ARCHER

WHITE PAPER

8 Steps to Modernize Compliance

Organizations today must comply with a multitude of regulations, industry standards, internal policies and contractual commitments. Failure to comply can result in failure to achieve objectives, regulatory fines and sanctions, litigation-related losses, and reputational damage. The challenge of compliance is made even more difficult by rapid regulatory growth. In fact, 37% of compliance practitioners polled worldwide cited the volume and pace of regulatory change as the biggest challenge they face.[1]

Growing, changing obligations also expose organizations to substantial cost. For example, just to comply with U.S. federal regulations, estimated compliance costs in banking range from 5-10% or more of non-interest expense[2]; for manufacturing, 11%[3]; and across the healthcare industry, contributing to 25% administrative costs annually.[4]

Organizations must commit not only financial resources to compliance obligations but also human resources. The U.S. Bureau of Labor Statistics projects 6% growth over the next several years in the demand for compliance officers.[5] This is at a time when the unemployment rate for compliance officers is at historically low levels.[6] This suggests there will be insufficient resources to fulfill the need.

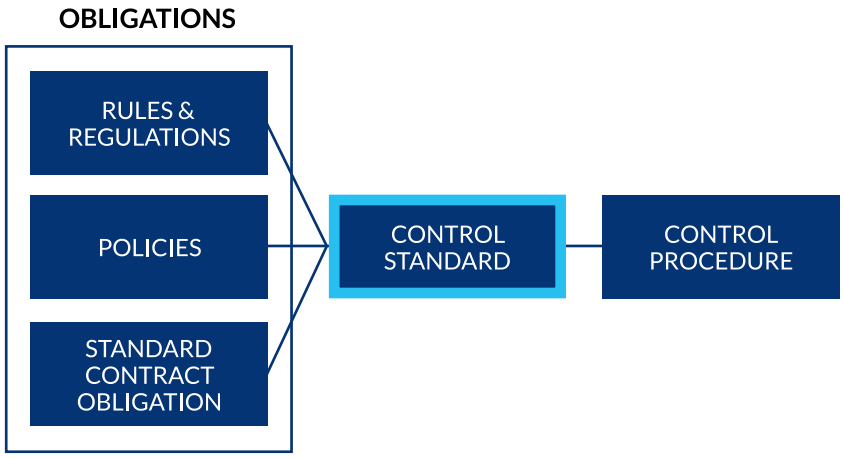
In light of all these factors, organizations need to find ways to operate compliance programs more efficiently and effectively. The following steps to modernize compliance programs can help achieve that end.

37% of compliance practitioners polled worldwide cited the volume and pace of regulatory change as the biggest challenge they face.[1]

Steps to Modernize Compliance

1. Harmonize Obligations

Many statutory rules and regulations, standards, policies and procedures, and contractual obligations have overlapping requirements, yet compliance programs are designed to address obligations individually. When organizations instead identify common links and map together, multiple obligations can be harmonized around one control standard statement, which can be further linked to control procedures implemented to ensure compliance.



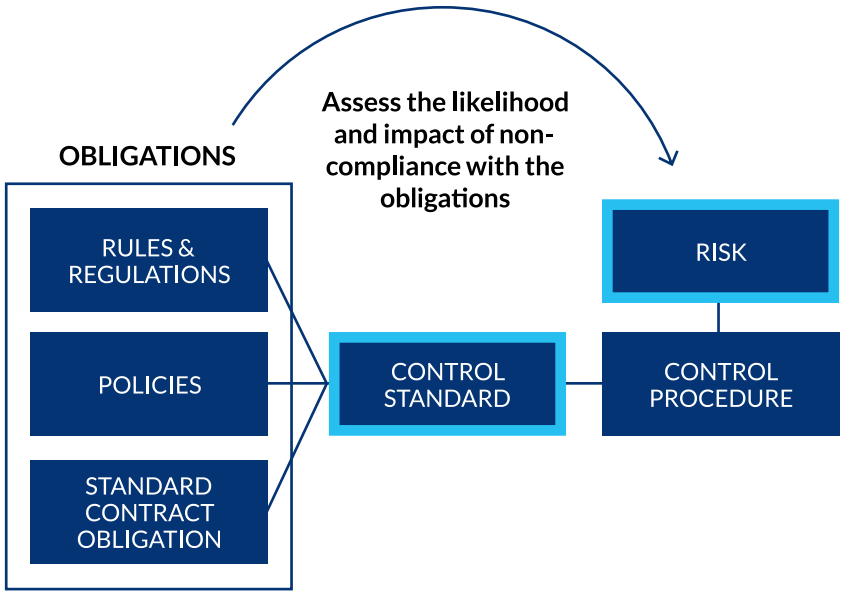
Control procedures (aka internal controls) are technical or organizational activities designed to mitigate risk. Controls may be detective, preventive and/or corrective. A well-designed control will be identified as continuous or periodic and be assigned to a named individual for accountability.

Control standards are statements that harmonize comparable obligations. For example, in addition to laws requiring that only authorized individuals have access to systems and data, this obligation may be found in standards (such as PCI), information security policies and contractual obligations. The obligations can be logically linked and harmonized via a control standard statement and then logically linked to actual control procedure(s). The point is to be able to test one control to demonstrate compliance with all related obligations, saving time and freeing up compliance resources for other, more critical activities.

2. Adopt Risk-based Compliance

No organization has the unlimited compliance resources it would take to achieve 100% compliance with all obligations, and so must carefully choose where to allocate resources, based on the relative likelihood and impact of a compliance failure. For example, the penalties for enabling terrorist financing are quite severe in the U.S., compared to those for accidentally failing to sign a tax filing. An organization would therefore do well to devote considerably more resources to anti-terrorist compliance.

Applying risk assessment principles to compliance is a modern approach to enhancing the efficiency and effectiveness of an organization's compliance program.

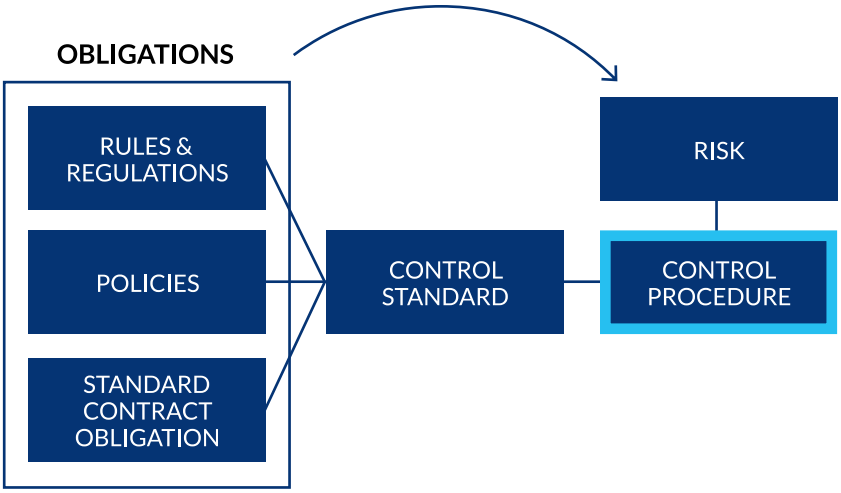


Risk assessment methodologies can be qualitative or quantitative; the appropriate methodology often depends on the maturity of an organization's risk management program and available resources.

Risk assessment methodologies can be qualitative or quantitative; the appropriate methodology often depends on the maturity of an organization's risk management program and available resources. Organizations may assess risk on an inherent basis, residual basis or both (a best practice). For example, there is the inherent risk that a worst-case violation of the EU General Data Protection Regulation (GDPR) could result in a fine of up to €20 million, or 4% of annual global revenue, whichever is greater. Violation of a customer contract obligation is likely to be capped at a much lower amount. In both cases, consideration of existing risk treatments would likely yield much lower residual risk assessments.

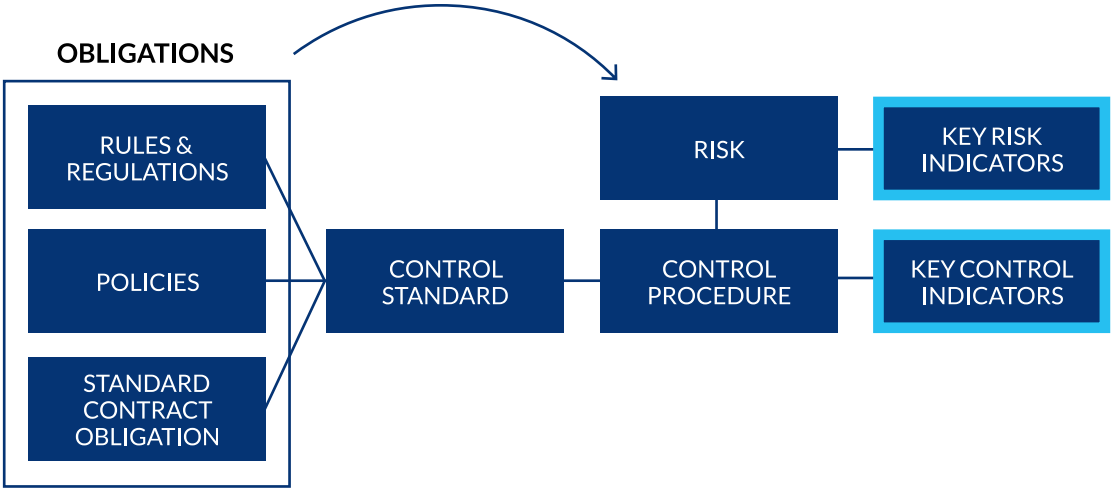
3. Institute Risk-based Controls

Once risk assessments are completed and risk ratings have been assigned to obligations, control procedures designed to treat noncompliance should be established commensurate with the level of risk. Using the example above, an organization would establish more robust and onerous control procedures to minimize the likelihood and impact of GDPR noncompliance than it would to address the prospect of a customer contract violation.



4. Establish Continuous Monitoring

Continuous monitoring refers to tracking both metrics associated with risks and controls that indicate changing risk and control procedures. Optimally, indicators selected for monitoring will be leading indicators of increasing risk and deteriorating controls.

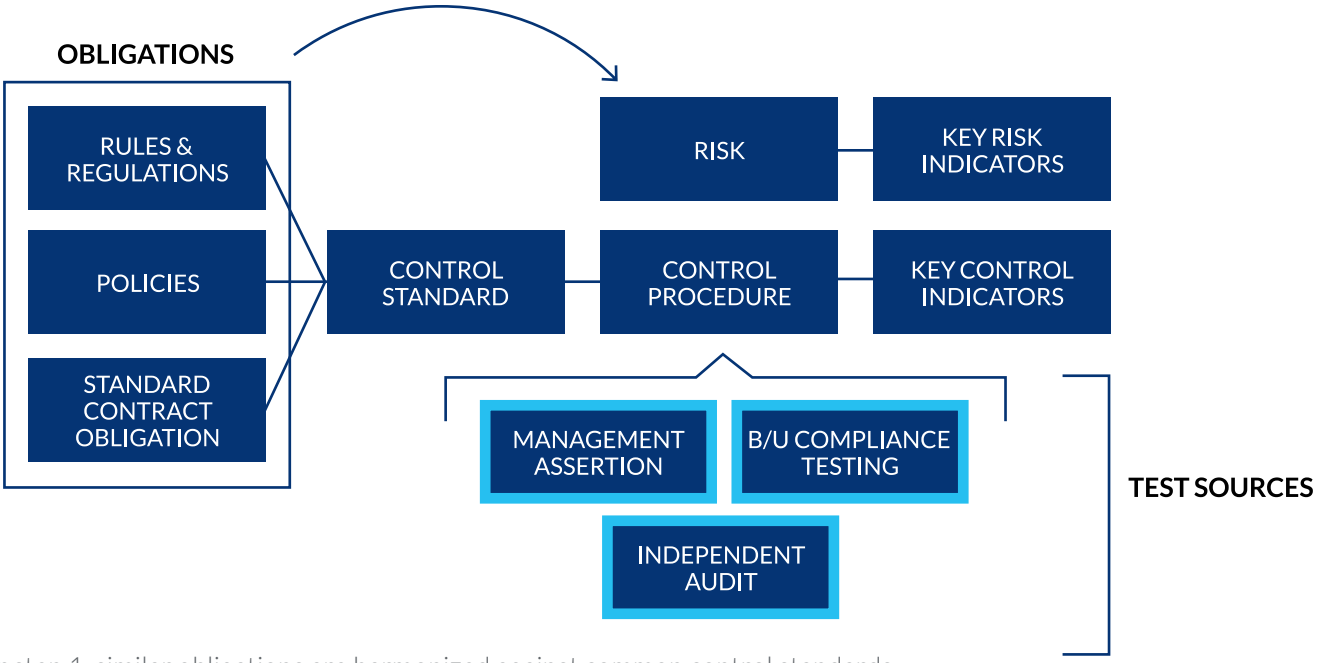


An example of a risk indicator related to an existing law or regulation might be the amount of actual fines being assessed by a regulator or industrywide litigation settlements associated with the obligation. As that cost increases, the inherent risk associated with noncompliance increases. An example of a metric associated with a control would be a count of the number of times a control failed, resulting in an internally recorded compliance violation.

For organizations focused on information security, Archer's portfolio of products can provide both controls and key indicators. (See How Archer Helps Modernize Compliance Programs, below.)

5. Streamline Compliance Testing

Testing the design and effectiveness of controls is often the most time-consuming (and therefore, most potentially time-saving) aspect of an organization's compliance program, as it usually encompasses assurance from business unit management, the compliance team and the independent audit team.



a. Per step 1, similar obligations are harmonized against common control standards, enabling the organization to satisfy testing of multiple obligations.

b. Per step 2, assessment of the risk of obligations can reveal which compliance obligations are most important, which helps prioritize where limited resources should be devoted to mitigate the risk of noncompliance. This same information can help prioritize which controls to thoroughly test based on the potential impact of noncompliance.

c. Per step 4, continuous monitoring can indicate where inherent and residual risk is increasing, including where control design and effectiveness are breaking down, to inform the choice to test related controls to make sure they are still operating as designed. In this scenario, testing is not performed at some arbitrary interval but only if and when controls appear to be deteriorating.

d. A best practice in compliance management is to avoid the same controls being tested each test cycle by three different testers. Modernized compliance programs will often rely on the results of the most recent compliance test. If management has most recently tested the control and reports it is operating, the control is deemed to be operating. However, if the compliance team or internal audit team have tested the control more recently and found it not operating, the control would be deemed not operating, regardless of what management asserted earlier. This avoids all three lines of defense testing every control, every cycle.

Testing the design and effectiveness of controls is often the most time-consuming (and therefore, most potentially timesaving) aspect of an organization's compliance program.

e. During control testing, questions often arise about test sample size, testing methodology, frequency and the role of each line of defense. Organizations with modern compliance programs can avoid this by employing "test procedure libraries," which compile proven steps to follow to test existing control procedures.

Test remediation is a final consideration. When any tester indicates a control has failed, the failure should be logged and assigned to an accountable individual, along with a commitment date for remediation. Once management asserts a control deficiency has been remediated, the independent audit team can test the assertion to validate it.

6. Manage Changes

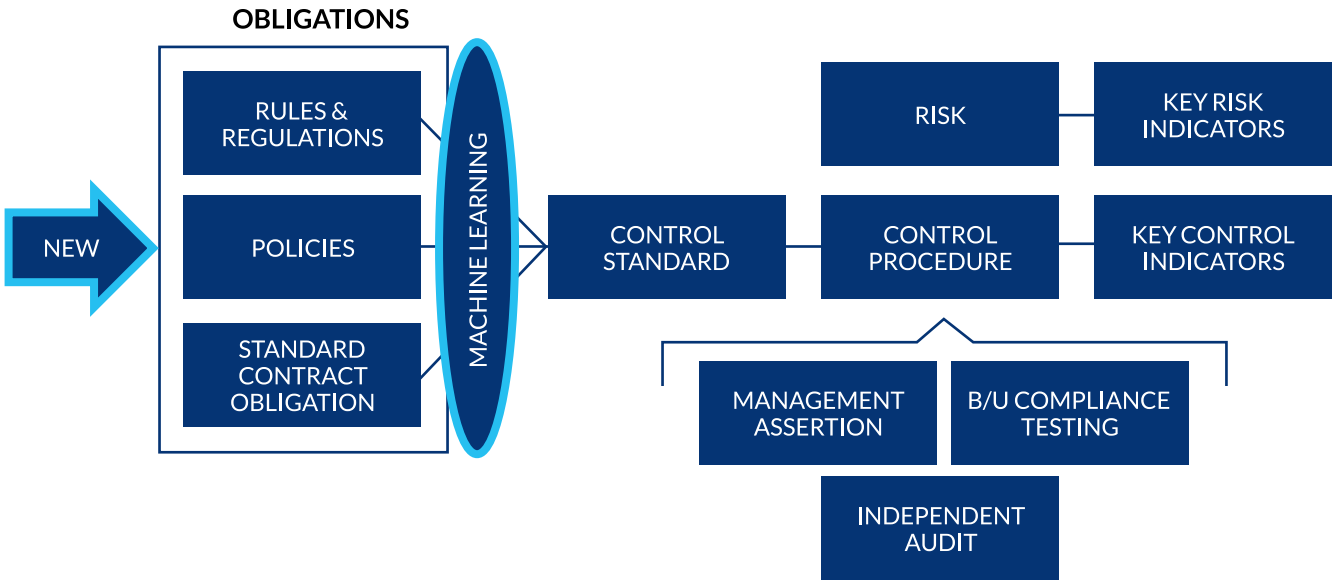
The top risk identified in a 2020 global survey of 1,063 board members and C-suite executives is the "impact of regulatory change and scrutiny on operational resilience, products and services."[7] Given this has been true in five of the last eight years this survey was conducted, it is not surprising to see organizations modernizing their approach to capturing and evaluating prospective changes. For example, one of Archer's customers, a U.S. super regional bank, requires cataloguing of all prospective, new and changing:

- Laws and regulations.
- Products and services.
- Reorganizations.
- Third parties.
- Strategic objectives.
- Business processes.
- Mergers and acquisitions.
- Geographic market changes.

These are routed to key stakeholders to provide input to manage associated risk and compliance. If a response is deemed necessary by a group, it is assigned to accountable individuals and monitored against commitment dates. This proactive approach to change management provides a best-case approach to managing new and changing compliance-related risk.

7. Apply Machine Learning

Sometimes, regulatory change can introduce a gap between an organization's existing obligations and its risks and control procedures. The traditional approach is to manually map the change to the organization's documented control standards, risks and controls, which requires too many scarce resources to be sustainable. A modern approach utilizes machine learning to do the mapping, saving time and money.



8. Manage Third-party Compliance Risk

Third parties introduce compliance risk, whether they originate with whitelabel products and services, third-party technology, contract labor or a thirdparty supply chain. While the risk may be mitigated via contract risk transfer, the organization is ultimately liable for third parties' compliance violations, and must therefore incorporate third parties within its compliance risk management program.

How Archer Helps Modernize Compliance Programs

Archer integrated risk management is well-suited to facilitate an organization's journey to modernize their compliance program. Archer® Suite addresses the eight steps to modernizing compliance described in this paper. Archer integrated risk management can also be used to demonstrate to key stakeholders and regulators how the organization fulfills various compliance obligations.

It also serves as a governance control through which all elements of an information security governance program can be documented, assessed and managed. With Archer Suite, organizations can not only govern information security but also demonstrate to stakeholders and regulators that the governance program is operating effectively.

Archer advisory services address the need to implement compliance risk management tools and practices to ensure success. Archer enables a phased approach, because maturing compliance risk management is an ongoing process. Archer helps assess current readiness to manage compliance risk by making it possible for organizations to perform a gap analysis of current compliance risk posture compared to desired levels based on industry best practices; identify types of risks to mitigate and continuously manage, as well as processes to track compliance; and develop a roadmap to move to a desired level of compliance risk.

Modernizing compliance prepares organizations to better monitor and manage changes in obligations, understand how changes impact the organization's compliance risk profile and assess whether changes are required to improve compliance risk management.

Summary

Maintaining an effective compliance program can be one of the most difficult, timeconsuming and expensive activities organizations face today and into the future. Applying modern principles and techniques allows organizations to demonstrate compliance efficiently, effectively and at a lower cost than traditional approaches allow. Modernizing compliance prepares organizations to better monitor and manage changes in obligations, understand how changes impact the organization's compliance risk profile and assess whether changes are required to improve compliance risk management.

About Archer

Archer, an RSA company, is a leader in providing integrated risk management solutions that enable customers to improve strategic decision making and operational resiliency. As true pioneers in GRC software, Archer remains solely dedicated to helping customers understand risk holistically by engaging stakeholders, leveraging a modern platform that spans key domains of risk and supports analysis driven by both business and IT impacts. The Archer customer base represents one of the largest pure risk management communities globally, with over 1,500 deployments including more than 90 of the Fortune 100.

ARCHER
An RSA Business