ARCHER

EBOOK

Guide to Modernizing Compliance in the Digital Era

Why modernize compliance?

Modernizing will prepare your organization to maintain compliance with a constantly growing, changing set of obligations:

- Statutory rules and regulations
- Industry standards
- Internal policies and procedures
- Customer contractual obligations
- Third-party contractual obligations

Follow the eight steps in this e-book to build a more efficient, effective compliance program.

A Growing Concern

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

1 Harmonize Obligations

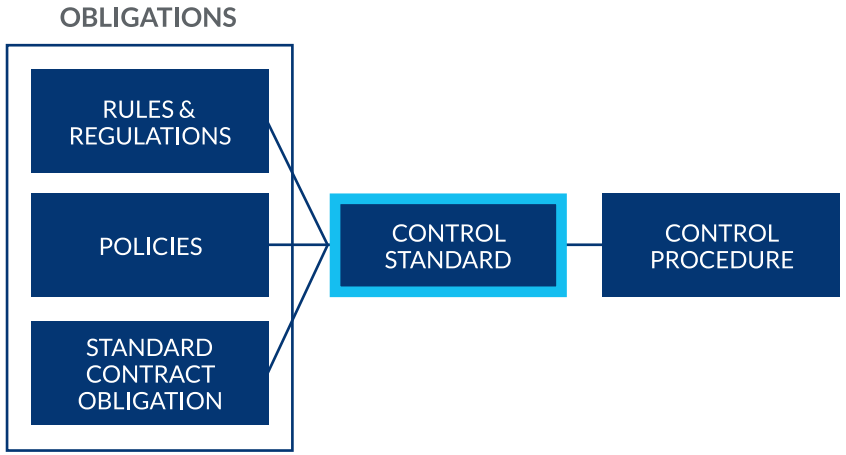
Identifying commonalities and mapping them together, instead of addressing each obligation individually, can save significant time and expense.

As compliance requirements grow, they also often overlap. Identifying commonalities and mapping them together, instead of addressing each obligation individually, can save significant time and expense.

Two Keys: Control Standards and Control Procedures

- Use control standards to harmonize similar requirements. For example, if several regulations, policies and contracts require that only authorized individuals have access to data, you would develop a control standard statement about granting access to authorized individuals and apply it to all obligations.
- Link the standard to the control procedure (or procedures) you implement to address the common requirement. In the example above, that could be a control for enforcing multifactor authentication across the organization.

Once you have control standards and related control procedures in place, you can apply the "test once, satisfy many" concept, in which you test one control (or set of controls) to demonstrate compliance with all related obligations at once.



2 Adopt Risk-Based Compliance

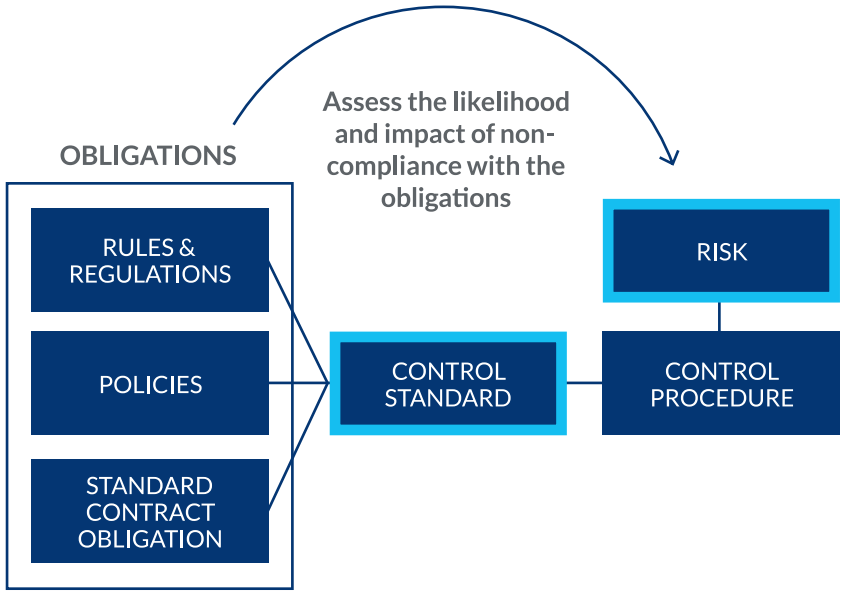
6%
Projected increase in demand for compliance officers[2]

2.3%
Unemployment rate for compliance officers[3]

Given that no organization has unlimited human and capital resources to devote to compliance, it's necessary to prioritize compliance obligations based on the relative risk they pose.

Assessing Relative Risk to Set Compliance Priorities

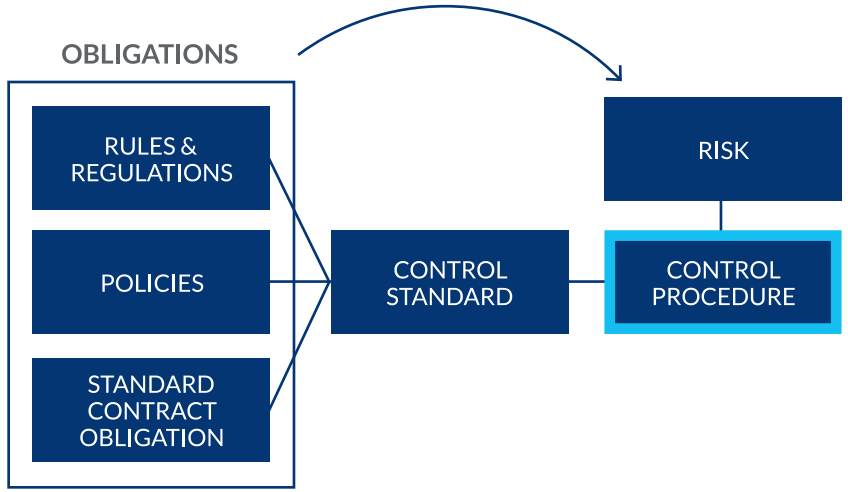
- Apply risk assessment principles to compliance to enhance compliance program effectiveness. Risk assessment methodologies will vary; the appropriate choice may depend on the maturity of your organization's risk management program and available resources.
- Choose to assess risk on an inherent basis, residual basis or both (a best practice). For example, there is an inherent risk that violating the EU General Data Protection Regulation (GDPR) could bring a multimillion-dollar fine. But taking existing risk treatments into account would likely mean lower residual risk.



3 Institute Risk-Based Controls

Once your organization has assessed its compliance risk, it's time to establish control procedures commensurate with the level of risk.

Going back to the example in step two, you could choose to establish more robust control procedures to minimize the likelihood of GDPR noncompliance than to address the prospect of a violation that has been assessed to pose less financial risk (for example, a violation of one of the terms of a business contract).



Establish control procedures commensurate with the level of compliance risk.

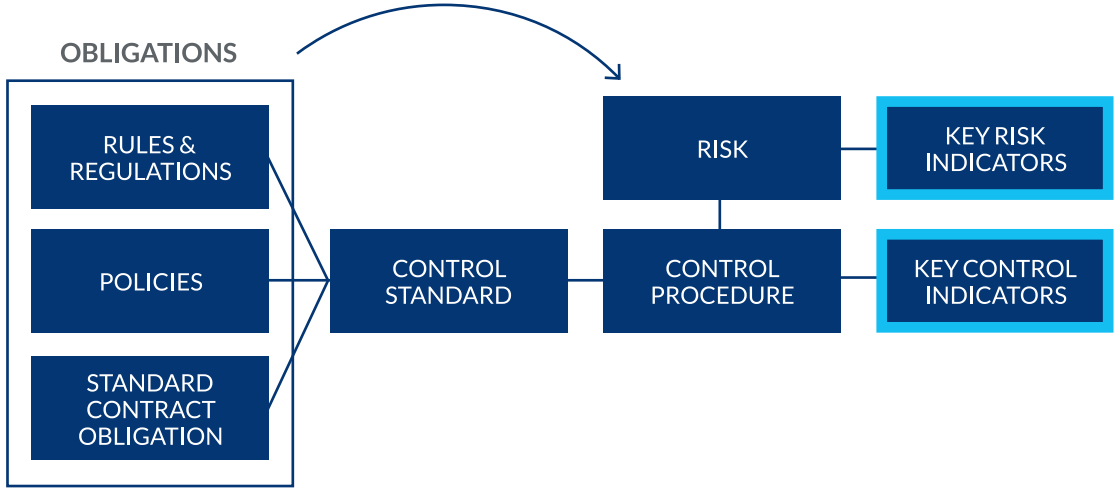
4 Establish Continuous Monitoring

Continuous monitoring refers to the process of watching metrics associated with risk, and controls that are indicators of changing risk and control procedures.

What Indicators Should You Monitor?

Optimally, indicators selected for monitoring will be leading indicators of increasing risk and deteriorating controls.

- For example, a risk indicator might be the amount of fines associated with the obligation; as the amount 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.



Optimally, indicators selected for monitoring will be leading indicators of increasing risk and deteriorating controls.

5 Streamline Compliance Testing

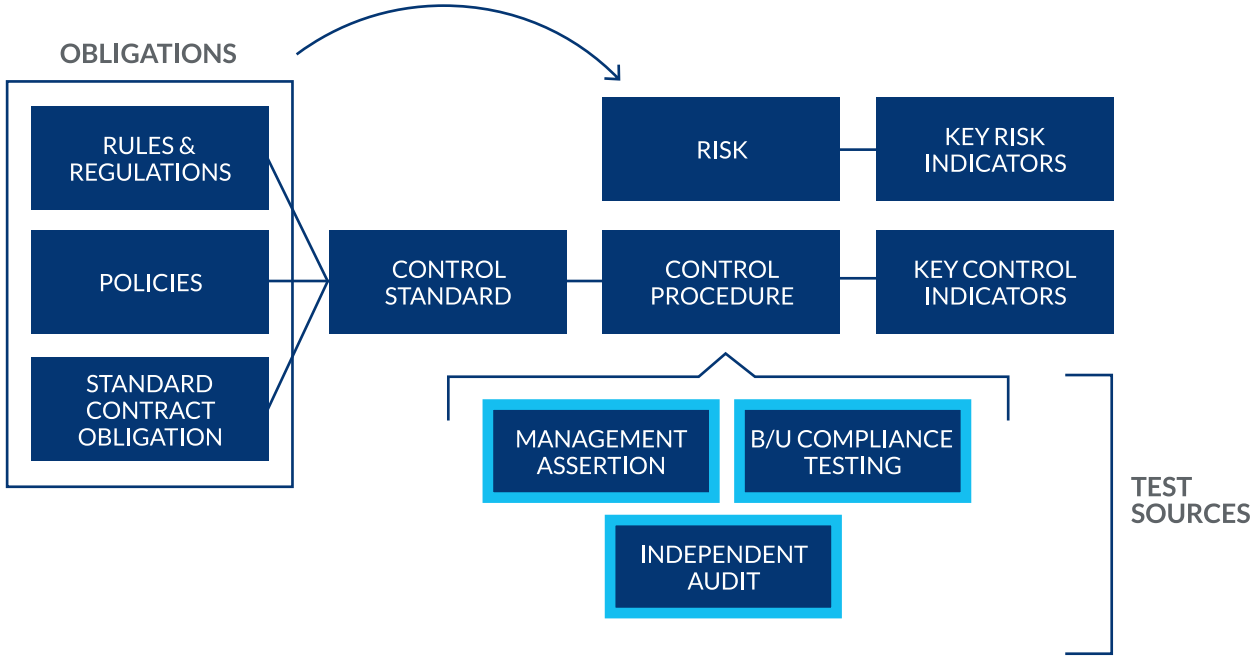
$1.9 trillion

Annual cost of federal regulation and intervention[4]

Testing the effectiveness of controls is likely the most time-consuming aspect of an organization's compliance program, and therefore the area where the most time savings can be realized.

Best Practices for Streamlining Testing

- Assess relative compliance risk to determine which controls are most important to test.
- Use the results of continuous monitoring to test based on indications of deteriorating controls.
- Avoid duplication of effort by relying on the most recent test results in a test cycle, instead of having multiple teams test the same controls.
- Reduce unnecessary complexity by using test procedure libraries of proven steps to follow to test control procedures.
- Do not test controls that are already in the process of remediation.



6 Manage Changes

One way for organizations to manage risk associated with regulations and regulatory change is by modernizing their approach to capturing and evaluating prospective change.

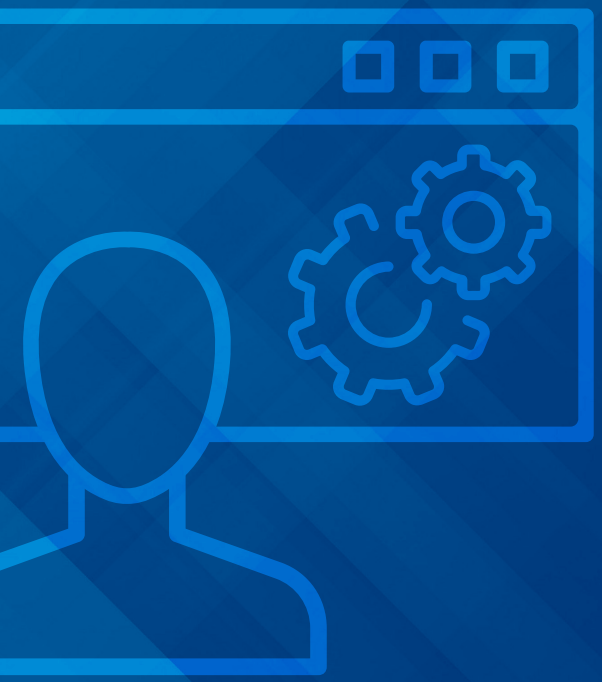
For example, one of Archer's customers, a U.S. super regional bank, requires cataloging of all prospective, new and changing:

- Laws and Regulations
- Strategic Objectives
- Products and Services
- Business Processes
- Reorganizations
- Mergers and Acquisitions
- Third Parties
- Geographic Market Changes

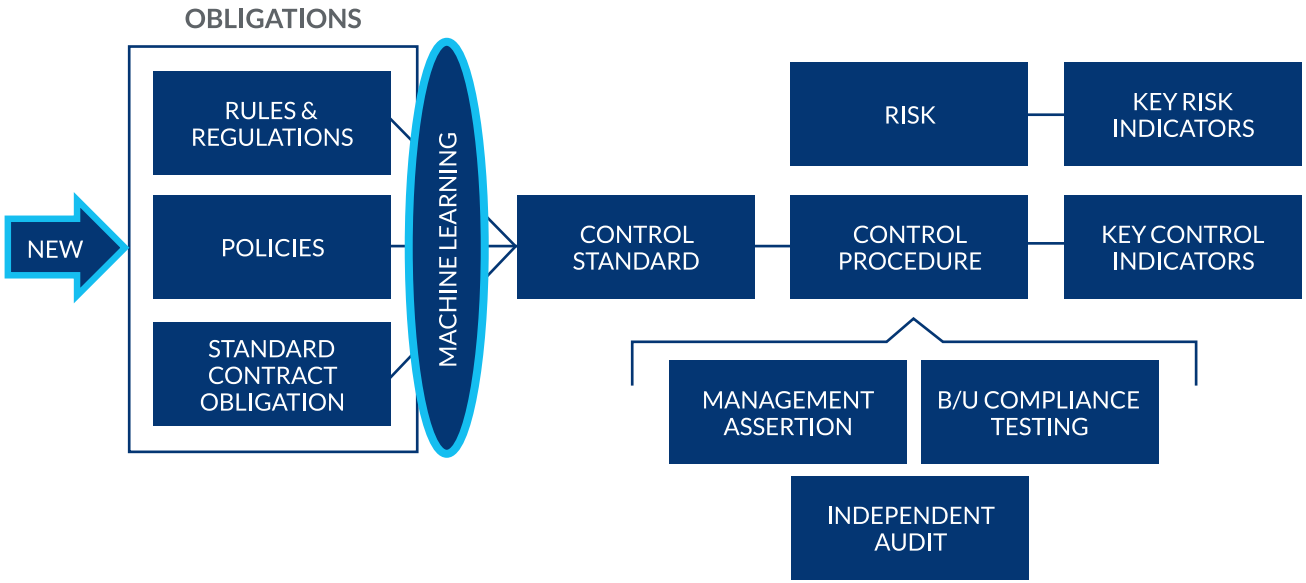
Once cataloged, these are routed to key stakeholders for evaluation. If a response is deemed necessary, it is assigned to accountable individuals and monitored through to completion. This proactive approach to change management provides a best-case approach to managing compliance-related risk.

The top risk identified in a 2020 global survey of board members and C-suite executives was the impact of regulatory change and scrutiny.[5]

7 Apply Machine Learning



The traditional approach to determining whether there is a gap between a new regulatory or policy requirement and an organization's existing compliance obligations is to manually map it to documented control standards, a time-consuming, resource-intensive process. A modern approach applies machine learning to map new and changing obligations to control standards, saving time and money.



Applying machine learning saves time while improving accuracy.

8 Manage Third-Party Compliance Risk

An ever-increasing number of an organization's activities rely on third-party relationships. If those third parties violate laws, regulations, standards, policies or contractual obligations, the organization is ultimately liable.

Incorporating Third Parties Into Compliance Risk Management

- Evaluate the compliance risk posed by a third party before formalizing the relationship.
- Determine the amount of compliance risk the third party could introduce in a worst-case scenario.
- Evaluate the design and effectiveness of the third party's internal controls.
- Monitor associated compliance risk on an ongoing basis.
- Regularly refresh evaluation of the third party's compliance controls.

If an organization's third parties violate laws, regulations, standards, policies or contractual obligations, the organization is ultimately liable.

How Archer Helps Modernize Compliance Programs

Archer integrated risk management facilitates the journey to modernize compliance, addressing all eight steps described in this e-book. It also serves as a governance control for documenting, assessing and managing information security governance and can be used to demonstrate compliance program design and effectiveness.

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.

1. Stacey English and Susannah Hammond, Cost of Compliance 2019: 10 years of regulatory change, Thomson Reuters, 2019
2. Bureau of Labor Statistics, U.S. Department of Labor, Occupational Outlook Handbook, Data for Occupations Not Covered in Detail, on the internet, visited May 1, 2020
3. Compliance Officer, Best Jobs Rankings, U.S. News & World Report, on the internet, visited May 1, 2020
4. The Cost of Regulation and Intervention, Competitive Enterprise Institute, April 19, 2018
5. Illuminating the Top Global Risks in 2020, Protiviti and NC State Poole College of Management, Enterprise Risk Management Initiative, 2020

ARCHER