Conducting an Efficient IT Risk Assessment to Comply with HIPAA

How to Do It, and Why You May Need to (Even if You Aren't in the Healthcare Industry!)

Mark Lachniet, Solution Architect, CDW Corporation

Version 1.0

Monday, July 28, 2014

CDW LLC, 200 North Milwaukee Avenue, Vernon Hills, IL 60061 — 800.800.4239

Table of Contents

Overview

As a solution architect for CDW, I consult regularly on Health Insurance Portability and Accountability Act (HIPAA) compliance projects for a variety of industries that handle protected health information (PHI). Hospitals, medical billing companies and law firms are particularly interested in assessing their security and compliance posture. In the following document, given the caveat that I am not a lawyer and am giving my subjective opinion, I give an overview of the types of organizations that should be doing HIPAA assessments, describe the four most essential components of an IT HIPAA risk assessment, provide links to specific resources and tools you can use, briefly describe some of the decisions to make about the parameters of your risk assessment, and provide templates for the types of tasks I have seen undertaken by organizations. This general methodology could be used for any assessment project with a compliance component such as one to assess alignment with the Payment Card Industry (PCI) credit card rules or the Gramm–Leach–Bliley Act (GLBA) for financial institutions with a few minor changes.

Do You Need a HIPAA Security Risk Assessment?

If you are subject to HIPAA compliance, you are required to perform regular risk assessments as per CFR 164.308(a)(1)(ii)(A). Even if you aren’t required to comply, it still represents an attempt to establish best practices and standards. And you can start with the methodology presented here. In the past, HIPAA compliance was primarily a concern only for healthcare organizations, organizations that manage their own medical plans, and related industries. If you weren’t in one of these relevant fields and handled PHI, your responsibilities were probably governed by a business associate agreement (BAA) with an organization that *was* required to comply. These agreements were a hassle to maintain and keep current, and tended to be lacking in specific requirements — particularly regarding information security. It was a painful and costly system for both healthcare providers and their partners (with the possible exception of the lawyers negotiating the agreements). Fortunately, this system was simplified and clarified by the 2009 HITECH act that changed the rules by making "*business associates of covered entities directly liable for compliance with certain of the HIPAA Privacy and Security Rules' requirements.*"

Still, compliance can be complex and would best be discussed with legal counsel. If your organization views, stores or communicates PHI, particularly as a service provider, there is a good chance that you may be a business associate and thus required to comply with HIPAA, and hence perform risk assessments. As per 45 CFR 160.103, this includes "***legal, actuarial, accounting, consulting, data aggregation** …, **management, administrative, accreditation**, or **financial services** to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates*." Thus, with a few exceptions, if you are in any way seeing another organization's PHI in your official capacity, you probably need to comply with HIPAA. If you are a healthcare provider, there may also be financial incentives for performing certain tasks, including risk assessments.

What Kind of Risk Assessment?

The good news is that HIPAA compliance does not require any particular way of conducting a risk assessment. You are allowed, and indeed encouraged, to design an assessment that makes the most sense for your unique circumstances. That is not to say that there isn't plenty of guidance available to help you. There are a number of good resources from any number of sources for help with risk assessments, including software such as the HealthIT.gov Security Risk Assessment Tool and written methodologies such as the National Institute of Standards and Technology 800-30 "Guide for conducting Risk Assessments." Indeed, the variety of tools, whitepapers and checklists can be daunting, and finding the time and expertise necessary to implement them can be problematic.

Setting Your Assessment Goals

To put it bluntly, is your goal simply to show enough due diligence that you can say you have made an effort? Or do you actually care about making a lot of significant improvements and reducing risk? Or are you somewhere in between? Consultants often jokingly call the former case a "checklist risk assessment" because it is conducted as cheaply as possible just to put a checkmark in a box on a list of requirements. These assessments rarely make any difference to the organization other than meeting organizational requirements or passing a superficial external audit. On the other end of the spectrum is a comprehensive and actionable assessment involving technical and procedural components, involvement of stakeholders from diverse areas of the organization, and prioritized and specific suggestions for improvement that can be tracked and acted on over time.

Obviously, there is a wide range of effort that one can put into a risk assessment. Indeed, it is easily possible to do *too much* risk assessment and security work, to the point where the costs of your prevention efforts are greater than the benefit to the organization. The level of depth to pursue is a business decision that should be made by senior management, informed by subject matter experts in IT, security and compliance. On the one extreme, I had an IT director tell me that the management at his law firm had explicitly told him not to implement *any* real security (such as non-guessable passwords) and that they would simply litigate the issue if something bad happened. On the other extreme, many compliance and security professionals oversell the business case for security and risk assessments by promoting fear, uncertainty and doubt (FUD) too often and too loudly, thereby lowering their credibility (and often shortening their tenure at the organization). The correct answer lies somewhere in the middle, and varies based on the organization’s maturity, budget and risk.

Risk Assessment Components

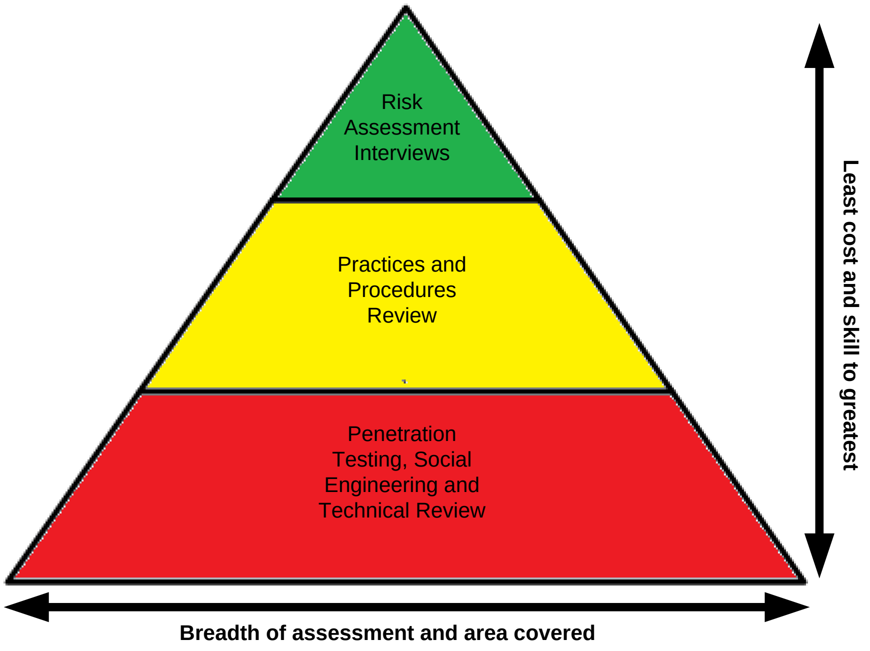
Good risk assessments tend to include at least three distinct assessment components of varying complexity, followed by a good reporting system with internal and external checks and balances. They include:

1. **Stakeholder Risk Assessment Interviews-** These are interviews with key stakeholders from across the organization, sometimes called risk assessment interviews.
2. **IT Security Practices and Procedures Gap Analysis-** This consists of a review or gap analysis of the practices and procedures in place within the organization, with an emphasis on identifying system dependencies and vulnerabilities.
3. **Penetration Testing or Vulnerability Assessments-** This is detailed technical testing to determine the organization’s actual vulnerability to threats such as hacking, loss of PHI or other incidents through penetration testing.

4. **Detailed and Actionable Reporting-** This is a reporting process that includes multiple stages of internal and external peer review, and creates a report with prioritized recommendations that can be tracked and acted on over time.

These components vary in terms of the required level of effort and technical skill needed to perform them. To visualize this diversity, consider the following diagram:

Figure 1 – Breadth/depth of assessment versus cost/skill

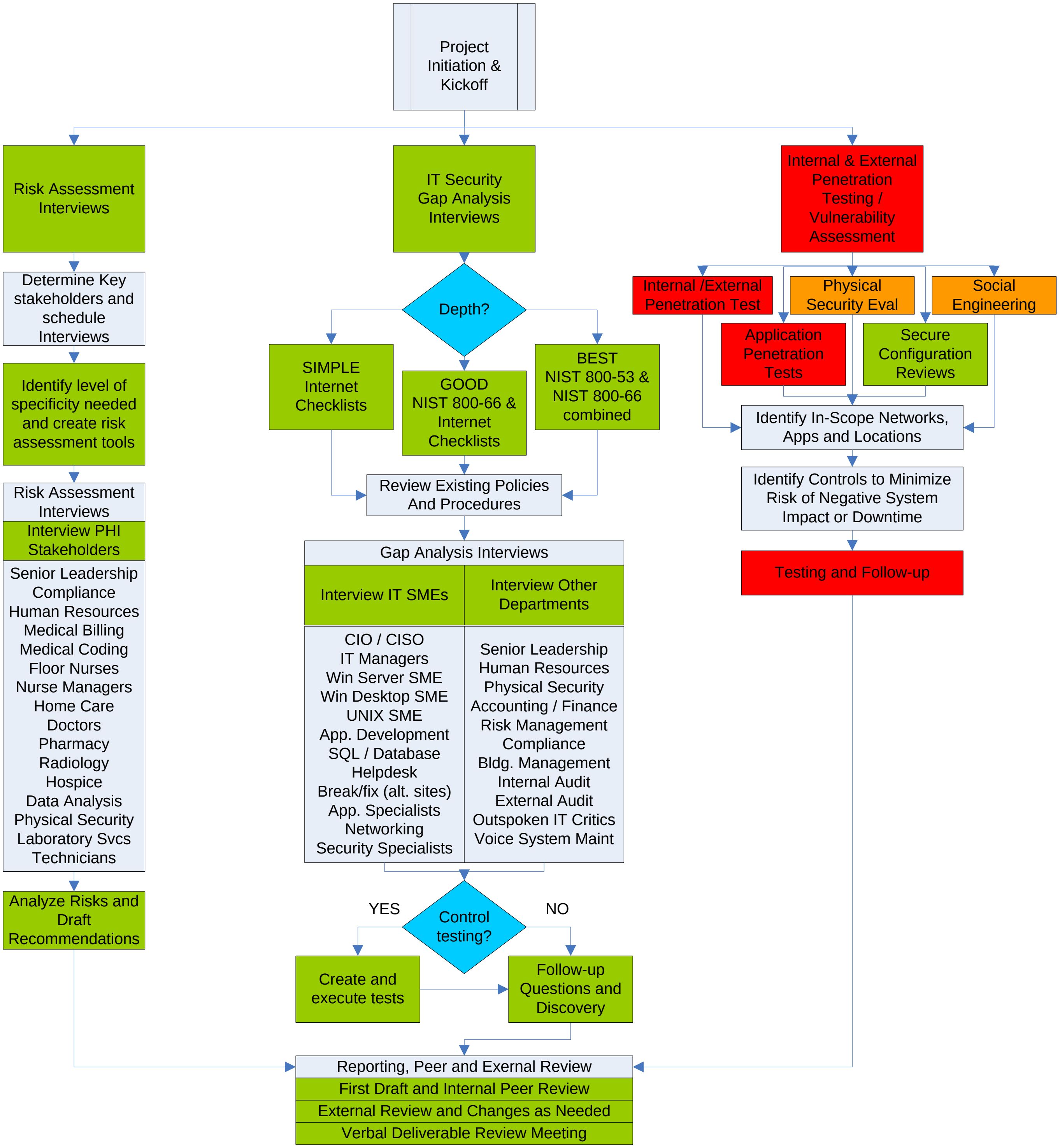

Risk Assessment Interviews
Practices and Procedures Review
Penetration Testing, Social Engineering and Technical Review
Least cost and skill to greatest
Breadth of assessment and area covered

At the top of this pyramid, we have risk assessment interviews. These can be performed by virtually anyone with good organizational, social and research skills. This first layer is constrained in scope, and tends to focus just on HIPAA compliance requirements without deeply examining the underlying organizational systems that support them. In the second layer of the pyramid, the analyst will perform a review of the organization's practices and procedures. This can be done superficially with a checklist or external standard, or in great depth by probing deeply into specific practices and procedures, as well as by identifying dependencies and unique issues that are specific to the organization. This review can help give assurance that the organization is sufficiently well managed to consistently meet regulatory needs. At the bottom layer of the pyramid are tasks such as penetration testing, social engineering and technical reviews of security systems that can only be performed by those experienced in specific tools and technologies. While this raises the bar for the level of skill and cost to perform the assessment, it demonstrates the actual security of the organization's security controls as a whole. Penetration testing is particularly helpful because it can identify the organization's greatest security and compliance problems by demonstrating that they can indeed be exploited, giving proof of this exploitation and describing how to prevent such exploitation in the future.

The Risk Assessment Methodology Flowchart

To better understand how the three components of the methodology shown in the above pyramid might fit into a unified project with other aspects such as planning and reporting, I have prepared the following flowchart. First, we will present the flowchart as a whole, and address specific sections in more detail in future sections. The purpose of presenting this diagram here is to show how the various pieces of an assessment might fit together, and it is not necessary to understand it in detail at this time.

Figure 2 - HIPAA Risk Assessment Flowchart


Project Initiation & Kickoff
Risk Assessment Interviews
IT Security Gap Analysis Interviews
Internal & External Penetration Testing / Vulnerability Assessment
Determine Key stakeholders and schedule Interviews
Identify level of specificity needed and create risk assessment tools
Risk Assessment Interviews
Interview PHI Stakeholders
Senior Leadership
Compliance
Human Resources
Medical Billing
Medical Coding
Floor Nurses
Nurse Managers
Home Care
Doctors
Pharmacy
Radiology
Hospice
Data Analysis
Physical Security
Laboratory Svcs
Technicians
Analyze Risks and Draft Recommendations
Depth?
SIMPLE Internet Checklists
GOOD NIST 800-66 & Internet Checklists
BEST NIST 800-53 & NIST 800-66 combined
Review Existing Policies And Procedures
Gap Analysis Interviews
Interview IT SMEs
Interview Other Departments
CIO / CISO
IT Managers
Win Server SME
Win Desktop SME
UNIX SME
App. Development
SQL / Database
Helpdesk
Break/fix (alt. sites)
App. Specialists
Networking
Security Specialists
Senior Leadership
Human Resources
Physical Security
Accounting / Finance
Risk Management
Compliance
Bldg. Management
Internal Audit
External Audit
Outspoken IT Critics
Voice System Maint
Control testing?
YES
NO
Create and execute tests
Follow-up Questions and Discovery
Internal /External Penetration Test
Physical Security Eval
Social Engineering
Application Penetration Tests
Secure Configuration Reviews
Identify In-Scope Networks, Apps and Locations
Identify Controls to Minimize Risk of Negative System Impact or Downtime
Testing and Follow-up
Reporting, Peer and Exernal Review
First Draft and Internal Peer Review
External Review and Changes as Needed
Verbal Deliverable Review Meeting

Risk Color Coding

One additional piece of information that is represented in the flowchart view is color coding for the relative risk of the given tasks. I have attempted to identify those tasks which may represent the potential for the organization to experience unexpected negative events such as system or network failure, inconvenience through user password lockout or employee distress. I have attempted to color code based on the following standard:

COLOR CODE	EXPLANATION / CONSIDERATIONS
Light blue, white and blue	These are simply tasks or decisions with little inherent risk associated with them.
Green	Green tasks represent information sets or discussions. The discussion tasks have the same risk as any meeting on a sensitive topic. The risks are primarily ones of negative perception and interpersonal conflict. Individuals may feel uncomfortable answering questions, particularly regarding compliance or practices that they know to be substandard, or may feel "picked on" for being the subject of the assessment or audit.
Orange	Orange tasks are those that have a significant chance to alarm the organization's staff, but are unlikely to cause a technical disruption. For example, if analysts were observed physically compromising a secured area, a diligent employee might be concerned until they were informed that the test was approved. Similarly, if a number of targeted phishing e-mails or suspicious phone calls were to occur at the organization, this might also cause alarm until the reason was known.
Red	Tasks that are red carry a measurable risk of causing a system outage or problem. Usually, this risk is low, and can be made lower through careful communication between parties and the appropriate use of tools. Activities such as vulnerability scanning and penetration testing always carry these risks, especially when assessing outdated systems, or systems with resource constraints such as limited bandwidth or concurrent connections.

Risk Assessment Components

1. Stakeholder Risk Assessment Interviews

Risk Assessment Interviews

The first component is stakeholder risk assessment interviews. This is the most common type of risk assessment. The simplest method of performing this is to gather a group of key stakeholders and discuss and record the organization's perceived risks and vulnerabilities and associate subjective ratings to these measurements. Often, a list of compliance questions such as shredding of PHI and account creation procedures are used to ensure that the most critical requirements of HIPAA have been discussed. This is often what people mean when using the term "risk assessment," and it is also the portion of an IT risk assessment that addresses less technical issues such as the handling of printed PHI, privacy practices and policies, and physical security in addition to IT system security. These interviews must be conducted with the help of representatives from outside of IT. This part of the assessment can range from informal to highly detailed, and is more "paper oriented." For guidance on what a fairly formal and detailed risk assessment process might look like, I suggest starting with the previously mentioned NIST 800-30 document. While the NIST document is well thought out, it is also more complex than many organizations require. In my experience, most organizations benefit more from a less formal and qualitative risk assessment methodology. Some of the key questions to consider when deciding how to perform this interview-based part of the process are the following:

Determine Key stakeholders and schedule Interviews

- ○ Who should be involved? This will obviously depend upon your organization and industry, but there are a few things to keep in mind. First, it is important to step outside of one's normal comfort zone and get feedback from people that you wouldn't normally talk to. In almost every organization, I have found that getting representation from human resources, legal, facilities, compliance, physical security, finance and senior leadership to be invaluable. For information technology, include specialists in servers, workstations, networking, application development, database management, helpdesk, call centers and application specialists. In healthcare organizations, representation from departments such as in-patient and out-patient care, radiology, pharmacy, medical coding and billing, laboratory services, in-home caregivers, hospice, compliance and the emergency department helps to give a good perspective.

Identify level of specificity needed and create risk assessment tools

- How badly do you need to determine detailed metrics or measurements for your risk or return on investment? If you have thousands of systems to manage and a very limited budget, it may be worth the effort to perform a quantitative assessment and create a detailed weighting system that factors in system criticality, the likelihood of a threat being realized, the return on investment of controls and other factors. You will need a good tool or spreadsheet to do this, as well as awareness of the criticality or value of your systems. Unfortunately, to do this, you first need to know which systems are most critical and where your sensitive data is stored and processed, which is often not a trivial task. If you do wish to complete a truly detailed risk assessment, the first part of your process is to perform a business impact analysis (BIA) to figure out what is most important to the organization. Not surprisingly, a BIA is also almost always done as a first step in disaster recovery planning. As of July, 2014, the Information Systems Audit and Control Association (ISACA) has a free BIA form for this purpose. In addition, I have described how to perform a BIA in section 4.2.2 (Steps 1-3, starting at section 4.2.2) of an unrelated paper I have written on "Hostile Forensics." There is also a rough BIA spreadsheet that goes with this paper that you can download as a template at no cost. Conversely, when you are doing a more informal and intuitive assessment, this is typically called a qualitative assessment. Risk assessments are well documented in the NIST standards. Personally, I find that a simple metric ranking system of low/medium/high for your risk and likelihood metrics tends to provide enough information for most organizations, and has the added benefit of keeping costs and complexity *much* lower.

Interview PHI Stakeholders

- How can you best elicit honest and useful information? Conducting risk assessment discussions can be challenging, especially when in the context of security and compliance. Some people may naturally feel defensive and be concerned about not only being criticized, but also about losing their jobs if they disclose information about practices that are not compliant with policy or the law. One way to address this is to construct your interviews such that specific comments and concerns are not associated with specific individuals, and making interviewees aware of this from the start. Another technique is to interview individuals or groups of people of the same approximate peer level. I have found it extremely counter-productive to try to interview nurses in the same group as the CEO of the hospital or the compliance director. Almost inevitably, the perspective of how things operate is going to be perceived differently from the people "in the trenches" than by the people at the top of the organization chart. Another technique for eliciting good information is to further de-personalize your questions. Rather than ask questions such as "do you often e-mail PHI to the wrong address," phrase questions in organizational terms such as "do you think that PHI is accidentally sent to the wrong address often?" In this way, you can get an honest answer that doesn't incriminate the interviewee or their direct coworkers. At the end of every interview session, I also like to ask very open-ended questions such as "Where do you think the organization should put its most effort in compliance?" or "If you had a million dollars more budget and fifty more employees, how would you improve security?" to identify additional discussion points.

Example Risk Assessment Interview Matrix

As noted before, it is possible to capture the results of these risk assessments in a very granular way (NIST 800-30) or in a more informal and subjective way. I typically like to use a simple spreadsheet that tracks a limited number of information points such as the following:

- Threat. What is the threat or risk of a "bad thing" that we are concerned about?
- Control(s). What systems are currently in place that minimize the threat being realized? Are they effective? Are they based on policies and procedures or technical systems?
- Likelihood. How likely is the threat to be realized? Something that happens on a fairly frequent basis, such as accidentally leaving a chart on a counter where a visitor could see it, might be given a high rating. An incident that happens only infrequently,

perhaps a few times of year, might be a medium. An incident that has never occurred, or has occurred only rarely, might be given a low rating.

- Impact. If the "bad thing" were to occur, how bad would it be? How many individuals would it affect? An occurrence that only affects a single patient's records might be given a low rating, while a major incident, such as a lost backup tape containing data for hundreds or thousands of patients, would be rated as a high impact. Consider also the potential financial impact of fines from the federal government, as well as a loss of confidence in the organization by its clients.
- Notes. Capture additional information worth noting such as relevant departments or physical locations, and suggestions for improvements.

A simple interview-based risk assessment tracking spreadsheet might look like the following:

THREAT/RISK	CONTROL(S)	LIKELIHOOD	IMPACT	NOTES
Disclosure of PHI in e-mail to wrong recipient, or by not encrypting with [PHI] subject line tag	Training and optional encryption through IronPort mail appliance	Medium	Low	May include occasional error by forgetting to flag as PHI, accidental sharing of PHI with coders in plain text format
Overheard verbal discussion in common areas such as nursing stations, ED front desks or patient intake	Training and use of private interview areas when possible	Medium	Low	Signs are used to provide personal space for areas where people wait in lines. Private cubes are used for patient intake.
Loss of sensitive pictures of patients' affected areas on Cancer Center digital camera through theft or loss	Camera kept in area that is frequently monitored	Low	High	Potential for multiple patient disclosure, including pictures of sensitive areas. Staff was not aware of media disposal requirements. It's recommend this device be stored in locked cabinet when not in use.

Disclosure of PHI through lost or stolen proximity card being used to access electronic medical record (EMR) system	Procedure to report stolen or lost card, video surveillance, staff likely to notice patient or visitor using EMR computer	Low	High	Would have to have physical access to a machine in order for this to occur. Staff would quickly notice a missing card and report it, but if they failed to do so significant access could occur.
Postal mail of PHI to wrong mailing address	Ongoing efforts at improving data accuracy, especially in billing	High	Medium	Happens often due to data entry errors, including from outside agencies requesting procedures. It could happen with multiple records at a time due to automated systems.
PHI sent to wrong patient with similar name but different data of birth	Daily activity to check for known name conflicts	Medium	Low	Typically only applies to one-off discharge paperwork
Fax PHI to wrong number, but the number provided is an actual fax machine	Policy to validate fax number, routinely call to ask if the fax was received	Low	Low	A surprising number of documents are faxed to restaurants or to an employer fax instead of patient's private fax number.

Even with the limited information gathered using a tool such as the table above, it is fairly easy to identify areas that exhibit the most risk. These need to be addressed and added to the list of recommendations in the final report.

2. IT Security Practices and Procedures Gap Analysis

The second area of the risk assessment is that of performing an IT security practices and procedures gap analysis. In order to understand how an organization's systems and information is managed, and by extension how well it protects its PHI and complies with HIPAA regulations, it is necessary to understand the organization's day-to-day operations. Once again, there is a wide range of detail one can analyze in this stage of the assessment.

IT Security
Gap Analysis
Interviews

Perhaps the first choice is to identify a set of objective standards by which to measure the organization. Even the most experienced and expert assessor should come armed with some form of security framework or checklist. Although this should not be used simply as a list of questions to ask by rote, it is useful to refer to during the analysis to ensure that all key topics have been discussed. A well-recognized framework also has the added bonus of being able to align with standards recognized by other organizations and regulatory agencies, thereby making future assessment and planning work more efficient.

Security Guidelines and Checklists

Once again, there is an almost overwhelming amount of information that can be used as a standard for this part of the assessment. I generally consider there to be three major tiers of usefulness for external guidelines that can be used:

1. Simple: These consist of "free" HIPAA checklists and tools from the Internet. It is possible to find software or simple checklists of only 5 – 10 pages of length on the Internet. Although I do not recommend these as they frequently do not have enough detail to determine if practices and procedures are actually effective. A couple of these have been identified already in previous sections. However, if resources are limited, a simple checklist from a reputable source is better than nothing.

SIMPLE
Internet
Checklists

2. Good: This information is found in detailed HIPAA-focused guidelines. At a bare minimum, I recommend using a well-constructed framework such as the NIST 800-66 document entitled "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) security rule." This document is clear and well written, and has specific guidance on HIPAA requirements. It also maps HIPAA requirements to more detailed standards such as NIST 800-53, as discussed below, if you wish to go deeper in your analysis. The disadvantage to using a moderately-detailed document, such as 800-66, is that while it identifies specific HIPAA requirements and relates it to other controls, it does not fully address the security of the underlying systems supporting regulated systems, and the environment in which they

GOOD
NIST 800-66 &
Internet
Checklists

BEST
NIST 800-53 &
NIST 800-66
combined

operate. As such, there could be factors that materially affect security in practice that are not discussed in these guidelines.

3. Best: This is detailed information along with security frameworks combined. The best-case scenario is to assess the organization based on a specific and detailed set of technical and procedural criteria. In my experience, there are very few frameworks that do this well. And without a doubt, the best technical frameworks are the NIST 800-53 documents entitled "Security and Privacy Controls for Federal Information Systems and Organizations" (and their more subject-specific peer documents from NIST). While I regularly use version 3 of this document, version 4 has been available for about a year and many organizations are working to adopt it. This standard is excellent in that it is especially detailed, and largely devoid of superfluous information. The level of detail is such that if one wanted to develop an incident response procedure, they could refer to this document and come up with a good list of minimum standards and key components. Fortunately, NIST 800-53 and NIST 800-66 have already been mapped against each other, so that an organization could assess themselves against 800-53 and then relate it to HIPAA objectives later. For organizations that struggle with understanding how to best manage information security, and with a less technical emphasis, I would point you to the Information Technology Infrastructure Library (ITIL) standards, and the COBIT framework from ISACA. Although I rarely use these latter two resources in my engagements, as they work better to address management's "tone at the top" and the way that management activities are conducted rather than identifying technical security standards, they can be valuable tools, especially for larger organizations or those subject to regulations such as the financially-focused Sarbanes–Oxley Act.

Reviewing Organizational Material and Performing Interviews

Regardless of what framework you use for analyzing practices and procedures, and thereby identifying gaps and potential improvements, there are some aspects of the process that are universal.

Review Existing Policies and Procedures

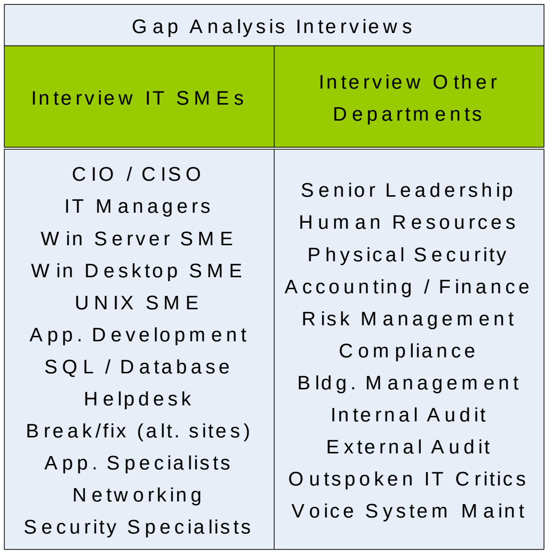
Review Existing Policies
And Procedures

First, I suggest that you start the interview process by gathering all of the relevant policies and procedures that you can identify and reading these ahead of time, including HIPAA privacy policies. Even the results of requesting the policies can be interesting. I have been in organizations where the IT director was under the impression that all of the organization's units followed his policies, only to discover that some units had their own completely different sets of policies. When reading the policies be on the lookout for issues such as:

- Conflicting policies. Are there policies that contradict each other? One common conflict is in the use of the Internet for personal purposes. Some organizations have one policy that says all systems are for business purposes only and another policy that says limited browsing is acceptable as long as it does not impact job performance.
- Outdated policies. Are there policies that refer to systems or technologies that no longer exist? A good policy will not be so specific as to mention particular systems or software. If you see a reference to an AS/400 or to "Napster," make a note of it.
- Obvious templates. Many organizations save time by adopting security policies based on templates that they have taken from Internet resources such as the free SANS.org template collection or commercial packages such as Information Security Policies Made Easy. There is absolutely no shame in using premade policies as a starting point, as long as they are customized to the local environment and people are trained to follow them. However, a surprisingly large number of organizations will simply take a bunch of policies and copy them up to their own internal repositories with minimal editing and call it done. An experienced assessor can immediately spot these, and is likely to think that someone did this simply to try to deceive an auditor at some point.
- Keep the policies in mind when interviewing. When interviewing internal stakeholders on practices and procedures, it is valuable to keep a few things in mind. First, do the people you talk to actually know the contents, or existence, of the policy if they should? Are employees trained on the policies? Second, are the policies actually followed and enforced? Many organizations still persist in having a policy that states that Internet browsing is not allowed at work, and very few of these organizations actually follow the policy. Often it is senior leadership that sets a bad example by, for example, demanding exceptions to the content filter for golf.com. Unless all employees know the policy, follow it and there are consequences for not doing so, the policy is worthless. Worse, having a policy that has been approved but not followed could set a bad legal precedent.

Gap Analysis Interviews

At this point, it is time to interview the key stakeholders inside and outside of IT. First, you need to have an adequate understanding of the subject matter to ask the probing questions that identify security gaps. In particular, it is essential to understand system dependencies at a deep technical level. This task is particularly difficult for assessors that do not have a strong background in IT. Indeed, in my experience, it is easier to turn a good engineer into a good auditor than the other way around, and auditors that lack these critical skills are often criticized as being "checklist auditors." Take, for example, an electronic medical records system that contains PHI. It is fairly easy to ask HIPAA-relevant questions such as ”Does the system have access logging?” or ”Is there a formal system for provisioning and removing user access?” What is more difficult is identifying the underlying technologies that make the system work and spot possible flaws in them. So while an individual following a simple checklist may ask the above questions, an experienced technical analyst, armed with NIST 800-53, may ask more probing technical questions such as:



Gap Analysis Interviews	
Interview IT SMEs	Interview Other Departments
CIO / CISO IT Managers Win Server SME Win Desktop SME UNIX SME App. Development SQL / Database Helpdesk Break/fix (alt. sites) App. Specialists Networking Security Specialists	Senior Leadership Human Resources Physical Security Accounting / Finance Risk Management Compliance Bldg. Management Internal Audit External Audit Outspoken IT Critics Voice System Maint

- <u>Exactly how does authentication work</u>? Is it stored in a local database, or integrated with another directory such as Microsoft Active Directory? How are rights to screens or records provisioned — locally in the application or by directory group membership? Does the system use Lightweight Directory Access Protocol (LDAP) for authentication, and if so, are LDAP connections encrypted? Are credentials stored in an unencrypted format in configuration files or executables? If an external authentication system is used, how secure is it? If it were possible to compromise Active Directory, could it lead to a disclosure of PHI?

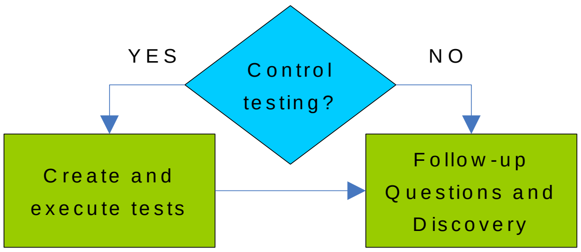
- Where is data actually stored? Exactly which back-end databases store the application data, and how are they secured? Is a single SQL database account and password used for all database access, or is database access provisioned more granularly? How can direct access to underlying data be obtained without using normal application security? For example, could a domain administrator connect to the database server and enumerate PHI? Could a default password, or a password discovered on a less secure SQL server be used to access PHI on the back-end database?
- What are the application's interfaces? Does the application export data to a data warehouse or reporting application, and if so, are these applications secured? Is data imported and exported to other systems by scripted file transfers, and if so, are these file transfer systems secure and monitored? If data is transferred to federal or state information exchanges for purposes such as identifying epidemics or at-risk communities, are these connections secure? If data is transferred to partners and vendors, such as after-hours radiology support or prescription drug insurance exchanges, are these activities secure?
- How is the system built, updated and maintained? Was the server originally configured according to a set of security standards or hardening guides? Is its configuration documented? Are patches applied on a timely basis, not only for the core operating system but for all application components such as database servers and middleware? Are vulnerability assessments run on a regular basis to double-check that everything is functioning as expected?
- Is the underlying network layer secure? Are networking systems such as switches, routers, virtual networks, etc. adequately secured? Could a compromise of a network switch allow for a compromise of any of the security systems that the application depends upon? Could an attacker with access to network equipment obtain credentials that could be used to access PHI within the application?
- If there were a breach of PHI, could you adequately investigate it? Is there an incident response plan that takes the specific details of the system into account? Are there adequate systems to detect if there is a breach of data in the application? If a breach were reported to you, would you be able to perform the investigation within 30 days of discovery? Does the system retain logs not only of changes to PHI but also views? Are there shared user IDs that could make attribution of PHI access to a

specific individual impossible? Are logging systems in place to retain logs for an extended period of time, such that a breach could be investigated if it were reported six months after the fact?

This is just a small subset of the type of questioning that normally takes place during gap analysis discussions, but they should demonstrate the level of detail that should be gone into as part of good practices and procedures gap analysis.

Control Testing or Follow-up Questions

Once you have learned how your subjects believe things work, you must decide whether or not to determine first hand whether what they are telling you is correct. Is it enough to simply ask probing questions of the right people? If so, it is essential not only that the people you work with actually understand how these systems work, but that they are also being honest with you. This often means having an executive sponsor either sit in on the process or give a mandate up-front to be honest and direct in their responses. In a more formal audit, the assessor will actually perform substantive testing to validate that things are in fact working as presented. This may mean creating and executing tests such as sitting down at systems to review configurations, perform reviews of work history documentation to verify that tasks are being performed, look through change management logs or any number of other tests. Doing substantive testing can be extremely time consuming, and therefore it greatly increases the amount of effort required for the assessment.



3. Penetration Testing or Vulnerability Assessments

The third aspect of the risk assessment process is penetration testing. Up to this point, we have been discussing ways to elicit information about compliance status and information security through review — mainly through dialogue, but also through review of documentation and possibly hands-on checking of systems. This approach is an excellent way to get a

Internal & External Penetration Testing / Vulnerability Assessment lot of information in a fairly short period of time, but it does not necessarily reflect the *actual* security of the organization and how resistant it is to a targeted attack. To truly understand the security of the environment and how vulnerable the organization is, it is necessary to perform penetration testing. Penetration testing involves engineers skilled in “hacking” techniques attempting to breach the security of the environment in order to obtain administrator access, PHI or other critical information. Penetration testing should be performed externally (on Internet-accessible systems) and internally (from the inside network) as well as on wireless systems.

Penetration testing is similar, but not identical to performing vulnerability assessments. As the difference between these two concepts is sometimes difficult to understand, let’s attempt to differentiate these two approaches:

Vulnerability Assessments

Vulnerability assessments attempt to identify as many vulnerabilities as possible in IT systems, and rank and prioritize these vulnerabilities. Typically, this is usually done using security scanning tools such as Tenable’s Nessus scanner. One advantage to this approach is that it is not very difficult or time consuming to perform. Indeed, the level of skill necessary to run a simple security scan can be rather minimal, and many organizations do their own regular scanning internally. Tools such as Nessus also have a variety of features such as credentialed client-side scans that are especially useful for compliance such as discovering locally stored PHI. Regardless of what tool you use, I strongly recommend investing in a product that can perform these features. The end result of a vulnerability assessment tends to be a report with a long list of technical problems that should be fixed, some prioritization of which fixes are most important, and references or guidance on ways to fix the problems. One disadvantage of the approach is that there tend to be a large number of findings, which although prioritized by a tool, may not truly represent an accurate reflection of which items are truly the most important to fix, and sometimes leading to information overload. To visualize this with a metaphor, consider a burglar that goes around your house checking all the doors and windows to see if they are locked, but not actually entering them, then going home to write down what he saw.

Penetration Testing

Penetration testing builds on the results of a vulnerability assessment by attempting to actually exploit the weaknesses discovered. Penetration testing also uses a great deal more human intelligence to make logical and intuitive leaps and attacks that a tool is unable to make. Thus, rather than simply identifying vulnerabilities, a penetration tester exploits these vulnerabilities to prove that they can indeed lead to significant access. A penetration test, particularly when conducted from the inside network by a skilled analyst, usually results in a near-complete compromise of the IT infrastructure and thus the systems that it supports. This often results in a decrypted list of system passwords, copy of the CEO's email, proof of access to PHI and any number of other examples of successful exploitation in the final report.

In my experience, our penetration testing team is successful in getting significant administrator access in about 95 percent of all internal tests conducted. Instances where a skilled penetration tester is unable to succeed, particularly from the inside network, are rare. The advantages this approach provides are proof that the vulnerabilities are more than theoretical, and to show how a dedicated attacker could compromise the network. In particular, this shows how a sequence of different attacks could be leveraged to obtain access across multiple systems and platforms. For example, a penetration tester might be able to identify a single un-patched server, compromise this server and use information on that server (such as discovered passwords) to compromise additional systems, eventually leading to a complete compromise. When properly reported, this can lead to a far more useful set of prioritizations for remediation than those provided by a vulnerability assessment. It is difficult to perform penetration testing without extensive experience, but some guidance such as the Penetration Testing Execution Standard (PETS) guidelines may be of value for new learners and experienced assessors alike.

Disadvantages of penetration testing are that it is more time consuming and expensive, and it requires a significant amount of technical knowledge. To return to the analogy of the burglar and the house, rather than check every door and window and go home to write a report, a penetration tester will climb through the first open window, rifle through your personal files, make copies of your keys so they can come back later and possibly even sneak into your bedroom and take pictures of you drooling while you sleep. Time permitting, they may also try a different window, shave your dog and post the video to YouTube. While immensely valuable for proving to upper management that vulnerabilities are more than theoretical and that more emphasis on security is needed, it can also be a very uncomfortable experience for those responsible for maintaining the systems that have been compromised.

Choosing Penetration Testing Versus Vulnerability Assessments

Despite being somewhat more resource intensive, penetration tests are preferable to vulnerability assessments in almost all cases, in that they provide guidance on those attacks that are most likely to be successfully perpetrated by an actual attacker. This adds a layer of prioritization to that which might be provided by a vulnerability assessment, because it shows which vulnerabilities are actually exploited in the wild, and can put an emphasis on an integrative and interconnected view of security, rather than a large list of individual issues to fix. That said, for organizations with a very small budget and a very small number of systems to manage, a vulnerability assessment may be the best choice.

Social Engineering and Physical Security

In some cases, approaches such as social engineering are used to test the security awareness of employees in the organization. This might include sending phishing e-mails, impersonating employees and calling the help desk to obtain password resets or other mischief. In other instances, these social engineering techniques could be combined with creative abuse of flaws in physical security to access restricted areas. This type of physical penetration testing can be used to show whether (and how easily) it is possible to bypass physical security controls to access areas that they should not be able to access. In past projects, we have discovered vulnerabilities such as door locks that could be easily opened using a credit card, or been able to simply follow employees into secured areas as they enter (a technique known as "piggy-backing").

Social Engineering

Physical Security Eval

Application Penetration Tests

Application Penetration Tests

In some cases, specific applications should be subject to additional scrutiny. Although a penetration test will likely find multiple ways to compromise internal systems, it is impossible to find all of them. For this reason, extra emphasis should be placed on applications that hold particularly sensitive data, and especially those that were not developed by well-known and reputable development companies. Applications that are Internet-accessible and were developed internally or by small software development shops are especially important to assess. A particular problem is that many web applications have security vulnerabilities such as SQL injection or ways to bypass authentication that could allow an attacker to access PHI or compromise the system. For more information on application penetration testing, the best available information is at the Open Web Application Security Project (OWASP) web site, and a number of free and commercial tools are available.

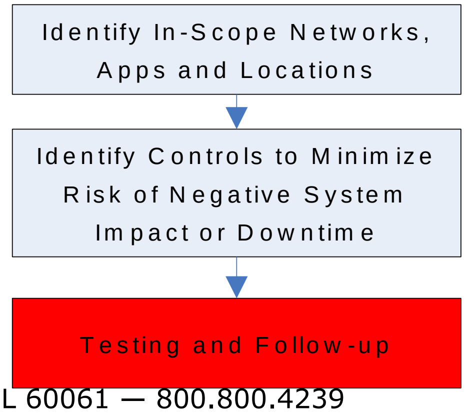
Secure Configuration Reviews

Secure Configuration Reviews

In some cases, the ideal way to verify the security of a system is to review the way in which it is configured. This is particularly the case for devices that are difficult to test on the network. For example, firewalls and intrusion prevention systems often operate in a way that is opaque to assessors that do not already have access to the system. While an assessor may be able to test a particular theory such as ”Can I use my home system to bypass security?” it is time consuming and difficult to devise and perform an adequate number of these tests to validate the security of the device. In another example, there may be systems that can only be accessed using a particular protocol, or with a limited number of accounts and passwords, such as UNIX systems or client workstations that cannot be remotely accessed. If the penetration tester is not successful in getting access to these systems, they will be unlikely to find vulnerabilities that an insider with access could discover and use. To address this risk, the preferred method is to provide the assessor with valid credentials to the system and perform a review of the system’s configuration manually. In the case of a firewall or router, this may mean providing a copy of the running configuration. In the case of the workstation, this may require providing physical access and an account to a workstation.

Establishing Scope and Minimizing Risk

In all cases, whether simple vulnerability testing or thorough penetration testing, it is important to minimize the risk of unfortunate and unforeseen events during testing. Testing can and does cause outages. To avoid this risk, establish up front


Identify In-Scope Networks, Apps and Locations
Identify Controls to Minimize Risk of Negative System Impact or Downtime
Testing and Follow-up

what systems are in scope for testing and how communication will take place during the assessment to minimize system outages. In particular, identify systems that simply should not be tested. Printers, telephones and very old systems are good candidates for exclusion from the scan. In the case of Internet penetration tests, be especially careful to only scan the correct IP address ranges, and not those of your network neighbors. Shared IP address ranges such as in hosting facilities are a particular problem. A similar mistake (on the part of the assessors) is to scan their own workstations as part of the assessment. It is particularly embarrassing if your penetration testing workstation shows up in a report as having vulnerabilities. When performing automated scanning, monitor the scans as they occur and monitor network performance and discussions around the office to determine if you are causing problems.

4.Detailed and Actionable Reporting

Reporting, Peer and Exernal Review
First Draft and Internal Peer Review
External Review and Changes as Needed
Verbal Deliverable Review Meeting

The fourth and final aspect of the risk assessment is effectively communicating the findings and recommendations of the assessment. With all of the information created by the three main components of the IT HIPAA risk assessment (risk assessment interviews, practices and procedures gap analysis and penetration testing), there can be an overwhelming amount of information to assimilate. In order to make this information useful, there obviously needs to be guidance on how the organization can avoid "information overload" and move forward in making improvements. All too often, large reports of this type are so overwhelming that the organization simply doesn't know where to start. Among the things that a good process will do to minimize this risk are:

- <u>Tailor the report(s) to the audience</u>. The report contents of a gap analysis are significantly different from the results of a penetration test, and are often read by very different audiences. In the former case, the audience tends to be somewhat less technical. For this reason, having two different reports — one for technical details such as the penetration test and one for the interviews and gap analysis often makes sense. Similarly, within those documents there should be varying levels of detail, including a less technical executive summary and list of key findings, followed by detailed technical information.

- Use a vendor-agnostic approach. It is not the job of a risk assessor (whether internal or external) to promote a personal agenda, additional services or products. In particular, those of its own company or its favored partners. This is not only unethical, but it reduces the credibility of the assessors and ultimately the work that they have performed. In the event that you may have a potential conflict of interest (such as reviewing the work done by other departments of your own organization) it is important to present the facts and concerns as objectively as possible, and not minimize any problems found. In terms of making suggestions for new products or services, the focus should be on the functional requirements of the systems that are needed, and you should suggest that the organization perform its own research into which options best fit their needs. It is perfectly acceptable to mention products by name when explaining desirable features or detailing solutions that can meet specific needs so that they can be better researched and compared to alternatives.
- Give specific guidance on issues and remediation. A risk assessor should never identify a problem for which he cannot suggest a solution, and preferably multiple solutions. For any problem identified, there should be at least one way identified to mitigate the risk. In some cases, solutions may be as simple as implementing a policy or procedure that employees are trained on and held accountable to such as using strong passwords. In other cases, there may be a very limited number of solutions, such as making very specific changes to technical systems such as disabling insecure password protocols or separating systems of varying criticality onto different networks. Specific references to whitepapers and external guidance on how to perform the steps necessary to fix the issues should be given. Findings should be mapped to external standards such as those developed by NIST and the federal government to provide an external and objective justification for why the recommendations are made, and how one might address them.
- Use an internal and external peer review system. Risk assessments tend to create large reports. It is not unusual to have information-packed reports running into hundreds of pages. For this reason, it is easy to make mistakes both technical and grammatical. To minimize this risk, it is essential that documents undergo multiple stages of review. First, an internal review should be conducted to ensure that the contributions from multiple authors are combined in a cohesive and understandable

way. Ideally, a technical editor will be used to correct grammatical and formatting errors and suggest better language. Most importantly, the *recipient* of the reports will be provided with an opportunity to review the documents in draft form to ensure that there have not been any factual misunderstandings and that the information presented is clear and politically appropriate for the organization. It is perfectly reasonable for the organization being assessed to make requests for changes in languages and tone, as long as it does not make a substantive change in findings. Where trouble can arise is when the assessed organization desires to have entire findings removed for some reason or another, and this can lead to tense and awkward discussions. Unfortunately, many organizations do not take the time to review their draft reports and make such suggestions. This is unfortunate, as taking the time to do so can make the entire process much more valuable.

- Present the results in person or verbally. Simply providing a large and detailed report is not enough. You must take the time to walk through the document with the organization in whatever level of detail they deem appropriate. This can often be grueling and take hours to do, but it is the only sure way to ensure that what has been discovered and recommended was understood well enough to be acted on. If necessary, break the process into discrete chunks of time. For example, a shorter meeting for management, followed by a longer or more detailed meeting with technical staff. Alternately, schedule one meeting for the technical results and one for the interview and gap analysis results. Once an initial report review has been conducted, provide ongoing opportunities for questions so that issues can be discussed that may not have been thought of beforehand.

Choosing Your Approach

In the previous sections of this document, a number of different options and approaches to performing an assessment have been presented. The best assessment will be tailored to your organization’s budget, available skill-set and tolerance for risk. Although it is impossible to identify the correct approach for an unknown and theoretical organization, a few trends or service packages do seem to recur frequently:

Category	Steps to Perform	Notes
Minimal Compliance	○ Perform risk assessment interviews ○ Review simple checklists of compliance	For organizations with little or no technical staff or budget, in my opinion, this is the minimum that can be done and still meet the intent of HIPAA compliance regulations.
Moderate Assessment	○ Perform risk assessment interviews ○ Perform and interview-based gap analysis as per NIST 800-66 ○ Perform vulnerability scanning of Internet and internal network	For organizations with technical individuals, although perhaps not security specialists, this is a reasonable option. You will identify insecure systems and evaluate your environment with a deeper understanding of the intent of the HIPAA regulations.
Deep Assessment	○ Perform risk assessment interviews ○ Perform an interview-based gap analysis as per NIST 800-53 and 800-66, and map the results ○ Perform penetration testing of Internet, internal and wireless networks ○ Perform application testing of sensitive applications not from major software vendors, especially Internet-accessible systems ○ Perform secure configuration reviews on systems of unknown security ○ Perform social engineering via phone, e-mail ○ Evaluate physical security	This is the approach that I recommend to the majority of my clients. It covers a wide range of topics, uncovers many issues for remediation, and tests the actual resilience of the environment to attack. Costs are kept lower by using an interview-based process rather than doing extensive testing of controls to determine if they are being followed as represented. The security awareness of staff will be tested through phone calls and phishing e-mails, and physical security systems will be evaluated. Devices that have not been explicitly evaluated for security such as firewalls will be assessed manually for possible improvements.

Enterprise Class	○ Perform a Business Impact Analysis to identify critical systems ○ Perform risk assessment interviews ○ Perform an interview-based gap analysis as per NIST 800-53 and 800-66, and map the results ○ Develop and perform tests to validate that controls, policies and procedures are being followed ○ Perform penetration testing of Internet, internal and wireless networks ○ Perform application testing of sensitive applications not from major software vendors, especially Internet-accessible systems ○ Perform configuration reviews of all critical infrastructure ○ Perform social engineering via phone, e-mail ○ Evaluate physical security	This category of testing is largely reserved for organizations that must meet a very high level of compliance, such as federal contractors or large companies. Testing is practically an ongoing process, as there will be many things to assess, and these will change and need to be re-tested regularly. Gap analysis assessments will perform detailed testing to determine if practices and procedures are being followed on a consistent basis. At this level, full-time assessors will likely be needed, and costs will be high. However, if this level of diligence is consistently applied to the environment and a program for acting on findings is in place, the effective security of the organization is likely to be above average.

Summary

This document outlines some of the tasks, tools and issues to consider when performing efficient IT HIPAA risk assessments. It also identified some of the combinations of options that an organization might use to meet its compliance objectives while keeping costs and effort at a reasonable level. Hopefully, this overview is of benefit and can be used by organizations either on their own or in collaboration with a consultant or partner. I hope that this document will be of value to you, and I welcome your comments and questions.

About the Author

Mark Lachniet is a Solution Architect at CDW in the Security Assessment group. He has worked in IT security consulting for over 14 years. In addition to working as a consultant, he has worked as a K-12 school district technology director and as an instructor for a masters-level information assurance degree program. Mark is a licensed private investigator in the state of Michigan, and holds a number of certifications including the Certified Information Systems Auditor (CISA) and Certified Information Systems Security Professional (CISSP). Mark is a frequent presenter at information security conferences and has served on the boards of various professional organizations, including as president of the Michigan chapter of the High Tech Crime Investigation Association (HTCIA). Mark can be reached at mark.lachniet@cdw.com for questions for comments.

Assistance with this document was provided by Roth Chapin, David Russell, Brian Self and Mike Kosinski of CDW Corporation, although all errors are my own.