Global Information Assurance Certification Paper

Audits Made Simple

GIAC (GCCC) Gold Certification

Author: David W. Belangia, dwbelangia@hotmail.com
Advisor: Stephen Northcutt

Accepted: March 6, 2015

Abstract

A company just got notified there is a big external audit coming in 3 months. Getting ready for an audit can be challenging, scary, and full of surprises. This Gold Paper describes a typical audit from notification of the intent to audit through disposition of the final report including Best Practices, Opportunities for Improvement (OFI), and issues that must be fixed. Good preparation can improve the chances of success. Ensuring the auditors understand the environment and requirements is paramount to success. It helps the auditors understand that the enterprise really does think that security is important. Understanding and following a structured process ensures a smooth audit process. Ensuring follow-up on OFIs and issues in a structured fashion will also make the next audit easier. It is important to keep in mind that the auditors will use the previous report as a starting point. Now the only worry is the actual audit and subsequent report and how well the company has done.

dwbelangia@hotmail.com

1. Introduction

"Virtualization, mobilization, and cloud technology have created new points of entry into business, leaving them vulnerable to covert cyber-attacks," states a report by Ernst & Young. (Cyber security: considerations for the audit committee, 2013) Executives are struggling with the potential for a data breach, and resolving this business risk is high on their agenda. While most audit committee members are financially solid, they lack knowledge of technology issues, making understanding of this risk difficult.

"Management must adequately evaluate the costs and benefits of their IT budget to ensure that they are not handcuffing those tasked with the onus of implementing cybersecurity measures. They must ensure that proper controls and procedures are in place to protect, detect, and respond to cyber incidents." (Coleman, 2014)

Independent validation of cyber security posture is an important aspect to ensure security of the business. "The very survival of the organization depends on the ability of the board and management not only to cope with future events but to anticipate the impact those events will have on both the company and the industry as a whole," Tom Horton. (Rai, 2014)

"Audit is a public interest activity. Audit reports build confidence in financial statements and give credibility to companies and comfort to stakeholders. Company also benefit from the insight that auditors have into business processes and the wider market environment." (Audit Insights, 2015)

The process for managing the audit process using industry best practices and practical experience is important to the institution. Understanding the process and working the audit process, as a formal project, will help ensure the audit is conducted smoothly, allowing executives to obtain high value and understand the risk being accepted. SANS, through the AUD 507 discussions, provides a six-step process; planning, entrance conference, fieldwork, preparing the report, exit conference, and the report to management. (Hoelzer, 2014)

dwbelangia@hotmail.com

This project requires a structured approach with subsequent activities dependent on the previous activities. These activities are discussed in-depth to facilitate an organized approach, using both the sections within the paper and the attached project schedule. The activities are sequenced and have dependencies, so it is recommended the reader follow the order of the paper and the project schedule to ensure information from one section can be used in next section. Figure 1 – Audit Management Timeline (page 5) provides a graphical representation of the project schedule (Appendix A – Audit Management Schedule) with estimated durations for activities. This graphical representation provides information on the project flow of activities to be executed. The project flow is as follows (hyperlinks to sections within this paper):

Notification
Assemble Project Team
Education and Training
Technical Assessment Protocol
Trusted Agents
Data Call
Monitors
Agenda Development
Conference Rooms
Clearances
Read Ahead
Final Preparation
Entrance Conference
Field Work
Preparing the Report
Exit Conference
Report to Management

After the final audit report has been provided, the institution must start the process of addressing issues and opportunities to improvement. These activities include:

Findings and Opportunities for Improvement
Categorizing/Tracking
Resolution/Sustainability

Developing a solid approach to the audit using traditional project management tools can ensure the maximization of the audit value. All activities relating to the audit should be discussed, evaluated, scoped, and managed to maximize the value proposition. Appendix A – Audit Management Schedule provides a template project schedule to

dwbelangia@hotmail.com

support the audit process. Success with an audit helps management understand the risk management is accepting, highlight gaps in security, and generate ideas on how to improve. These results are an important aspect of managing the business risk.

dwbelangia@hotmail.com

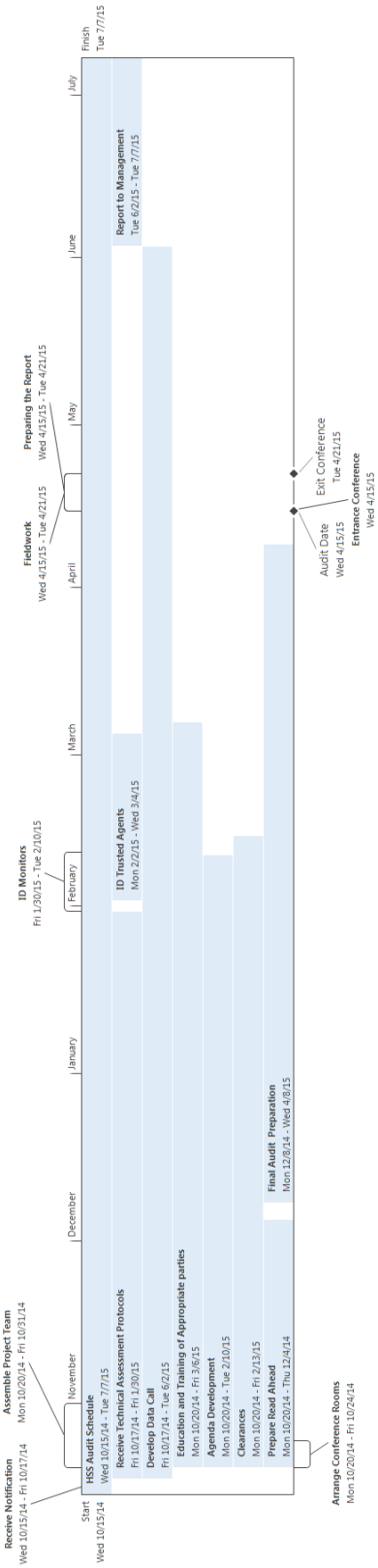


Figure 1 – Audit Management Timeline

dwbelangia@hotmail.com

2. Audit Planning

2.1.1. Notification

Initial notification of the planned audit should be formal via a letter or an Announcement Memorandum between the organization to be audited and the auditors. Depending on the complexity and scope of the audit, this announcement could be received six months prior to the audit. If received too late the audit management preparation processes will not be thorough and at risk of effective execution.

The notification must be routed through the appropriate channels. Most organizations have an internal audit organization that should be engaged early. Many organizations have contractual requirements necessitating the audit. The audit might be driven by national requirements or a request from the customer. Regardless of the audit source, engaging the proper people early will avoid confusion later.

This notification might contain several additional documents such as the cyber security technical assessment protocols for the intended targets (business systems, particular asset, or whole environment), a memorandum of understanding to document intent and processes to be followed, and an agreement regarding trusted agent responsibilities to de-conflict the engagement activities.

If the notification document was not routed through the client, then the CIO/CISO should notify the client of receipt of the notification and provide a copy to the client. The CIO/CISO should be consulting with the execution arm of Information Technology to ensure minimization of operational impacts and provide early notification of the audit.

2.1.2. Assemble Project Team

A Project Manager must be identified early to ensure success of the audit. Based on the complexity of the audit, the Project Manager might be required to execute the scope full time. Assigning the proper Project Manager and other resources might require reassignment of existing work to other members in the line organization. This effort should be underestimated.

dwbelangia@hotmail.com

Decisions must be made on additional roles (Logistic Lead, someone to manage the agendas, communications lead, team members, stakeholders, and training coordinator). The Project Manager must assemble the team and create/revise the project schedule.

2.1.3. Education and Training

Based on the scope of the engagement, there will be certain training requirements for the auditors and the audited organization. The training for the auditors will include particulars with regards to the site being audited (facility evacuations, special hazards, site unique cyber requirements [personal cell phone/computer use, wireless, Bluetooth]).

Understanding training requirements will enable the smooth execution of work and reduce surprises. Training that can be conducted for the auditors, before they arrive, is beneficial to the organization. It is important to keep in mind that the auditors help identify risk for management, and having them perform training once on site minimizes their productive time.

Additional training should be developed and delivered based on scope to the organization's personnel who will be interviewed by the auditors. The subject matter experts should and will be ask questions about operations and controls. These are easy, but people want to please auditors and will offer opinions or even try and answers questions they are not sure about or not within their scope. It is important to answer the questions but not offer opinions or use this time to help the case to spend more money.

2.1.4. Technical Assessment Protocols

Shortly after the notification, the auditors will provide a document describing the scope (Technical Assessment Protocols). This document will discuss the auditor's plans to perform the audit to include management, operational, and technical aspects of the audit. The document will address de-confliction activities such as Trusted Agents, issues with scanning due to fragile systems, and other areas of concern.

The organization being audited must learn the basics of the standards that the auditors will be using to perform the audit. This knowledge will allow better tailoring of the subsequent data calls, coordination of the resources, and areas to prepare. (Weil)

dwbelangia@hotmail.com

The Technical Assessment Protocols should be received as soon as possible. It is imperative to receive this document to begin preparation. It will identify the audit lead and contact information for all auditors that participate in the engagement.

The Technical Assessment Protocols will provide the data call and the desired format. It will provide information for delivering the data call and the time requirements for delivery. Marking the elements of the data call appropriately (Official Use Only, Sensitive, Classified, etc…) is extremely important.

A discussion must be conducted with stakeholders to review the Technical Assessment Protocols. This is an opportunity to understand the scope and provide feedback to the auditors and even modify the scope.

2.1.5. Trusted Agents

During early meetings, the team should recommend the proposed Trusted Agents. It is suggested that there be a Primary Trusted Agent and a Backup Trusted Agent to assist the audit team with all testing and penetration efforts. The Trusted Agents' primary responsibilities are to assist in removing roadblocks, provide an independent review for de-confliction, and prevent unintentional impacts to operations. The Trusted Agent should be available fulltime, if necessary, to work with the auditors during the audit ensuring attention to detail and the elimination of conflicts. The Trusted Agent(s) will provide insights to the auditors on the environment, how things work, and attempt to eliminate misunderstandings.

The Trusted Agent signature sheets will require the Trusted Agent(s) signatures, the Trusted Agent's manager's signature, an internal cyber security point of contact (the Chief Information Officer (CIO) or Chief Information Security Officer (CISO)), and the auditor's management chain (lead auditor) signature.

The Trusted Agents must be identified early, allowing for de-confliction of their day jobs. These positions will be full-time through the duration of the audit. These Trusted Agents must be approved for this function by their management, the CIO/CISO, and the customer. Once agreement has been received on the Trusted Agents, then the Agreement must be read and signed by the Trusted Agents and their management. The

dwbelangia@hotmail.com

Project Manager will coordinate signatures on the Agreement and will provide the signed Agreement to the Audit Lead, institutional management, and the client before the site audit.

2.1.6. Data Call

One of aspect of the notification must include the request for information, frequently referred to as a Data Call. Before the auditors arrive, the auditors will request lots of information, e.g. network diagrams, system inventories, control descriptions. The more the auditors understand before they arrive, the more efficient and useful the audit will be. (Weil) Ensure the data call is delivered quickly and accurately.

Where possible, every attempt should be made to leverage existing information that has already been gathered. The organization probably responds to multiple data calls during a typical year. It is a fair bet that the auditors have copies of those data calls.

By this time, the institution should have identified the audit lead and the audit lead's associated contact information. The format for the data call, the necessary information for delivering the data call, and the time requirements of the data call should have been received. All data call requests should be coordinated using a single primary contact to ensure efficient use of resources and tracking of the provision of the data call elements to the auditors. The auditors will receive lots of information and might not understand they have something already.

It is imperative that all elements of the data call are marked and managed appropriately (Official Use Only, Classified, etc…). The data call is normally requested by topographical area and will be arranged as either management, technical, or operational. It is strongly recommended that each topographical area be organized in a fashion that allows easy retrieval.

All data call elements should be printed and organized in binders for easy referral and reading by the auditors before they arrive on site. In addition, the electronic copies of the data call should be placed on electronic media. These artifacts should be printed and developed a week before the auditors arrive. The intent is to place the data call in the room for easy access.

dwbelangia@hotmail.com

2.1.7. Monitors

The provision of personnel (monitors) to coordinate the meeting for each agenda item is important. These monitors take attendance, ensure introductions are made, collect actions, keep sessions within schedule time constraints and summarize deliverables or request from the meetings. This allows the interviewees to concentrate on answering questions, providing clarification, and explaining processes. In addition, during the daily out brief, the monitors review notes and make sure the institution keeps an accurate accounting of areas of concern, requests for additional information, and provides an independent insight into how they perceived the meetings.

Monitors should be suggested by the line organization to ensure knowledge and understanding. Their job is to run the sessions and ensure all questions get answered or collected for answering at a later time. They are not there to assist in answering questions.

In case of emergency, the Project Manager must ensure that an attendee list is taken for each session. This will allow for ensuring everyone is safely out, if an evacuation is necessary. Also, emergency contact information for all visitors is needed to ensure notification can be made if something occurs while the auditors are on site. The monitors will perform this function.

2.1.8. Agenda Development

Keeping all management parties involved in the audit status is paramount to success. It is important to establish early the protocols for the client and the institution's management. The Project Manager must work with the CIO/CISO to determine the desired amount of time and frequency that either the auditors or the project team should plan with management. For example; during an audit, there should be an in-brief for management to have the auditors explain the process and intent. The Project Manager should ensure there are daily out-briefs at close of business each day to capture requests and questions the auditors might have. In addition, it is a good time for the auditors to identify any concerns or request for additional information. The daily out-briefs will be about half an hour.

dwbelangia@hotmail.com

The development of the agendas is a Project Manager responsibility and should be accomplished at least one month before to the audit. The agenda should be specific and should be coordinated with the Auditors. It is important to have the right people, rooms and topics for success. When doing system security reviews, it is anticipated that the review will be conducted at the location of the system. This gives the auditors the ability to actually look at equipment and talk with employees to gain a better understanding of strengths, weaknesses and vulnerabilities. It is important to not forget to arrange transportation to and from locations.

As part of developing the agenda, the Project Manager should request if any Audit personnel would require a tour. If a tour is determined to be required, the Project Manager and Logistic Person will contact the Protocol organization at the institution to arrange the tour and ensure a knowledgeable tour guide is available.

Based on the agenda, the institution should know what rooms are required and be able to determine availability early. The institution should reserve the required conference room(s) four months before the audit. Base the size of the conference room on the quantity of auditors expected to be in the room at one time and add 8 people to that number for capacity.

Each day should start with a safety or security topic. Ensure someone is ready to lead this discussion each day. Safety topics that are regionally adapted would be weather concerns, traffic concerns, road construction, local police, high altitude symptoms, or other appropriate topics.

Ensuring that daily in-briefs and out-briefs and the appropriate stakeholders are present is imperative for success. These daily briefings allow the institution to correct misunderstandings, provide additional information, and show engagement and importance of the audit to management.

Daily briefings should be held with the interviewees, monitors, and institutional staff. This can be accomplished while the auditors are performing their daily briefing to each other (usually late in the day). During this meeting of the institutional participants, actions are collected and assigned to individuals for action. It is anticipated that the

dwbelangia@hotmail.com

auditors will conduct a daily out-brief with the team (recommend very small institutional participation) after the auditor's daily meetings. During these meetings, there should be a validation of actions collected from the daily meeting. There may be additional actions not captured from the previous meetings that require attention. Immediately after the auditor briefs the institution, another short meeting should be conducted to assign actions for anything new.

2.1.9. Conference Rooms

The quantity of people in the sessions will vary. Conference room space should be comfortable and easily located. The Institution must ensure rooms are reserved for the daily in-brief, daily out-brief, final out-brief, daily discussions, and any individual interview requirements.

Reserve another room for technical testing and penetration exercises. This room should have good network connectivity to the target networks. The auditors may ship their own equipment so be sure the institution has someone to accept the equipment and to ensure there are no security concerns.

2.1.10. Clearances

Each site will have unique requirements for the sensitivity level of the information being audited by the auditors. Many federal sites have extensive requirements. This section might not apply to some commercial organizations but is included here for those where it does apply.

Transferring clearances, ensuring that badge receipt/access goes smoothly, and ensuring appropriate security authorities are assigned can be challenging. Key advice is to start early. It is suggested that this process start two months before the auditors are supposed to arrive on site. On boarding visitors can present delays and unexpected concerns. Ensuring identification of required training is paramount as without the training, access might be denied to the auditors.

dwbelangia@hotmail.com

2.1.11. Read Ahead

It is also recommended that a document be developed to guide the auditor based on the topographical areas. The development of the story for each data call element helps fill in gaps in understanding for the auditors.

The task of auditing is a complex activity. Ensuring that the auditors understand and can fill in the gaps with regards to approaches can be important in the issues identified and how well the auditors believe the controls mitigate risk.

2.1.12. Final Preparation

One month and then two weeks before the auditors are due on site, check the clearance transfer, badging process, and progress against required training. Training will be unique based on the planned audit areas. Coordinate with the institution's Training Division and Badging to ensure appropriate training has been identified and completed.

One month and then two weeks before the auditors are due on site, check the status on all rooms' reservations.

Two days and one day before arrival of the auditors on site check the room statuses. Ensure everything is clean and arranged properly. Deliver the data call artifacts to the room the morning the auditors are schedule to arrive.

Conduct a briefing for monitors on collecting the attendees list, understanding the evacuation process, capturing actions, ensuring they know agendas, interviewees, and locations for auditors and meetings. If the location is outside of the normal conference room, ensure the monitors know transportation details.

Two weeks before auditors arrive, recheck management calendars to ensure management members expected to attend session are available, that they know location of their participation, and any transportation details.

2.1.13. Entrance Conference

Arrange for someone to meet the auditors at the entry point into the facilities. Explain rules at the particular location (personal cell phone uses, computer use, and any special needs of the auditors). Once the auditors have been processed into the facilities,

dwbelangia@hotmail.com

escort them to meeting rooms. Explain where the restrooms are. Explain any unique requirements that the institution might have. Discuss attendance, emergency contacts, and evacuation details.

Once in the meeting location, immediately route a sign-in sheet collecting local contact information, names, affiliation, etc… While this signup sheet is being passed around, start introductions letting the audit team go first. Next work through introductions and comments by the client and then the institution's management.

Explain the local processes including the role of the monitors and trusted agents. Solicit input and questions from the auditors. Ensure everyone agrees on agenda and then start presentations of topographical areas if appropriate. Some auditors do not want presentations.

It is imperative at this point to ensure the auditors understand management's commitment to the process. The meetings should be scheduled by a senior manager and that manager should be present at the entrance and all out-briefs to ensure continued engagement by the staff. This senior manager should also perform introductions in a very structured manner. The lead auditors should be introduced and ask to talk about the scope of the audit, approach and anticipated agenda. Next the senior manager should introduce any client representatives and ask them to discuss the scope, approach, and any other items they deem appropriate. Then the senior manager should introduce the staff, discuss the scope, and offer assistance to the auditors during their visit. By having the senior management participate in this fashion; the auditors, client and staff understand this is important.

2.1.14. Fieldwork

The auditors will undoubtedly request meetings with a wide variety of personnel to help them understand the policies and procedures and validate that the items identified are in fact implemented. During these sessions, be sure to include the subject matter experts and monitors.

dwbelangia@hotmail.com

Revise agendas daily. Add additional interviews requested by the auditors and also schedule interviews with subject matter experts that can resolve issues identified. These additional interviews must be coordinated with the auditors.

2.1.15. Preparing the Report

The final report must not be completed until after the exit conference. The auditing team should have a good idea of content and should be drafting the report during their audit. This provides the auditors the opportunity to explain the issues and obtain additional clarity if possible. It is possible that an issue might simply be a misunderstanding and by identifying the issue early, the institution can explain further and resolve the misunderstanding.

Normally the final report will not be completed while the auditors are on site. The auditors will continue to develop the report and potentially request additional information for a period of time after departure.

Once the report is close to being finalized, the auditors will provide the report to the institution for a fact checking review. It is to the auditor's and the institution's benefit to ensure all facts are accurate and well understood. If the institution is to fix issues and leverage OFIs, having the facts provides a solid starting point for fixing problems.

2.1.16. Exit Conference

The auditors will request the institution's management to schedule the exit conference. During this meeting, the auditors will present their findings to the management team and SMEs. There should be no surprises during this exit conference. It is imperative that the auditors have reviewed and been provided clarification on all issues being discussed.

An analysis of the risk to the institution should include how each issue could impact the viability of the institution. This should be explained in terms that allow the management team to understand the risk and make decision of the resolution of issues.

dwbelangia@hotmail.com

2.1.17. Report to Management

Once the final report has been fact checked, all questions answered; then the final report should be formally transmitted to the management team. This report should contain an executive summary allowing senior managers the ability to read a small section and understand the risk.

The body of the report should contain enough information to explain all issues and OFIs. Details need to be provided to allow the technical teams to understand the findings and take corrective actions. If insufficient details are provided, the audit's value will be reduced. The intent of the audit to measure risk and provide management the opportunity to disposition that risk.

3. Preparing for the Next Audit

3.1. Findings/Opportunities for Improvement

The audit is done and the auditors have left. The auditors should have a defined schedule for delivery of the final report. This time line must allow time for the institution to fact check any issues, findings or opportunities for improvement. It is important to ensure a clear understanding of any issues that are documented and/or expressed. To fix a problem, the institution must know the details and agree the interpretation of the issues.

3.2. Categorizing/Tracking

The institution must have an approved process for Contractor Assurance. This process must require an oversight board for disposition of issues, findings, and opportunities for improvement. A proposed formal process that reflects something similar to *Figure 1. Casual Analysis Procedure Steps* must be used. By following the Define/Analyze/Document steps, the underlying problems will be identified and allow understanding and the development of viable solutions.

dwbelangia@hotmail.com

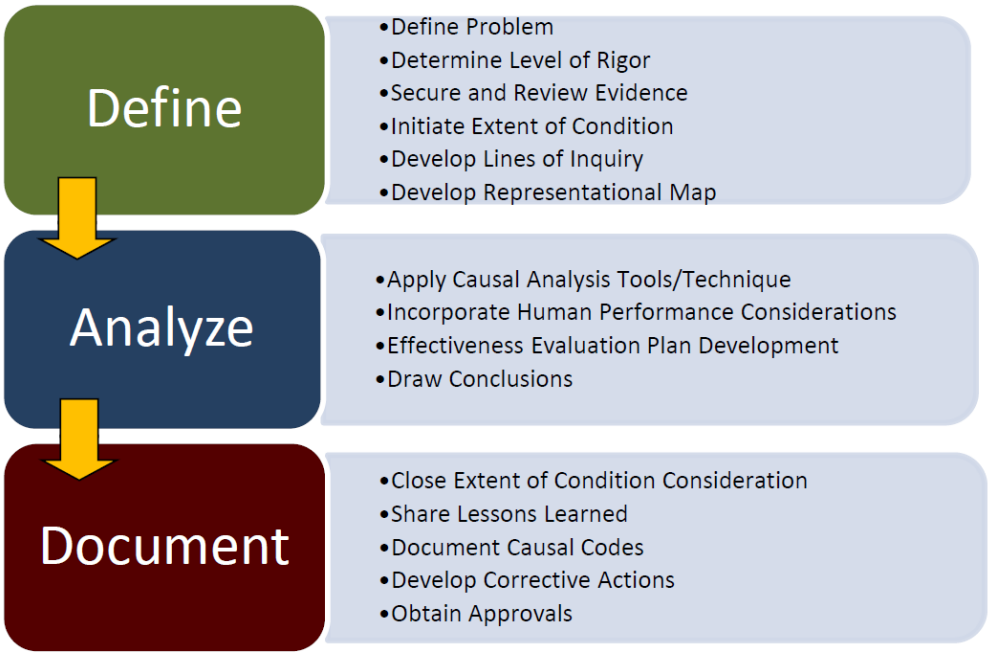


Figure 1. Causal Analysis Procedure Steps (LANL Procedure, 2015)

3.3. Resolution/Sustainability

Resolving issues requires a clear understanding of the issue to enable a process to investigate and categorize the root causes of events. The Root Cause Analysis (RCA) process helps identify what, how and why the issue exist and thus aids in preventing the recurrence. Root causes are the underlying problem, can be identified, and controls can be designed to facilitate prevention in the future. Obtaining an understanding of why an event occurred is the key to developing effective solutions that are sustainable.

The RCA has four steps to include data collection, causal factor charting, root cause identification, and the recommendation of solutions with their implementation. (Rooney, 2004)

Step 1 – data collection – involves performing analysis and collecting pertinent information. This can be accomplished by assembling subject matter experts and asking why, why, why. Repeatedly asking "Why" (five is a good rule of thumb) helps peel away the symptoms which leads to the root cause. (Six Sigma) This step will be the most time consuming.

dwbelangia@hotmail.com

Step 2 – causal factor charting – requires the graphical representation of the collected data to identify gaps in knowledge describing the events that lead to the failure. It should be used to drive the data collection efforts.

Step 3 – root cause identification – provides the opportunity to identify underlying reasons for each causal factor. This approach allows a line of questioning that facilitates answering questions on why this particular event occurred.

Step 4 – recommendation of solutions and their implementation – allows the analyst to formulate solutions to root causes that are achievable and will eliminate the recurrence ensuring sustainability.

All institutions should conduct assessments of their cyber program. To support continual improvement, all previous issues should be revisited to ensure the improvements actually corrected the issue and the improvement is being maintained. A review of issues, their resolution, and understanding the impact of the changes is essential to ensure the next audit is successful. Repeat findings will be more difficult to resolve and the loss of credibility can be devastating.

4. Conclusion

Planning and executing a successful audit that supports senior management's requirements for identifying and allowing a decision on accepting risk from cyber security threats can be difficult and time consuming. Performing it correctly adds tremendous value. All organizations must engage in audits to satisfy contractual requirements and validate the protections being provided to the organization.

By using this paper to assist in executing an audit, the framework driven approach described in the document provides a structured roadmap to surviving the audit and maximizing the value proposition. The sections in this document are presented in a logical manner that will progressively get the company through the audit. The paper and schedule are structured so that for each family of activities in the paper, the schedule identifies unique activities. Working the two together will ensure that all activities happen in a logical fashion within manageable time lines.

dwbelangia@hotmail.com

Appendix A – Audit Management Schedule provides a proposed schedule that has activity dependencies that allow sequencing of events based on a normal calendar (5 days x 8 hours). Once you populate WBS 1.1 with the actual audit dates, the schedule calculates the proposed timing of all other activities. This schedule will allow the organization's team to prepare adequately for the audit and ensure activities receive the appropriate attention. It is recommended the institution change the calendar to reflect the institution's Holidays and any differences in the work week. The activities are duration based and not level of effort based. Unfortunately this minimizes the ability to resource load and de-conflict resource allocation, but does provide useful durations for planning the audit.

5. References

Audit Insights. (2015). Cyber Security 2015. *Information Technology Faculty.* Retrieved from http://www.icaew.com/en/technical/audit-and-assurance/audit-insights.

Coleman, D. (2014, December). Taking Responsibility for Cybersecurity. *Audit Analytics.* Retrieved from http://www.auditanalytics.com/blog/taking-responsibility-for-cybersecurity/.

Cyber security: considerations for the audit committee. (2013). *Cyber security: considerations for the audit committee*. Ernst & Young. Retrieved from http://www.ey.com/US/en/Issues/Governance-and-reporting/Audit-Committee/Cybersecurity---Considerations-for-the-audit-committee.

LANL Procedure No. P322-1. (2015, February). *Causal Analysis and Corrective Action Development.*

Raj, S. (2014). *What The Board of Directors Needs to Ask.* The Institute of Internal Auditors Research Foundation. Retrieved from https://na.theiia.org/special-promotion/PublicDocuments/GRC-Cybersecurity-Research-Report.pdf.

Hoelzer, D. (2014, Q2). *Effective Auditing, Risk Assessment, and Reporting.* SANS Audit 507 Auditing and Monitoring Networks, Perimeters and System.

Rooney, J., Heuvel, L. (2004, July). Root Cause Analysis for Beginners. *Quality Progress.* Retrieved from http://www.nmenv.state.nm.us/aqb/Proposed_Regs/Part_7_Excess_Emissions/NMED_Exhibit_18-Root_Cause_Analysis_for_Beginners.pdf.

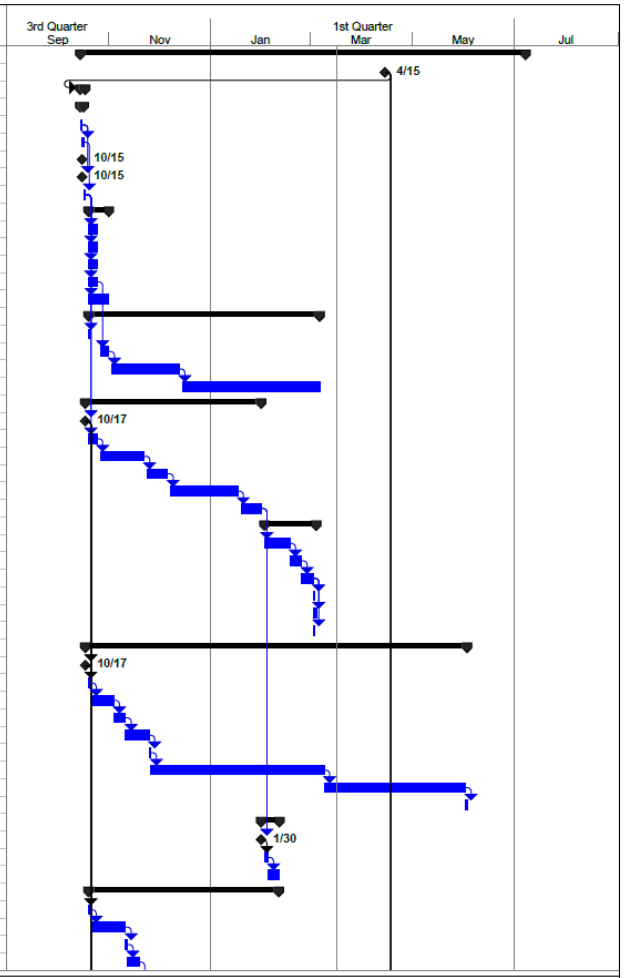
Six Sigma. Determine the Root Cause: 5 Whys. Retrieved from http://www.isixsigma.com/tools-templates/cause-effect/determine-root-cause-5-whys/.

dwbelangia@hotmail.com

Weil S. Pre-audit planning: Four keys to a successful IT security audit. Retrieved from http://searchsecurity.techtarget.com/tip/Pre-audit-planning-Four-keys-to-a-successful-IT-security-audit.

dwbelangia@hotmail.com

ID	WBS	Paper Section	Task Name	Duration	% Compl	Start	Finish	Predecessors
1	1		**HSS Audit Schedule**	190 days	0%	Wed 10/15/14	Tue 7/7/15	
2	1.1		Audit Date	0 days	0%	Wed 4/15/15	Wed 4/15/15	
3	1.2	2.1.1	**Receive Notification**	3 days	0%	Wed 10/15/14	Fri 10/17/14	2FS-130 days
4	1.2.1		**Not Received from Client**	2 days	0%	Wed 10/15/14	Thu 10/16/14	
5	1.2.1.1		Route Announcement Memorandum to Client	1 day	0%	Wed 10/15/14	Wed 10/15/14	
6	1.2.1.2		Client Provides Notification	1 day	0%	Thu 10/16/14	Thu 10/16/14	5
7	1.2.2		**Received from Client**	0 days	0%	Wed 10/15/14	Wed 10/15/14	
8	1.2.2.1		Client Provides Notification	0 days	0%	Wed 10/15/14	Wed 10/15/14	5
9	1.2.3		Assignment of Project Manager (PM)	1 day	0%	Fri 10/17/14	Fri 10/17/14	6
10	1.3	2.1.2	**Assemble Project Team**	10 days	0%	Mon 10/20/14	Fri 10/31/14	
11	1.3.1		Identify Logistics Person -Clearances, Badging, Rooms	5 days	0%	Mon 10/20/14	Fri 10/24/14	9
12	1.3.2		Identify Agenda Master	5 days	0%	Mon 10/20/14	Fri 10/24/14	9
13	1.3.3		Identify Communications Lead	5 days	0%	Mon 10/20/14	Fri 10/24/14	9
14	1.3.4		Contact/Solicit Team Members from Operations and CIO	5 days	0%	Mon 10/20/14	Fri 10/24/14	9
15	1.3.5		Assemble Team and Develop Schedule of Planned Activities	10 days	0%	Mon 10/20/14	Fri 10/31/14	9
16	1.4	2.1.3	**Education and Training of Appropriate parties**	100 days	0%	Mon 10/20/14	Fri 3/6/15	
17	1.4.1		Identify Training Coordinator	1 day	0%	Mon 10/20/14	Mon 10/20/14	9
18	1.4.2		Identify Training/Communications Requirement for Auditors	5 days	0%	Mon 10/27/14	Fri 10/31/14	14
19	1.4.3		Develop Targeted Training	30 days	0%	Mon 11/3/14	Fri 12/12/14	18
20	1.4.4		Deliver Training to Targeted Audience	60 days	0%	Mon 12/15/14	Fri 3/6/15	19
21	1.5	2.1.4	**Receive Technical Assessment Protocols**	75 days	0%	Fri 10/17/14	Fri 1/30/15	
22	1.5.1		Receive Initial Technical Assessment Protocols	0 days	0%	Fri 10/17/14	Fri 10/17/14	9
23	1.5.2		Schedule Meeting with Stakeholders	5 days	0%	Mon 10/20/14	Fri 10/24/14	9
24	1.5.3		Solicit Comments on Assessment from Stakeholders	20 days	0%	Mon 10/27/14	Fri 11/21/14	23
25	1.5.4		Provide Comments Feedback to Auditors on Scope and Schedule	10 days	0%	Mon 11/24/14	Fri 12/5/14	24
26	1.5.5		Received Resolution from Auditors	30 days	0%	Mon 12/8/14	Fri 1/16/15	25
27	1.5.6		Adjust Audit Assessment if Appropriate	10 days	0%	Mon 1/19/15	Fri 1/30/15	26
28	1.6	2.1.5	**ID Trusted Agents**	23 days	0%	Mon 2/2/15	Wed 3/4/15	
29	1.6.1		Identify Trusted Agents	11 days	0%	Mon 2/2/15	Mon 2/16/15	27
30	1.6.2		Solicit Approval from Trusted Agent from Line Managers	5 days	0%	Tue 2/17/15	Mon 2/23/15	29
31	1.6.3		Work any Issues with Selection of Trusted Agents	5 days	0%	Tue 2/24/15	Mon 3/2/15	30
32	1.6.4		Ensure Trusted Agents are Available and Understand Priority of Audit	1 day	0%	Tue 3/3/15	Tue 3/3/15	31
33	1.6.5		Obtain Required Signatures	2 days	0%	Tue 3/3/15	Wed 3/4/15	31
34	1.6.6		Provide to Lead Auditor	1 day	0%	Tue 3/3/15	Tue 3/3/15	31
35	1.7	2.1.6	**Develop Data Call**	162 days	0%	Fri 10/17/14	Tue 6/2/15	
36	1.7.1		Receipt of Data Call Details from Auditors	0 days	0%	Fri 10/17/14	Fri 10/17/14	22
37	1.7.2		Schedule Meeting with Stakeholders	1 day	0%	Mon 10/20/14	Mon 10/20/14	36
38	1.7.3		Collect Any Data Call Elements from Previous Audits	10 days	0%	Tue 10/21/14	Mon 11/3/14	37
39	1.7.4		Review Previous Data Call Elements with Requested Data Call	5 days	0%	Tue 11/4/14	Mon 11/10/14	38
40	1.7.5		Solicit Collection Approach with Project Team	10 days	0%	Tue 11/11/14	Mon 11/24/14	39
41	1.7.6		Determine Electronic and Paper Formats and Approach	1 day	0%	Tue 11/25/14	Tue 11/25/14	40
42	1.7.7		Collect Data Call Elements	73.5 days	0%	Wed 11/26/14	Mon 3/9/15	41
43	1.7.8		Ensure Elements are Labeled Properly Based on Sensitivity	60.5 days	0%	Mon 3/9/15	Mon 6/1/15	42
44	1.7.9		Organize Data Call Elements	1 day	0%	Tue 6/2/15	Tue 6/2/15	43
45	1.8	2.1.7	**ID Monitors**	7 days	0%	Fri 1/30/15	Tue 2/10/15	
46	1.8.1		Schedule Meeting with Staekholders	0 days	0%	Fri 1/30/15	Fri 1/30/15	27
47	1.8.2		Solicit Candidates for Monitors	2 days	0%	Mon 2/2/15	Tue 2/3/15	46
48	1.8.3		Solicit Approval from Monitor's Line Managers	5 days	0%	Wed 2/4/15	Tue 2/10/15	47
49	1.9	2.1.7	**Agenda Development**	81.5 days	0%	Mon 10/20/14	Tue 2/10/15	
50	1.9.1		Solicit Agenda Items from Auditors	1 day	0%	Mon 10/20/14	Mon 10/20/14	22
51	1.9.2		Receive Proposed Agenda from Auditors	15 days	0%	Tue 10/21/14	Mon 11/10/14	50
52	1.9.3		Schedule Meeting with Stakeholders	1 day	0%	Tue 11/11/14	Tue 11/11/14	51
53	1.9.4		Identify Appropriate Participants For Interviews	5 days	0%	Wed 11/12/14	Tue 11/18/14	52



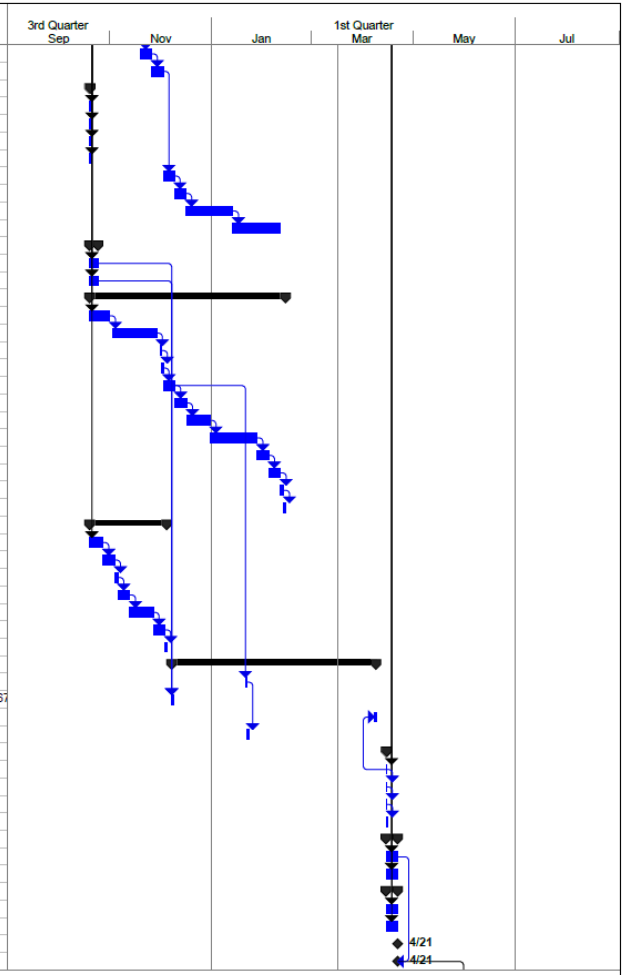
Project: Audit Management Schedule
Date: Tue 3/17/15

Task | Split | Milestone | Summary | Project Summary | External Tasks | External Milestone | Inactive Task | Inactive Milestone | Inactive Summary | Manual Task | Duration-only | Manual Summary Rollup | Manual Summary | Start-only | Finish-only | Progress | Deadline

Appendix A – Audit Management Schedule

dwbelangia@hotmail.com

ID	WBS	Paper Section	Task Name	Duration	% Compl	Start	Finish	Predecessors
54	1.9.5		Obtain Approvals from Line Management	5 days	0%	Wed 11/19/14	Tue 11/25/14	53
55	1.9.6		Identify Time, Location, and Participants for Interviews	5 days	0%	Wed 11/26/14	Tue 12/2/14	54
56	**1.9.7**		**Annotate Agenda**	**0.13 days**	0%	**Mon 10/20/14**	**Mon 10/20/14**	
57	1.9.7.1		Include Daily Team Meeting COB	1 hr	0%	Mon 10/20/14	Mon 10/20/14	22
58	1.9.7.2		Include Time for Auditor Discussion COB	1 hr	0%	Mon 10/20/14	Mon 10/20/14	22
59	1.9.7.3		Include Daily Brief by Auditors to Stakeholders	1 hr	0%	Mon 10/20/14	Mon 10/20/14	22
60	1.9.7.4		Determine and Include Briefing to Senior Management Daily	1 hr	0%	Mon 10/20/14	Mon 10/20/14	22
61	1.9.8		Obtain Approval on Agenda	4.5 days	0%	Wed 12/3/14	Tue 12/9/14	55
62	1.9.9		Determine if Tour is Required	5 days	0%	Tue 12/9/14	Tue 12/16/14	61
63	1.9.10		Work With Protocol to Establish Tour	20 days	0%	Tue 12/16/14	Tue 1/13/15	62
64	1.9.11		Work With Appropriate Organizations for Tour Guides	20 days	0%	Tue 1/13/15	Tue 2/10/15	63
65	**1.10**	**2.1.9**	**Arrange Conference Rooms**	**5 days**	0%	**Mon 10/20/14**	**Fri 10/24/14**	
66	1.10.1		Reserve Conference Rooms for Interviews	5 days	0%	Mon 10/20/14	Fri 10/24/14	22
67	1.10.2		Reserve Test Lab-Conference Room for Penetration Testing	5 days	0%	Mon 10/20/14	Fri 10/24/14	22
68	**1.11**	**2.1.10**	**Clearances**	**85 days**	0%	**Mon 10/20/14**	**Fri 2/13/15**	
69	1.11.1		Solict Input on Who, When, What type Access, Etc. From Auditors	10 days	0%	Mon 10/20/14	Fri 10/31/14	22
70	1.11.2		Receive Information Requested	20 days	0%	Mon 11/3/14	Fri 11/28/14	69
71	1.11.3		Enter Visitors in Access System	1 day	0%	Mon 12/1/14	Mon 12/1/14	70
72	1.11.4		Notify Badging of Visit	1 day	0%	Tue 12/2/14	Tue 12/2/14	71
73	1.11.5		Check Database to Confirm Visitor, Clearance, and Endorsements Are Transferred	5 days	0%	Wed 12/3/14	Tue 12/9/14	72
74	1.11.6		Identify Required Training	5 days	0%	Wed 12/10/14	Tue 12/16/14	73
75	1.11.7		Coordinate Any Training That Can Be Done Before Arrival	10 days	0%	Wed 12/17/14	Tue 12/30/14	74
76	1.11.8		Auditors Complete Off Site Training	20 days	0%	Wed 12/31/14	Tue 1/27/15	75
77	1.11.9		Ensure Training Plans Are Accurate	5 days	0%	Wed 1/28/15	Tue 2/3/15	76
78	1.11.1		Schedule On Site Training/Reserver Room and/or Trainer	5 days	0%	Wed 2/4/15	Tue 2/10/15	77
79	1.11.1		Communicate On Site Training Requirements to Lead Auditor	2 days	0%	Wed 2/11/15	Thu 2/12/15	78
80	1.11.1		Request Early Access to Badging if Appropriate	1 day	0%	Fri 2/13/15	Fri 2/13/15	79
81	**1.12**	**2.1.11**	**Prepare Read Ahead**	**34 days**	0%	**Mon 10/20/14**	**Thu 12/4/14**	
82	1.12.1		Decide on Potential Audit Storys	6 days	0%	Mon 10/20/14	Mon 10/27/14	22
83	1.12.2		Develop Story Board Outline	5 days	0%	Tue 10/28/14	Mon 11/3/14	82
84	1.12.3		Obtain Approval on Story Board Outline	2 days	0%	Tue 11/4/14	Wed 11/5/14	83
85	1.12.4		Identify Subject matter Experts for Story Boards	5 days	0%	Thu 11/6/14	Wed 11/12/14	84
86	1.12.5		Develop Story Boards	10 days	0%	Thu 11/13/14	Wed 11/26/14	85
87	1.12.6		Review/Approval of Story Boards	5 days	0%	Thu 11/27/14	Wed 12/3/14	86
88	1.12.7		Provide Story Boards to Auditors	1 day	0%	Thu 12/4/14	Thu 12/4/14	87
89	**1.13**	**2.1.12**	**Final Audit Preparation**	**88 days**	0%	**Mon 12/8/14**	**Wed 4/8/15**	
90	1.13.1		Check on clearance transfers, badging, and training	1 day	0%	Wed 1/21/15	Wed 1/21/15	73FS+30 days
91	1.13.2		Check on Conference Rooms	1 day	0%	Mon 12/8/14	Mon 12/8/14	66FS+30 days,67
92	1.13.3		Conduct Briefing for Monitors	1 day	0%	Wed 4/8/15	Wed 4/8/15	95SS-5 days
93	1.13.4		Check Calendars of Stakeholders	1 day	0%	Thu 1/22/15	Thu 1/22/15	90
94	**1.14**	**2.1.13**	**Entrance Conference**	**0.5 days**	0%	**Wed 4/15/15**	**Wed 4/15/15**	
95	1.14.1		Meet the Auditors at Arranged Location	1 hr	0%	Wed 4/15/15	Wed 4/15/15	2
96	1.14.2		Escort The Auditors to Rooms	1 hr	0%	Wed 4/15/15	Wed 4/15/15	95
97	1.14.3		Obtain Emergency Information While The Auditors are On Site	1 hr	0%	Wed 4/15/15	Wed 4/15/15	96
98	1.14.4		Perform Introductions	1 hr	0%	Wed 4/15/15	Wed 4/15/15	97
99	**1.15**	**2.1.14**	**Fieldwork**	**5 days**	0%	**Wed 4/15/15**	**Tue 4/21/15**	
100	1.15.1		Manager Work Effort by Auditors	5 days	0%	Wed 4/15/15	Tue 4/21/15	2
101	1.15.2		Ensure Questions are Addressed	5 days	0%	Wed 4/15/15	Tue 4/21/15	2
102	**1.16**	**2.1.15**	**Preparing the Report**	**5 days**	0%	**Wed 4/15/15**	**Tue 4/21/15**	
103	1.16.1		Auditors Begin Developing Report	5 days	0%	Wed 4/15/15	Tue 4/21/15	2
104	1.16.2		Work with Auditors to Assist in developing the Report	5 days	0%	Wed 4/15/15	Tue 4/21/15	2
105	**1.17**	**2.1.16**	**Exit Conference**	**0 days**	0%	**Tue 4/21/15**	**Tue 4/21/15**	
106	1.17.1		Auditors Present Findings to SME, Stakeholders, and Management	0 days	0%	Tue 4/21/15	Tue 4/21/15	100FF



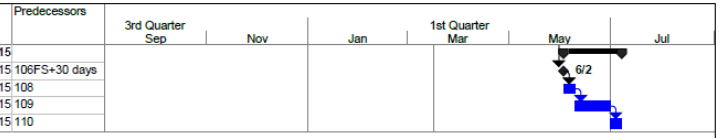
Project: Audit Management Schedule
Date: Tue 3/17/15

Task
Split
Milestone
Summary
Project Summary
External Tasks
External Milestone
Inactive Task
Inactive Milestone
Inactive Summary
Manual Task
Duration-only
Manual Summary Rollup
Manual Summary
Start-only
Finish-only
Progress
Deadline

Appendix A – Audit Management Schedule

dwbelangia@hotmail.com

ID	WBS	Paper Section	Task Name	Duration	% Compl	Start	Finish	Predecessors
107	**1.18**	**2.1.17**	**Report to Management**	**25 days**	0%	**Tue 6/2/15**	**Tue 7/7/15**	
108	1.18.1		Receive Auditors Draft Report	0 days	0%	Tue 6/2/15	Tue 6/2/15	106FS+30 days
109	1.18.2		Provide Factual Accuracy Review	5 days	0%	Wed 6/3/15	Tue 6/9/15	108
110	1.18.3		Review Issues and Details	15 days	0%	Wed 6/10/15	Tue 6/30/15	109
111	1.18.4		Provide Feedback to Auditors	5 days	0%	Wed 7/1/15	Tue 7/7/15	110



Project: Audit Management Schedule
Date: Tue 3/17/15

Task | Split | Milestone | Summary
Project Summary | External Tasks | External Milestone | Inactive Task
Inactive Milestone | Inactive Summary | Manual Task | Duration-only
Manual Summary Rollup | Manual Summary | Start-only | Finish-only
Progress | Deadline

Appendix A – Audit Management Schedule

dwbelangia@hotmail.com