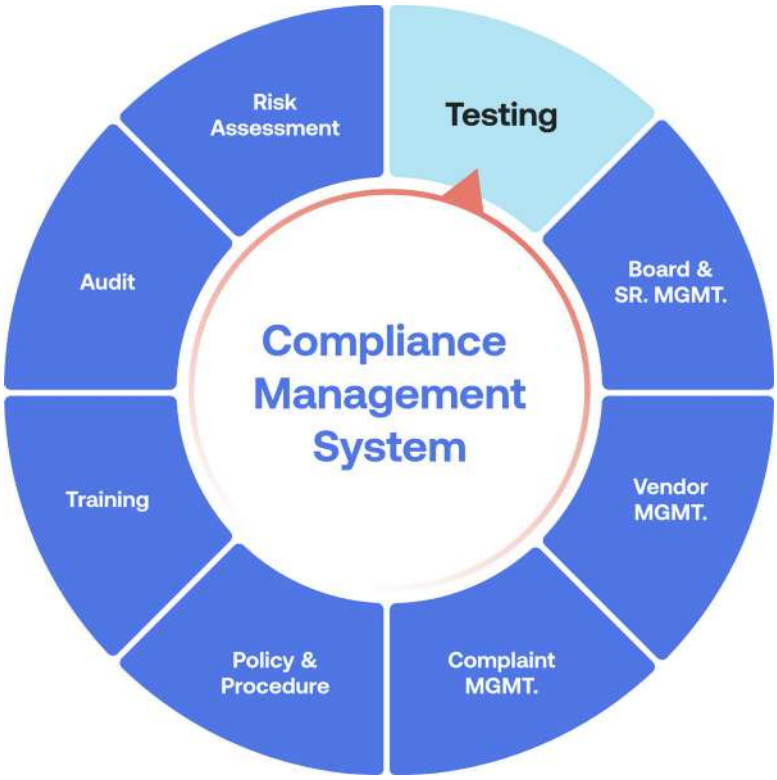
2022 Guide to Implementing an Effective Compliance Testing Program

AUDITBOARD

Table of Contents

Importance of a Compliance Testing Program

Compliance testing is an integral part of ensuring that your organization's Compliance Management System (CMS) is functioning as intended. As many workforces continue in a hybrid or remote working model, securing and protecting networks, information assets, and sensitive data — through effective compliance testing — remains a top priority in 2022. Identifying violations of requirements (e.g., regulatory or internal policy) and remediating the root cause in a timely manner is crucial to mitigating the compliance risks your organization is facing. Implementing an effective compliance testing program is of critical importance to ensuring the health of not only your CMS, but your entire organization.



When performing compliance testing, it is important to remember that you are testing against a rule, regulation, law, or statute, which means that any finding is technically a violation of law or a statute. Regardless of which function is performing your organization's compliance testing — whether it is the internal audit or compliance department — the eight steps discussed in this whitepaper will help you successfully implement an effective compliance testing process as part of your Compliance function.

Step 1: Build the Requirements Library

Whether your organization already has a small or piecemeal compliance testing program or you're creating a program from scratch, your first step will be to build the requirements library in order to establish the requirements applicable to your organization, which will later be used to identify the existing controls (or lack thereof) that mitigate the compliance risk to your organization.

A requirements library is essentially an inventory of in-scope requirements that are then used to identify the compliance risk to your organization. To build out the library, you will need to identify all of the regulatory requirements that are applicable to your company's operations. You may want to consult with a subject matter expert in your industry to assist with identifying all of your organization's in-scope requirements, then work with executives from each business function, including your legal team, to ensure that all applicable requirements have been captured.

Next, map the requirements to their applicable business function and work with the relevant business owners to define the compliance risks. At this point you should also validate the applicability of the requirement with the business owners. This will help the business understand in clear terms what each compliance risk is, why it could happen, and the importance of each requirement.

> **Best Practice:** make an effort to define the risk in terms that an employee at any level of the workforce will understand, from the analyst level all the way up to the executive level. Risk statements should distill relevant information into its most basic, actionable form.

Once requirements have been mapped and risks have been defined, identify the existence of controls to mitigate your compliance risks. This is an ideal opportunity to perform a cross-walk to determine how many controls mitigate each compliance risk and where testing should be focused in the future to minimize duplicative testing and reduce inefficiency.

This library should be established as the only source of truth in regard to the requirements that apply to your organization, and should be the only reference point used when communicating regulatory requirements. Having this central source of record is critical to helping your organization understand its obligations and what requirements it must abide by.

> **Best Practice:** maintain the requirements library within a cloud-based connected risk platform to ensure that the integrity of the source of truth is maintained. Within a system, controls can be implemented to prevent unauthorized users from making unintended additions, deletions, or other changes that could compromise the requirements library.

Step 2: Perform a Compliance Risk Assessment

First, you will need to define the parameters of your compliance risk assessment, including the measurement categories, factors to be measured, and data sources that will be used to conduct the risk assessment.

For each risk, evaluate the inherent risk — the risk of violating a requirement absent of controls — by measuring the impact and likelihood of a regulatory violation. Then, obtain the control effectiveness rating of the control that mitigates the risk. Once you have evaluated the inherent risk rating and control effectiveness rating, you can derive the residual risk for each requirement using a matrix.

Step 3: Develop the Compliance Testing Methodology

After performing the risk assessment, you will need to develop a compliance testing methodology to establish how you will test in-scope requirements and/or their associated controls.

To develop the testing methodology, you will need to define the following:

1. Testing approach, including purpose, scope, and objective.
2. Sampling method that will be used when performing testing.
3. Process to be followed when compliance violations or issues are identified.
4. Compliance testing function's involvement during the remediation process.
5. Reporting requirements, including the intended audience.

It is important to communicate the testing methodology to the audit stakeholders and any other relevant parties that perform testing to minimize any duplication of efforts. Communicating a clearly defined methodology to the business early on in the testing process can also help to promote cooperation by educating stakeholders about what to expect and the relevant time frame for testing. Even better, someone who understands the process is more likely to facilitate testing by supplying the information needed to test on schedule.

Your methodology may evolve year over year as your compliance program reaches a higher level of maturity. In the first year, your objective may be simply to ensure that all areas are compliant with law by testing all requirements in your library. In future years, compliance testing does not need to be limited to verifying compliance. It can also be an excellent opportunity to test the controls that mitigate the compliance risk.

Step 4: Build the Testing Schedule

Use the residual risk established in the compliance risk assessment to determine the testing frequency for each requirement. Your schedule will vary depending on your team size and objectives. The following is one example of a testing schedule:

- **High residual risk:** quarterly
- **Medium residual risk:** semi-annually
- **Low residual risk:** annually

Additionally, group your requirements by business function or overarching regulation and specify the time frame when each of those groups will be tested.

> **Best Practice:** add the scheduled period as a data point within your risk assessment to ensure you have testing coverage over all requirements.

Once your schedule is complete, communicate the schedule to your audit stakeholders so that each business function understands when you will be testing them and what you'll be testing against.

Step 5: Perform Testing

The following are the general steps for performing testing:

1. Notify your audit stakeholders about planned audits well in advance, including notifying them what will be required of process owners and department leads. Allot ample time for submitting document requests and reviewing the evidence gathered.
2. Obtain the data and materials required to perform testing against the regulatory requirements.
3. Test in accordance with the established testing methodology that you communicated to the audit stakeholder. This will create efficiency within the process by ensuring that your testing process stays consistent, as well as reducing confusion and frustration.
4. Document the testing programs and maintain evidence of the testing results.
5. Follow up on findings to ensure any issues or control gaps identified are not false positives.
6. Communicate final results to the audit stakeholder. Obtain approval or agreement on any issues identified from the impacted business function.
7. Once all testing steps are completed, draft and issue the final report of your results to the relevant parties such as the Audit Committee.

Step 6: Issues Management Process

Once you have identified and confirmed issues or control gaps, the next step is to implement an issues management process that defines how you will manage an issue from identification through remediation.

Start by entering identified issues into your issues management system. Then, assign ownership by establishing which business function is responsible for the

compliance violation based on the mapping you completed when building your requirements library.

Establish the severity impact rating. When rating violations of law, best practice includes assessing the pervasiveness, duration, and severity of the violation. Below is an example:

Date 1/10/2022	Issue ID 458952	Regulatory Violation Yes	Requirement 50 USC 3937(a)(1)
Overall SIR			High
Severity	Considerable impact to the customers since the interest rate being charged was greater than the 6% cap enforceable during the active duty period.		8.2
Duration	The issue occured for a period greater than two months but less than five months.		5.2
Pervasiveness	8% of the sample population tested failed.		7.8

Example of a severity impact rating featuring high severity and pervasiveness, and medium duration.

Finally, document the root cause of each issue, and work with the audit stakeholder to document the remediation plan to address that root cause, including milestones to be achieved and target dates.

Step 7: Validate Remediation

Once the milestones of the remediation plan have been completed, it is time to validate that the plan worked as intended. Validation should ensure that the corrective actions addressed the immediate issue, and that the long-term remediation prevents the issue from recurring in the future. Reperformance of testing may be required to adequately validate that the remediation plan worked. Also note that you will need to obtain evidence of remediation plan completion.

Step 8: Monitor Sustainability

Because compliance testing issues are violations of law, a best practice is to establish a period of sustainability that must be achieved in order to close the issue.

> **Best Practice:** use, at minimum, a two month period where no recurrence of the regulatory violation has occurred. Based on your company's risk appetite, you may want to increase the number of months.

At the end of the sustainability period, gather and maintain evidence that the issue did not reoccur. If the issue did not reoccur, you can close the issue.

If the issue did reoccur during the sustainability period, the next step is to reestablish the root cause and adjust the remediation plan accordingly.

Conclusion

Though companies that operate in a regulated environment are expected to have a CMS, some may opt to perform compliance testing in an ad hoc manner. However, doing so can lead to increased regulatory scrutiny, since your organization will not be able to effectively demonstrate that it has a fully functioning compliance testing program. By following these eight steps — or as many as are appropriate for your organization's maturity and risk appetite — you will be adequately positioned to get your organization's compliance testing program up and running.

About AuditBoard

AuditBoard is the leading cloud-based platform transforming audit, risk, and compliance management. More than 30% of the Fortune 500 leverage AuditBoard to move their businesses forward with greater clarity and agility. AuditBoard is top-rated by customers on G2 and Gartner Peer Insights, and was recently ranked for the third year in a row as one of the fastest-growing technology companies in North America by Deloitte.

To learn more, visit: AuditBoard.com.