COSMOS
Navigate the Compliance Universe

Compliance Today - July 2022
Guide to a compliance gap assessment

By Alisa Lewis, CHC, CRISC

Alisa Lewis (alisa.m.lewis@hotmail.com) is Director, Privacy and Compliance, at Diameter Health, Farmington, Connecticut.

- linkedin.com/in/alisa-lewis-chc-crisc/


Alisa Lewis

Would you be surprised if I told you we perform gap assessments in our daily lives? Take, for example, meal planning. You determine what you are going to eat for the week, identify the ingredients you will need, find out which of the ingredients you have already, make a list of the additional ingredients needed, and then go grocery shopping.

A gap assessment (or gap analysis) is a comparison between the current state and the desired state. The difference between the current state and desired state are the gaps. Once gaps have been identified, they should be documented, shared with management and appropriate stakeholders, and remediated by the appropriate personnel.

In the meal-planning example, the desired state is having all the recipe ingredients you need to make your meals for the week. The current state is the ingredients you already have in your home. The gaps are the ingredients you need to make the meals but you do not have on hand. The documentation of the gaps is the grocery list. And the remediation takes place when you buy the missing ingredients at the grocery store.

Five uses of a gap assessment

Gap assessment can be performed for a variety of circumstances. I have used them in several ways and have gained valuable information each time. Let us look at five uses of a gap assessment.

To determine whether your compliance program is adequately designed

Title 9 of the U.S. Department of Justice *Justice Manual* states, "critical factors in evaluating any [compliance] program are whether the program is adequately designed for maximum effectiveness in preventing and detecting wrongdoing by employees and whether corporate management is enforcing the program or is tacitly encouraging or pressuring employees to engage in misconduct to achieve business objectives."[1] Additionally, the manual states that to determine whether a program is well designed, the "prosecutor should consider the comprehensiveness of the compliance program."

While the *Evaluation of Corporate Compliance Programs* recommends a risk assessment be performed to determine whether an organization is adequately designed,[2] a gap assessment can be an important step before the risk assessment.

Here's why: No two organizations face the same sets of requirements. A compliance program that is adequately designed for one organization may not be adequately designed for another. To determine what "adequately designed" means to your organization, you need to consider the services you provide, your customers, and

applicable laws and regulations. Do you use offshore resources? Are you a federal subcontractor or do you receive Medicare or Medicaid payments? Are you a covered entity or a business associate? Answering questions like these will help establish applicable requirements.

Once you have determined your requirements, you can perform a gap assessment to determine what gaps exist between requirements and your current program. After gap remediation and once your controls have begun operating within your environment, you can perform an accurate risk assessment to ensure the remediation put in place is appropriate and is meeting the needs of your organization.

When you are new to the organization

Starting a new job at a new organization can be daunting. There is so much to learn and absorb. While employers have new-hire training programs in place, the training program most likely will not teach you everything you need to know about compliance within the organization. A gap assessment can be used to understand what requirements the organization has in place, identify how the organization is currently meeting requirements, and whether there are any gaps in meeting the requirements. It gives you a formal process for learning about the organizational requirements and using the information in a real and meaningful way.

When you are a part of a merger or acquisition

When your organization acquires or merges with another organization, each organization may have different controls in place, or controls implemented differently. The gap assessment process can help you identify compliance requirements, or other sets of requirements, under the new organizational structure. Through the gap assessment, you can systematically document the existing controls and determine whether there are any gaps.

To prepare for new regulations or requirements

Are you considering exporting goods or services? Are you expanding offerings to the European Union? Such changes affect your compliance landscape. If your organization is considering expanding services or tapping new markets, you need to be aware of compliance implications these changes will have on your current program. Through the gap assessment process, you will identify and document the requirements the new service or market will bring to your organization and assess what you may already have in place. It is possible your current processes may meet some of the new requirements or can be modified to meet the new requirements. The gaps identified can be used to create a list of tasks that can be incorporated into a project plan to bring your organization to compliance with the new service or market segment requirements.

To improve the maturity of your program

A compliance program maturity model is a tool that is used to measure program maturity. There are various compliance maturity models available. Each model may have different terminology, but in general, maturity levels range from ad hoc or incomplete to optimizing. Ad hoc or incomplete means the program is not formalized and processes are not repeatable. Optimized means the program is in a continual improvement state and is agile and can anticipate needs. To perform a maturity model gap assessment, you use a compliance program maturity model as the framework you are measuring against, determine the maturity you want to achieve (desired state), identify where your program currently falls on the model (current state), and assess gaps that exist between the two states. Remediation of the gaps increases the maturity level of your organization.

Overcoming obstacles

One obstacle of a gap assessment is that the process can be a significant investment of time depending on the framework selected, the number of resources (people) involved, and the availability of those resources. To overcome this drawback, you should obtain management support from both your manager and the chain of command. An effective way to do this is to explain why you are performing the gap assessment, the expected amount of time the assessment will take, the expected impact on other departments, and the outcomes expected. If your management understands the benefits of performing the gap assessment and you have a clear, identified plan of completing the assessment, management support can be gained.

The impact the gap assessment has on other departments can also be an obstacle. Other departments may be involved in the process through interviews or documentation gathering and remediation of the identified gaps. To overcome this obstacle, you will have to obtain buy-in from management across the organization. To obtain buy-in, explain why you are performing the gap assessment, the amount of time their respective departments will need to commit to the gap assessment, the expected benefits of the gap assessment, as well as the efforts that will be required to remediate the identified gaps.

Performing the gap assessment

A gap assessment is not a one-size-fits-all process. You will need to structure an assessment methodology that best works for you. The process that I have found to be most effective include the phases identified in Figure 1.

Figure 1: Assessment methodology structure

Phase 1: Plan

As with any project, planning is an essential component. There are various parts of gap assessment planning:

- Identify the scope;
- Determine methodology;
- Determine appropriate resources;
- Document project plan, including specific due dates;
- Identify roles and responsibilities; and
- Determine communication plan.

Identify the scope

The scope of the gap assessment includes the topic you are assessing and what business units are included. Are you going to assess your compliance program, compliance with Health Insurance Portability and Accountability Act (HIPAA)/Health Information Technology for Economic and Clinical Health Act regulations, contractual agreements, General Data Protection Regulation requirements, or a compliance program maturity model? The possibilities depend on the services your organization provides, your customers, and applicable regulations and requirements. If the organization is large, assessing one business unit may be most practical given the topic being assessed. If the organization is small, the assessment's scope may include the whole organization.

Once you have identified the scope, identify the framework that will be assessed. For example, if you are assessing your compliance program, you can use the U.S. Sentencing Commission Guidelines, the U.S. Department of Justice's *Evaluation of Corporate Compliance Programs*, or corporate integrity agreements to identify the requirements. The framework will be further documented in the identification phase.

Clearly identifying the scope before the gap assessment begins helps prevent scope creep. Scope creep, a project management term, is when "the original project scope expands…without the corresponding adjustments to time, budget, or other project resources."[3] Scope creep can happen if additional requirements are added during the assessment. It can negatively affect the assessment by increasing resource and time needs and delaying the completion of the assessment.

Determine methodology

Methodology is "a body of methods, rules, and postulates employed by a discipline: a particular procedure or set of procedures."[4] A gap assessment methodology is the method or procedure you will use to complete the assessment. The identification, investigation, and assessment phases described in this article are the gap assessment methodology. Methodology also includes the process used to obtain information (e.g., through interviews or reviewing documentation and other evidence for what is currently in place). Determining the methodology will help you assess the time it will take to complete the assessment and will help in developing the project plan.

Determine appropriate resources and stakeholders

Based on the scope of your assessment, identify who within the organization will be subject matter experts (SMEs) on current processes. Selecting a combination of nonmanagement and management personnel allows the assessor to gain a clear picture of the current processes. For example, if you are performing a HIPAA Privacy Rule gap assessment, determine which departments in the organization handle access requests, disclosure requests, restriction of disclosures, and other HIPAA Privacy Rule requirements. You may not be able to identify the specific person that will need to be interviewed during the planning phase; however, by identifying the department, you can provide information regarding the assessment to the department's management (see earlier "Overcoming Obstacles" section).

The gap assessment stakeholders will depend on the assessment scope. Stakeholders will include gap assessment resources (i.e., SMEs), management, and senior or executive management.

Document the project plan

Documenting a formal project plan is a crucial piece of planning a gap assessment. It provides an outline of the process that will be followed, timelines, and resources (departments or personnel involved). The project plan includes each phase of the gap assessment and tasks that will be required to complete the phases. If possible, estimate the number of hours or days each task and phase will take. The project plan also includes milestone dates that will help keep the project plan on time. The project plan is updated as the gap assessment progresses.

Identify roles and responsibilities

Prior to beginning the gap assessment, document roles and responsibilities of the resources involved to the extent possible. Roles can include the assessors, personnel resources for interviews and remediation, and management. Responsibilities include but are not limited to scheduling meetings, identifying the requirements, attending scheduled meetings, responding to interview questions, documenting the report, communicating

remediation requirements to personnel, completing remediation efforts, and monitoring remediation to ensure completion. A RACI (Responsible, Accountable, Consulted, Informed) chart is useful to document the roles and responsibilities. Defining roles and responsibilities during the planning phase will alleviate issues during the gap assessment.

Determine communication plan

During planning, also consider communication methods. Who are the key stakeholders that should be provided with updates? How frequently should updates be provided to them? What detail should be provided to them?

Each organization has a different information-sharing culture, and that should be considered in determining the communication methods and frequency. Sharing a high-level project plan that includes milestone dates with management, senior management, and other stakeholders gives them visibility into the project. If possible and appropriate to the organization, publish the project plan and updates to a shared drive or website so stakeholders and other resources can view it on an as-needed basis.

Phase 2: Identification

During the identification phase, identify the requirements that are a part of the framework and determine the applicability of the requirements to your organization. If you are unfamiliar with any of the requirements, research them or speak to SMEs to gain a better understanding. It is important to have a strong understanding of the requirements before you move on to Phase 3.

An important piece of this phase is documentation. Document the requirements, including the source document. This documentation can be done in a spreadsheet, text document, or software intended for this purpose. For example, if you are performing a gap assessment to identify gaps between contractual requirements and current processes, document each in-scope contractual requirement along with the source contract(s) the requirement was found in. This detailed documentation will supplement the final report and will ensure you are able to answer any questions about the requirement.

Not all requirements within the framework may be appliable to your organization. For example, if you are a HIPAA business associate, the requirement to maintain a notice of privacy practices does not apply to you.[5] Document these nonapplicable requirements along with the explanation of why they are not applicable to the organization.

The output of this phase is documentation of the desired state (i.e., the in-scope applicable requirements you are assessing gaps against).

Phase 3: Investigation

The purpose of the investigation phase is to determine how the organization currently adheres to the requirements identified in Phase 2. After identifying the applicable requirements in the selected framework, investigate the organization's current state by interviewing SMEs and reviewing documents. What policies, documentation, and processes are currently in place that meet the requirements? Document the organization's current state in the system or spreadsheet that the requirements were documented in during the identification phase.

Before interviews or document reviews begin, ensure you have a strong understanding of the requirements. Prior to interviewing, write down the questions you will ask the SME. It will make the interview go more smoothly, and the interviewee will appreciate that you were prepared. During the interview, write down what was discussed

and any responses the SME provided. If they mention a policy or procedure document in place, ask for a copy of the document. When you review the supporting documentation (e.g., policies, procedures), write down the name of the document, where it is stored, and what within the document met requirements.

The output of Phase 3 is documentation of the current state (i.e., how the organization is currently meeting the requirements identified in Phase 2).

Phase 4: Assess

The next phase is to assess the differences between the current state and the desired state. During this phase, examine the requirements documented in Phase 2 (the desired state) and compare them with the information learned from the resources and the documentation during Phase 3 (the current state). Any differences in the requirements as compared to the current state are documented as gaps. If the requirement is partially met, a gap should still be identified. Use the spreadsheet or system used in Phases 2 and 3 to document the identified gaps.

In addition to gaps, during this phase, document recommendations to remediate the gaps. The intent of the recommendation is to provide guidance to the organization to bring it into compliance with the requirement.

While not required to be a part of a gap assessment, organizational leaders may ask for gaps to be assigned a risk ranking to prioritize remediation. Since gap assessments are not designed to assess risk, the assessor can decide whether to include risk rankings. Unless a full risk assessment is performed on each gap, I recommend clearly documenting in your report (see Phase 5) that the purpose of the gap assessment was not to assess risk but to document gaps, and that the risk ranking is an estimation of a risk to help assign priority ranking.

The output of Phase 4 is documentation of the gaps between the desired state and the current state, as well as remediation recommendations.

Phase 5: Report

Thoroughly and accurately document the gap assessment findings in a report so the information and remediation recommendations can be shared with stakeholders. The report should include an executive summary, purpose, scope, methodology, findings summary, detailed findings, recommendations, and a conclusion. Including graphs with trends of data may be helpful to draw attention to areas of concern. In an appendix, provide a listing of resources that were interviewed and list documents that were reviewed.

Clearly documenting the purpose and scope within the report is important so readers have a strong understanding of what the gap assessment considered. If the purpose and scope are poorly documented, the readers may have unrealistic expectations of the assessment.

The detailed findings should include information of all the requirements that were assessed, including requirements where no gaps were identified and requirements that were determined not to be applicable. The detailed findings can be addressed in the body of the report or as an appendix.

Graphs showing high-level results and trends of data can be used in slide decks to share with senior management or the board of directors.

Phase 6: Remediation

The final phase is remediation. Remediation is "the correction of something bad or defective."[6] In the case of a gap assessment, the gaps identify the deficiencies between the desired state and the current state. The person or department that was identified for managing remediation during the planning phase will be responsible for the

remediation effort. For any gaps not remedied, the organization should determine how they are treated. If the gap is related to a contractual or regulatory requirement, the organization should consider managing the untreated gap as a risk.

Conclusion

A gap assessment can be used within a compliance department for multiple use cases, each with its own purpose. The assessment can provide a framework for ensuring the program is adequately designed, provide insight if you are new to the organization, help eliminate deficiencies after a merger or acquisition, prepare for new regulations, or help improve the maturity of the compliance program. If properly supported, planned, designed, and documented, a gap assessment can provide meaningful and actionable results that will enable your organization to go from its current state to its desired state.

Takeaways

- A gap assessment (or gap analysis) is a comparison between the current state and the desired state.
- There are multiple use cases for performing a gap assessment.
- To overcome obstacles, communicate the gap assessment plan with stakeholders and management to gain buy-in.
- Phases of a gap assessment include planning, identification, investigation, assessment, report, and remediation.
- Documentation of the desired state, current state, and gaps is an essential component of a gap assessment.

1 U.S. Dep't of Just., Just. Manual § 9-28.800 (2019).
2 U.S. Dep't of Justice, Criminal Div.,*Evaluation of Corporate Compliance Programs* (Updated June 2020), https://www.justice.gov/criminal-fraud/page/file/937501/download.
3 Jose Maria Delos Santos, "What is Scope Creep in Project Management?" ProjectManagement.com, last updated April 28, 2022, https://project-management.com/scope-creep/.
4 "methodology," *Merriam-Webster Dictionary*, accessed May 11, 2022, https://www.merriam-webster.com/dictionary/methodology.
5 "Does the HIPAA Privacy Rule require a business associate to create a notice of privacy practices?" FAQs, U.S. Department of Health & Human Services, last reviewed July 26, 2013, https://www.hhs.gov/hipaa/for-professionals/faq/390/does-hipaa-require-a-business-associate-to-create-a-notice-of-privacy-practices/index.html.
6 "remediation," Dictionary.com, last accessed May 11, 2022, https://www.dictionary.com/browse/remediation.