MEGAPLANIT

Developing And Maintaining An Effective Compliance Program

An effective compliance program can help ensure an organization is adhering to statutory, regulatory, and contractual requirements.

www.MegaplanIT.com

Table of Contents

Developing and Maintaining an Effective Compliance Program

What does a "Compliance Program" mean to you? Some people think of policies and procedures that must be followed. Although policies, procedures, and processes are important elements, they do not encompass all of the components required to plan and implement an effective Compliance Program. Compliance programs span people, processes, and technology. **A Model Compliance Program Consists of:**

☑ **Program oversight**

☑ **Critical documentation**

☑ **Education**

☑ **Measurement processes**

What can a model compliance program do for my business? A compliance program can help ensure an organization is adhering to statutory, regulatory, and contractual requirements. It can also serve as an early warning system, by using accurate monitoring and reporting, to alert on undesirable business events such as fines, legal violations, and data breaches. When led from the top of an organization, and adopted by teammates, the program can demonstrate an organization's commitment to its values and the integrity of its business relationships.

Compliance can be frustrating or it can feel like a moving target, as new standards, technologies, and business processes emerge. Implementing controls and maintaining compliance costs money and takes time away from other business initiatives. When not properly implemented, it might provide no immediately measurable value to the leadership team. Therefore, it is no surprise that some organizations do not always find instant business value in them and may relegate compliance to an IT or Finance Department as an annual checkbox exercise and set of tasks.

Fortunately, organizations have compliance options that can reduce friction and bring additional value to a business and its relationships. This whitepaper provides organizations with a path forward. We will walk through aspects of an effective compliance program and how it can be valuable to your business. We will also outline critical steps towards developing and implementing a useful and effective Compliance Program. It is paramount to recognize that Compliance Programs should not be adopted wholly from a template or checklist; they require customization based on the organization, applicable external requirements, and industry factors.

Program Oversight

A compliance program requires leadership. Multiple domains require attention when planning, implementing, monitoring, and maintaining a program over time. Moving compliance initiatives forward involves collaboration, planning, active participation in control design and implementation, as well as independent monitoring and reporting. Compliance objectives and tasks should properly align with business goals and address compliance requirements. Organizations often leverage external support or trusted advisors, to work alongside a designated compliance officer in identifying and assembling the pieces to an effective compliance program.

It can be difficult to determine who is best suited for compliance program management within an organization. Often organizations will assign compliance program oversight to IT staff who administer systems, applications, and networks that are related to the compliance scope. This can be due to insufficient business resources or prioritization. A better, more successful approach leverages external compliance experts to support and work alongside a designated internal Compliance Officer. With the right balance of internal and external support, a business can plan, assemble, and maintain an effective compliance program.

Key areas of attention under Program Oversight include:

Establishing a Compliance Program scope, based on defined requirements and standards

Clearly defining roles and responsibilities, including adequate authority to operate the program

Providing guidance and input on controls development and implementation

Conducting periodic Risk Assessments

Monitoring of the Compliance Program's implementation and effectiveness over time

Reporting of compliance status to a Board of Directors or governance body

Ensuring Objectivity and Independence of the compliance department and function

Managing personnel and avoiding conflicts of interest

Critical Documentation

Policy, procedures, and standards are typically generated to address enterprise-wide requirements. Historically, these documents would exist in printed binders and require periodic updates, to remain current. Today, organizations use online portals and electronic data archives to distribute, track and update these core documents. While a security policy or configuration hardening template may provide a general starting point or contain examples of types of content to include, policies and standards should reflect the organization's own culture, environment, and expectations of teammates within their defined roles.

Key Areas

Documenting controls, including control narratives and mappings to corresponding compliance requirements, is not always at the forefront of one's mind.

- **Who is managing these controls on an ongoing basis?**
- **How are the narratives and mappings updated when there are changes to internal processes, organizational staffing, or technology?**

Organizations without a control inventory face an uphill battle in responding to audits and assessments, as they may rely on undocumented controls that are assigned to unknown control owners. Sometimes, a control owner may retire or become separated from the company, and the control remains non-operational until it is identified by an audit or assessment.

Key areas of attention with respect to Critical Documentation include:

Owners
Assignment of Policy and Control Owners

Requirements
Policy coverage for all applicable external (e.g., regulatory) and internal requirements

Customization
Customize the documentation to reflect the organization's business environment, technology platforms used, company culture and company values.

Conseqences
Defined consequences for non-compliance to documented policies and procedures

Distribution
Routine sharing of documentation and updates to required personnel and third parties

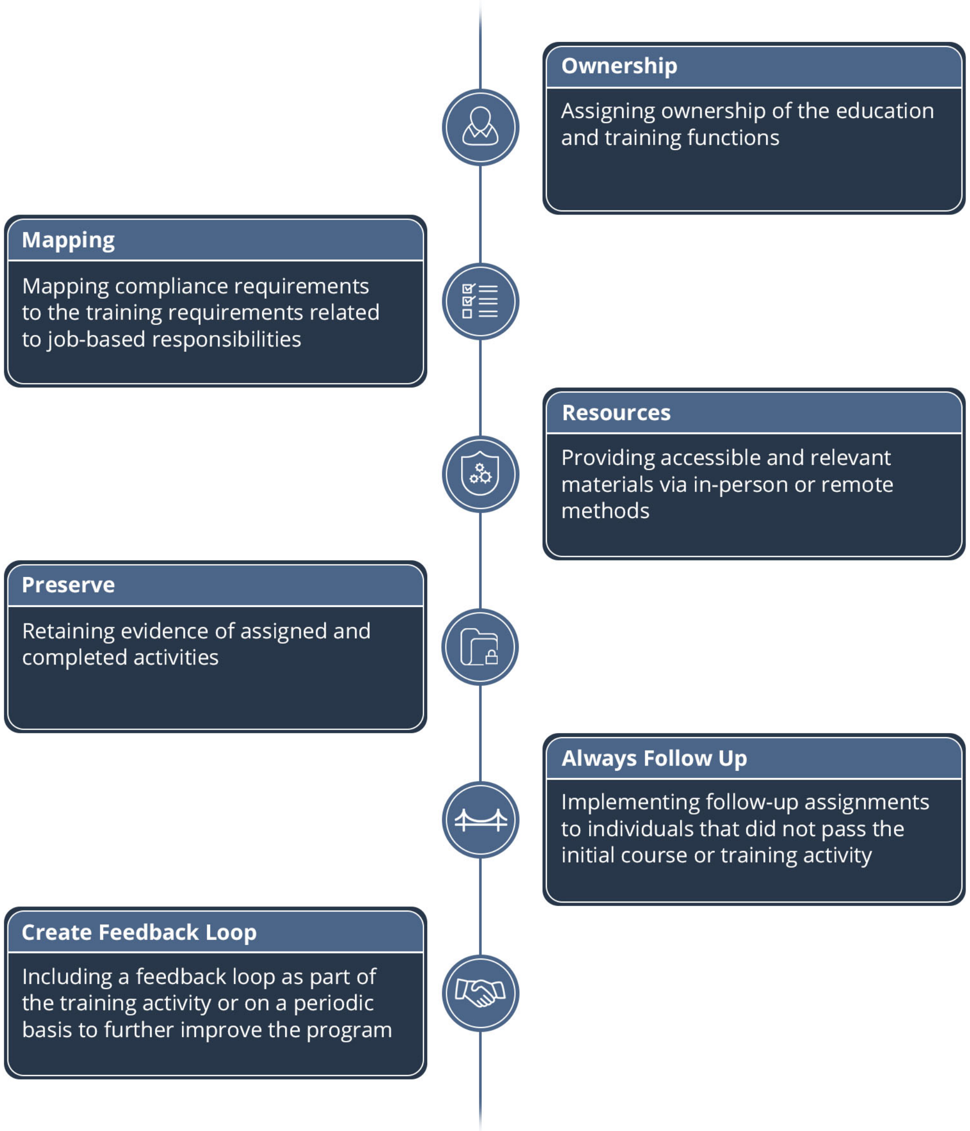
Acknowledgement
Acknowledgments by personnel, that they have received and understood the policy documents

Education

Compliance education and training has evolved over the years. Many of the in-person training in meeting rooms have migrated to online portals, offering computer-based training and interactive webinars. Education and training take time. Instead of working on active business initiatives, teammates are pausing to learn or annually refresh on key business compliance requirements and actions that can protect the interests of the organization and its customers. How much time do employees need to spend in training every year? How much phishing education and content is adequate? Is one slide deck on phishing enough? In some standards, mandatory training may only apply to a subset of personnel. For example, Secure Code training may apply to those involved in software development but not to an individual working in Accounting or Facilities.

Another factor related to education is the gamification of compliance activities. For example, periodic internal phishing tests are used by some organizations to engage more closely with teammates on an ongoing basis. Combining tests with visible results (leaderboard vs. a "wall of shame") can promote healthy competition and recognize individuals, departments, or business units for their positive performance. The engaging elements can often support knowledge retention and a higher level of participation while incentivizing people to do the right thing.

Key areas of attention with respect to Education include:



Ownership

Assigning ownership of the education and training functions

Mapping

Mapping compliance requirements to the training requirements related to job-based responsibilities

Resources

Providing accessible and relevant materials via in-person or remote methods

Preserve

Retaining evidence of assigned and completed activities

Always Follow Up

Implementing follow-up assignments to individuals that did not pass the initial course or training activity

Create Feedback Loop

Including a feedback loop as part of the training activity or on a periodic basis to further improve the program

Measurement Processes

The ongoing ability to appraise controls is the cornerstone of an effective program. Compliance Programs require accurate and useful monitoring and reporting. Understanding what needs to be measured and how to go about performing and reporting on the measurement results is an essential “feedback loop”. The output contributes to that “early warning system”, to alert on the compliance program’s overall health and effectiveness. A healthy and effective Compliance Program can more accurately oversee and report on the status of an organization’s compliance.

Key areas of measurement include:

Program Oversight

- ☑ Governance body participation in compliance oversight activities.
- ☑ Organizational structure and the Compliance Program’s Objectivity and Independence.
- ☑ Third party audits assessment results and how the output was used.
- ☑ Risk assessment results and how the output was used.
- ☑ Resource allocations to perform the required functions, roles, and responsibilities.
- ☑ Participation and engagement between compliance and leaders, departments, and teammates across the organization.

Critical Documentation

- ☑ Alignment to current compliance requirements and company culture.
- ☑ Accuracy of documented Control and Policy owners and assigned responsibilities.
- ☑ Personnel awareness of, and access to, published policies, standards, and procedures.
- ☑ Non-compliance occurrences and enforcement results.
- ☑ Periodic policy reviews.

Education

- ☑ Coverage of current compliance requirements and required topics.
- ☑ Participation and Completion Status of education activities.
- ☑ Retention of education and training completed for personnel, departments, and business units.
- ☑ Prevalence of remedial, targeted training required of personnel that did not pass knowledge tests or practical exercises (e.g., phishing simulation).
- ☑ Behavioral compliance trends over time.
- ☑ Personnel feedback (e.g., surveys) on perceived value, organizational alignment, and relevance of education and training exercises offered.

Measurement Processes Continued

Measurement activities can also contribute to greater efficiency within an organization. Are we spending too much time on certain activities or functions that could be addressed in a simpler way? Do we have duplicate controls in place that address overlapping control objectives across multiple external requirements? Do we even have the right controls in place to address the operational risks and technical threats that need to be managed on an ongoing basis? Did we buy two separate technology solutions that address the same compliance requirements? Understanding and mapping compliance requirements, controls design, and controls implementation can streamline the efforts required to address overlapping control objectives.

A compliance program should include a robust Audit Plan, with input from periodic risk assessments, 3rd party audits, penetration tests, and threat intelligence monitoring. Routine audits and assessments provide insight into the normal operation of controls within an organization. These may be performed by independent internal teams or external third parties. As part of the program's oversight, the audit results should be reviewed and the outputs incorporated into applicable remediation plans and process improvement opportunities. MegaplanIT frequently partners with organizations in conducting a variety of audits and assessments, to measure an organization's current security posture and/or adherence to specific compliance requirements.

Next Steps

Partnering With MegaplanIT

Effective Compliance Programs are attainable and manageable. They bring value and efficiency to a business environment when customized to your specific organizational needs. Development and maintenance of compliance programs are paramount to the safety and security of your assets. MegaplanIT can collaborate with your team and develop a tailored solution to your business environment for a vast array of compliance standards and security frameworks with its decades of combined security consulting experience. Our teammates are well-versed in security controls, compliance services, penetration testing, disaster recovery, as well as incident response and investigation.

For technical controls and operational security needs, we offer SIEM services. Our dedicated SOC analysts monitor your production environment 24/7 and detect as well as respond to security events, reducing your internal level of effort and need for qualified technical expertise. Maintaining a partnership with MegaplanIT will enable your business to grow safely and securely with a team of dedicated professionals to back your IT infrastructure and allow for safe and effective business processes.

Have A Question?

A MegaplanIT Expert Is Here To Help

Contact Us