would create a hardship, isn't cost effective or doesn't mitigate any risk. You'll be hard pressed to find many examples of these cases though.

You are going to create mounds of documentation during an audit. Therefore, the scoping activity discussed in our next article is so important. Typically, auditors will want to run reports based on certain criteria to show evidence a control is working. In some cases, such as system configuration, you might not be able to run a standard report. You might be able to provide a configuration file or possibly a screen shot to satisfy their needs. Either way your team needs to be prepared for the effort required to identify sources, specify report parameters and then run the reports. You'll usually underestimate this your first time through, so add a buffer to the time lines. It is better to under promise and exceed expectations than the other way around.

[PART 4]

The Audit Process

The audit process can vary from engagement to engagement, company to company, or even auditor to auditor. What you should find though is that IT auditors take a consistent approach to the engagement. The phases may have different names based on the environment, however the actual function of each phase should be consistent. It's very important for you to fully understand the phases of your audit to ensure you can have the appropriate resources and input available at each stage. It's very similar to the SDLC (Software Development Life Cycle). It's much easier and less costly to get all requirements for the project up front so no future work has to be scrapped.

The phases as I describe them are the initial Announcement of an upcoming audit, delivery of the Engagement Letter, Scoping Activity and Self-Identifying Gaps, the actual Fieldwork or Control Testing, and the Reporting phase. We'll talk about these in detail starting with the purpose of each phase and the role of IT management during that phase.

The Announcement Phase

The announcement phase of the audit is simply a time for the auditors to announce their intentions to audit a group, function, system, etc. Most internal audit departments try to plan their work out in advance just as you do. They may even know a full year in advance what their anticipated schedule is going to be. There probably won't be any details released other than a name for the audit, the audit manager or team leader, and a preliminary date. Be prepared as the further out the date, the more fluid it will be. The audit schedule is no different than any other operational group. Timelines slip due to personnel, weather, technology and other business drivers. This is only meant to give you the opportunity to see what's coming and begin preparation.

The timing of audit announcements can be brutal. Sometimes audits are on a cycle and you know to expect them every quarter, every other year, etc. These audits are much easier to plan for. The associated workload is known and you'll have a staffing plan to deal with it. You know you're going to have certain resources tied up with the engagement and you simply plan around it. Sometime though you get no warning and the auditors show up. Those are usually the audits that are the result of some other situation that didn't go as planned. You might not have known the timing of the audit but you probably won't be surprised that it is occurring.

The announcement phase of an audit is the key time for you as an IT manager to begin preparing for an audit. This is also the phase that most of us ignore, which costs us dearly. Once an audit is announced you should have ample time to begin getting ready for the auditors to arrive. Take advantage of this time as once the auditors are on site they will expect that you have already done your prep work and will be ready to move. During the announcement phase you want to begin collecting and centralizing all information that might be requested during the audit. Things like system documentation, work or change requests, policy, procedures, risk analysis information or penetration testing results. You may want to develop some sort of documentation portal where you can store the information and give the auditors granular access for a given period.

A big item that is often overlooked is review of any previous audits. Do you have any outstanding issues that need to be resolved? This is going to be the first thing on an auditor's check list. Leaving things like documented remediation plans unaddressed is one of them. Go back and make sure everything you said would be done after the last audit was done and that the appropriate documentation is completed. What do you think your chances are of getting a warning when the police officer pulls you over for speeding and upon checking your license sees that you have a drawer full of unpaid violations?

Assigning a POC for the auditors at this point makes sure you are kept in the loop regarding any changes. Should the intended purpose or timelines change, you will want to be the first to know. You should also begin to plan for resource utilization if you haven't already. Audit response can be time consuming. You need to make sure your people have availability during the engagement. If you see any red flags talk with your auditor. Now is the time to try and adjust the schedule, not three weeks before they are on site.

Ideally you have a self-assessment process, where you have continual process and system reviews to identify any gaps and work toward remediation objectives. If your organization doesn't have something like this, now is the time to start. You certainly don't want to appear lazy or negligent during this process.

Engagement Letter

The role of the engagement letter is for the audit team to spell out their specific objectives for this engagement. Perhaps they want to assess HIPAA compliance or review the effectiveness of your identity and access management controls. Their intentions should be clearly defined along with proposed timelines for each phase of the engagement. This is also a time for the audit team to introduce themselves to the business unit. Knowing who is on the audit team and what their role is will help the entire engagement flow more smoothly.

Besides just stating the objectives for the audit, the second major issue addressed by the engagement letter is to scope the audit. This entails determining which systems can be reviewed and the look back period (date range for review) among other details. This information is often just a best guess from the audit staff as they probably don't have the specific system knowledge to know if this scope is too big or too small to accomplish the stated objectives.

Once you receive the engagement letter you should begin to scrutinize the details. Are the dates as expected? Is the objective clear? Has it changed from the initial announcement? Is the scope too broad or too narrow? This is the time for you to drive the engagement. There are 4 key action items you have during the engagement process.

1. Do you agree with the overall time line for each phase of the audit? Auditors are famous for trying to get in and get out as fast as possible. You know what the operational impact is going to be on your systems. Perhaps you'll need to run 10 reports, which take 4 hours each to generate and you can only run them in your evening maintenance windows after the backup has run. This might mean you can only run one per night, and it will take you ten days just to run the reports. If the auditor has an expectation to be done with the evidence gathering in 5 days, you need to explain why this is unrealistic and negotiate the timeline. Don't drag things out just to play it safe though. Remember, the longer the auditor has to review and look over things the more they uncover and the more they want to probe, thus possibly expanding the scope of the audit.

2. Set clear objectives for the engagement. Understanding what the auditor hopes to accomplish will help you in the next phase, scoping. This is no different than getting business requirements from an operational unit before you begin coding their application. You should understand what they want to do before you can provide them anything. Another key in this is understanding definitions. Acronyms and abbreviations mean different things to different people. Even within the same company acronyms may be used differently by different business units. Agree up front to how you'll communicate these items. Also, make sure to clarify what someone means when talking in technical terms. People often throw around the terms authorized and authenticated interchangeably when discussing access controls. Make sure the term someone says is the term they mean.

3. Find out if the auditors have any pre-existing concerns about your organization or the systems. Unless you like being blindsided during the reporting phase this is your time to get all the cards on the table. If an auditor has anything they are looking for upfront they should tell you. It's not fair for you to be judged on criteria you don't know about. You may also find you have some perception issues you'll need to work through to make this a successful engagement.

4. Take this time to gain some visibility into your problem areas. Do you have any gaps that you've tried to get funding for but it just hasn't been a priority with management? That gap becoming an issue in the auditor's opinion report is sure to change this. Be careful though. This is a double edge sword. Your management may view this as an underhanded trick to get your pet project pushed through, or if it becomes a big issue you might be on the hook for not having responded to it earlier. Trying to balance getting visibility to known problem areas and just continuing to work them in the background takes some experience. I wouldn't recommend trying it on your first pass.

Scoping Activity and Self-Identifying Gaps

The purpose of the scoping activity is for the auditors to tell you what systems they plan to review, what the look back period will be, how many samples they plan to take, what the sample sizes will be, etc. Some of this information will be based on their previous experience with your organization or system. If this is an internal group that has performed the same audit several years in a row, their initial scope may be right on. If, however, this is the first time the audit has been performed, the team membership has changed, or the system has gone through a major revision, this might not be the case.

During the announcement phase you should have been going through a self-assessment and looking for gaps. That exercise may have resulted in some remediation plans. Most auditors will allow you to provide them with information regarding known gaps up front. If you have an action plan and have made significant process on the plan this can help improve your audit rating. Auditors are more concerned with ensuring things are done right than with who gets credit for finding the gap and making the changes. The scoping phase is a good time to disclose self-identified gaps. Some auditors prefer this happen during the engagement negotiations so be sure to check their expectations.

If negotiation isn't one of your strong suits, you either need to develop your skills in this area or have someone on your team who can do it for you. Auditors are driven by best practices and repeatable processes. If the auditor feels you're trying to get around these during the process, they will certainly push back. If you have a need to change the scope of your audit for any reason you need to be prepared to justify your reasoning. Thinking something will work better probably won't be enough to sway an auditor. You and your team need to utilize your specific knowledge of the system architecture and operation to explain why the scope needs to be modified. For example, maybe the audit scope includes reviewing any authentication process for user of a web application. In the architecture diagram provided to the auditor there is a proxy or load balancer in the middle. With your expert knowledge, you could explain how these devices have no direct impact on the authentication

process and the logs can be excluded from this audit. The auditors will rely on your knowledge to help drive the scope. They don't want to review meaningless data any more than you want to collect it for them.

Fieldwork and Control Testing

Fieldwork is the phase where most of the heavy lifting will take place. One of the first things an auditor will ask for is information relating to your process and procedures. They want to see how well these accomplish the successful implementation of your policy and related control standards. Some of your controls may not be documented. They will try to discern this during the fieldwork process. They will interview system administrators to determine how they perform their duties daily and then check for supporting documentation. Having written operating procedures is always best. Even if you're doing the right things, if it's not documented you can probably expect that issue to be noted on your final review. Without the written documentation, there is no level of assurance that the process will be repeated the same each time. Staff transition or a disaster could prevent the regular administrator from performing their duties and cause the process to be changed if not documented.

Once the auditor has identified all of the controls, they will review for effectiveness. Before even looking at the system, the auditor will try to ascertain if a control can meet a policy objective. They will look at the control and assume it has been implemented correctly and consistently. They will also consider the technology aspect of the control and the system it was meant to protect. If there is significant chance a policy could be violated even with the control in place it probably isn't going to be considered an effective control and will need to be reviewed. Sometimes this just means modifying the written documentation for the control to better reflect its design and other times you'll need to scrap the control and start over.

Once the effectiveness of the control has been considered, it will be reviewed for efficiency. This is the point we see how well something works. While the control may be deemed effective it may not be working well in the actual implementation. Perhaps it was implemented incorrectly or the process isn't being followed. Many things can impact a control's efficiency.

Since fieldwork is where the auditors begin to dive into your technology environment, you have home field advantage. Nobody knows the environment like you, so take advantage of that. Walk through your systems with the auditor to give them a personal connection to your team and environment. The more they understand the technology architecture, the easier it will be to negotiate with them to correctly scope the audit. Assigning a senior staff member as the point of contact assures the auditor you take this engagement seriously and want to do everything you can to make it a smooth process. You also get the benefit that if the

auditor tried to exceed the scope of the audit, your staff member will know the system well enough to catch and adjust the auditor's focus.

Review Prepackaged Testing Scenarios

Some auditors come with prepackaged or predetermined testing scenarios. Make sure you review these. They may or may not be appropriate for the way your environment is designed. Databases and directory services are prime examples. Both can be customized to the point they almost seem like in-house developed solutions. The standard fields an auditor tests may not be in use or may be used in vastly different ways by your organization. It's important that both of you understand this before going through the laborious process of pulling data. Don't be afraid to suggest scenarios you think will yield the results the auditor is looking for.

Many times, auditors ask for a report having no idea what the result of that report will be. I once worked for a company where an auditor wanted to see every manager's certification whose access for their staff members was still valid for every Active Directory account in the company. Once I explained that we had over 210,000 accounts, this would take about two days to run and would print out on about 30,000 pages they changed their tune. We were allowed to run smaller samples from several business units and finished with about 40 managers, 200 accounts and 5 pages. This was a statistically valid sample of the accounts, which would indicate if the control was efficient. Work with your auditors to find valid samples instead of testing the entire environment.

Reporting

Section 1: Opinion Statement

The first thing in the auditor's report will be their opinion statements on the overall effectiveness and efficiency of the controls in your organization. If all goes well and there are no major issues to report this should be succinct. In an internal audit, this will usually be no more than a couple of paragraphs and high level in nature depending on the system complexity and audience for the report.

External or regulatory audits are another story. I hope you like to read. In most cases, there will be an executive summary section if the opinion section is more than a few pages. If your auditor has uncovered multiple deficiencies, then the report will be as long as it needs to be to accurately describe the impact.

Section 2: Recommendations

The second portion of the report is the recommendations section. Auditors can't be too specific here as this would cause a conflict of interest when they next review the control. If they tell you step by step how to fix it and then pass the control in the next round, their motives would be suspect. If they again failed the control, you'd be none too happy with them. For this reason, they will tell you what needs to be fixed but not how to fix it.

Remember that this audit process has been a partnership between you and the audit team. It should be expected you will want to help shape the final report. After all, it is at least to some degree a reflection of how well you and your team do their job. You certainly don't want your signature on a scathing report that you had no input on. If an auditor balks at getting your input included in the final report, this is a red flag that must be addressed immediately.

You should also agree with everything on the report. You may not like everything that is stated or how it is stated but there should be no assumptions. Only facts should be reported and these facts should be backed up with evidence from the fieldwork. Feel free to challenge the auditor and show additional evidence of your own if you believe the report to be inaccurate. It's important to get these issues cleared up while the report is in draft format. You want a limited audience to see the "dirty laundry". Once the final report is published it's hard to have it changed.

During this phase, you'll also need to develop a timeline for remediating any identified control deficiencies. A little trick I like to use is to commit to building a project plan by a certain date but not to fixing the problem. Most times you have a week or two at best to review the draft report and build a management response. There is little chance you'll fully understand the changes that need to happen or the impact on budget and operations. Committing to building a project plan shows you're serious about fixing the problem but realistic about potential impact. Most auditors are fine with this because you will be tracking and reporting progress as you go. Just remember this needs to be fixed before the next audit cycle.

Summary Tips for a Successful Audit

Summary Tips for a Successful Audit

There are some things that are sure to sink an audit engagement. They are easy to avoid; however, I see people fall into these traps all too frequently. Simply knowing what some of these are should enable you to identify them and hopefully avoid them.

- The first is lack of communication. I probably don't need to spend much time describing what this does to a relationship. For this engagement to be a partnership you need to communicate effectively with your audit team. This means regular meaningful communication. It also needs to be a two-way street. If you feel a staff auditor isn't forthcoming with information, escalate to the team lead or audit manager. Explain how you view this as an opportunity to partner with them and want more from the engagement. I've never known a manager, audit or otherwise, to turn down this type of offer.

- Defensive attitudes have no room in an engagement. The auditors are simply doing their job to assess the controls of your environment. Nothing they do or say should be taken out of context and assumed to be an attack on you or your team. They are about the most objective group of individuals you'll ever meet. Every profession has "that guy". The one who lives to make life miserable for everyone around them. You might even know one in your line of work. If "that guy" happens to be your auditor, take the high road. Nothing good will come out of doing battle on a matter of principle. Do your best to work with auditors as professionals and your engagements will run amazingly smooth. Cop an attitude and you're in for a wild ride.

- If you're not willing to take time to complete the simple tasks, what does this say about your organization? While most technology professionals loathe creating documentation it is one of the easier tasks. Auditors will key on this every time. Spend the time and document your process. Not only does this make for a more successful audit, it helps with disaster recovery planning, cross-training, and reducing support costs.

- Talk with your auditor about their expectations and explain yours to them. It may be unrealistic for you to expect to have no gaps or deficiencies. Working with your audit team to communicate and document expectations will reduce the chance that one or both parties are completely surprised during the reporting phase.

- There is no substitute for management involvement in an audit. The more active a management team is in the audit the better chance for a satisfactory rating. I'm not advocating that a manger be the point of contact or run the audit engagement. They do however need to attend the kick off meetings, negotiate scope and time lines, provide input during fieldwork and influence the final report. If your team sees you interacting with auditors, they will take their cue from you. Hide and they'll hide, build partnerships and they'll build partnerships.

- Having a single point of contact works best for both teams. The auditors don't waste time tracking down the individuals responsible for a certain function or for documentation. Your team isn't constantly interrupted to provide testing evidence or documentation. The point of contact becomes the mediator. They can help narrow scope, revise testing scenarios and work with the auditor to streamline the request before it gets to your operational teams. Having a good point person working with auditors is invaluable. If you are in a highly regulated environment, such as banking or healthcare, having a person dedicated to working with auditors, tracking remediation plans, or writing management responses is a necessity for most mid-sized or larger organizations.

- Negotiate a win-win situation with the audit manager upfront. Find out what they want to accomplish through the audit and tell them your objectives. Find some common ground and work to build a scenario which gives you both the best opportunity to succeed. Failure to do this step is only going to hurt you. The audit is going to happen with or without your input. You might as well make the best of it and find a way to turn this into a positive experience.

- Preparing for an upcoming audit is essential. Start building audit prep into your daily routine. Make sure documentation is part of the build process. Tie operational processes to policy or control statements. The more work

you do to prepare for an audit the less you'll have to do during the audit. I'm usually more successful and comfortable performing tasks according to self-imposed deadlines than to seemingly arbitrary deadlines imposed by others.

- Self-audits are a great way to prepare for an audit. If you've gone through an audit you can use the same testing scenarios from the last cycle. This can be used as a dress rehearsal for your next audit. Your team will be better prepared and equipped to respond during the actual audit. You also get a sneak peek into what's happening in your organization.

  One of the things I always hated was finding out from an auditor that my team had decided at some point to not follow documented procedures without telling me. Sometimes they just changed the procedures to meet operational goals and in most cases the changes were warranted. However, if they aren't documented, you're going to be cited for this. Being able to identify gaps earlier and address them behind closed doors is one of the greatest values of the self-audit. If you do this frequently enough and your audit cycles are long enough the discrepancy might not even be found by an auditor based on their look back period.

  Having gone through the self-audit will give your team the confidence they need to interface with the auditors and build a solid relationship with them. Hopefully this will help bridge any communication gaps and reduce confusion during the audit.

There is no way to ensure you're going to come out of an audit unscathed. You can however minimize any potential negative impacts by being an active participant. The worst possible thing you can do is to let what happens, happen. This is a naïve and dangerous approach. By building relationships, engaging in the entire process, communicating and negotiating with the audit team, you stand a very good chance of improving the rating you would have received otherwise and are at least somewhat in control of your destiny.

Pratum

www.pratum.com

515-965-3756