Diligent

Building an Effective Common Controls Framework: A Checklist

THE IMPORTANCE OF A COMMON CONTROLS FRAMEWORK IN AN EVOLVING RISK LANDSCAPE

As cybersecurity breaches, fraud, third-party risk factors and compliance requirements intensify, it's more important than ever for organizations to maintain tight control on risk. Common controls play a big part in this.

But what exactly are common controls? The term is a broad umbrella encompassing safeguards against many types of risk: operational, **cybersecurity**, privacy, **third-party** and reputational. Two-factor authentication and validity checks are both examples of such controls.

Broader security controls extend protection to infrastructure and networks, and are often the foundation of an organization's security plan.

In today's world, an already-complicated controls environment is getting even more complex — fast. And **audit and IT teams** are spending more time and more resources just to keep up.

A common controls framework is a comprehensive set of control requirements that not only guides teams through existing compliance assessments, but also makes it easier to identify any gaps in their compliance programs.

How can your organization build a common controls framework that is efficient and cost-effective?

That's where a centralized controls management solution comes in. Such a solution leverages technology for more efficient, effective workflows and brings people, data and processes together in common controls activities.

THE RIGHT COMMON CONTROLS FRAMEWORK: A CHECKLIST

A number of technology solutions exist in the marketplace. When evaluating possibilities, the following questions and checklists can help you know what to look for, so you can focus in on the features that matter most.

Risk and Control Inventory

Wrangling controls starts with a thorough inventory of risks and evaluation of the controls you have in place for them. For example:

- [ ] What are all of the common controls across your organization?
- [ ] Which are appropriate for your organization's threat profile?
- [ ] Which need to be enhanced to meet security requirements?
- [ ] Do any of these controls do the same things?

Answers to questions like these help an organization optimize its controls in the short term.

In the long term, this data feeds into a common controls framework, which reduces the burden on risk teams by identifying issues and remedies before they cause damage.

Furthermore, with such a framework, organizations have a foundation for meeting the requirements of security, privacy and other compliance programs.

Documentation of All Internal Controls

Disparate systems and an ever-expanding controls footprint put audit teams at risk of duplicated efforts, wasted time and errors that jeopardize compliance. To maximize accuracy and efficiency while minimizing gaps, it's vital that all process owners work from a single source of truth.

When evaluating solutions, look for:

- [ ] A centralized risk and control library
- [ ] The ability to import data from other sources
- [ ] A system that aligns to all current compliance frameworks and automatically cascades relevant changes

Systems for Assessing Effectiveness

Which controls are adequate, and which need to be improved?

Common controls are only valuable to your organization if they work, and if audit teams can get a handle on deficiencies quickly, with minimal time-consuming—and costly—labor.

When evaluating solutions, look for:

- [ ] Automated workflows for testing
- [ ] The ability to pull in data from different applications across the enterprise
- [ ] A dashboard view into control status

Continuous Monitoring

Risk never sleeps. Issues often arise outside of regular office hours, from overlooked nooks of the business. To stay ahead of problems and keep executives informed, organizations need a 24/7/365 view, across the three lines of defense.

When evaluating solutions, look for:

- [ ] The ability to bring data from key business applications into a single source of truth
- [ ] A centralized platform for tracking and reporting deficiencies and issues
- [ ] A real-time assurance "report card," for quickly zeroing in on controls status

Diligent

So, you've identified a weak control. What now? Be prepared with a comprehensive, easy-to-follow plan of action.

A Rapid Reporting System

Time is of the essence when issues arise, or when changes negatively impact the protections your controls are designed to provide. To make every minute count, your controls framework needs to operate like a well-oiled machine, engaging all process owners.

When evaluating solutions, look for:

- ☐ Real-time alerts and automated workflows for quickly identifying and remediating issues
- ☐ Tracking, remediating and reporting through one centralized platform
- ☐ Easily digestible reports organized by entity, process, control status or issue

A strong controls management solution starts with boundaries. Clearly define what's protected in your organization—and what's not.

DILIGENT IT COMPLIANCE CAN HELP

Diligent IT Compliance checks all of these boxes and more. It's a centralized platform that puts controls management activities all in one place and aligns them to an organization's common controls framework, enabling deep visibility and powerful reporting.

Diligent IT Compliance offers:

- ☑ Automated workflows and processes that streamline monitoring and remediation, saving your teams time and reducing errors
- ☑ Executive dashboards that provide powerful reporting and deep visibility into your IT compliance program, enabling low-effort, data-driven decision-making
- ☑ The ability to apply a common controls framework, allowing you to build controls once, then use them to obtain multiple security certifications
- ☑ A unified platform that offers an aggregated view of your organization's IT compliance

Moreover, Diligent IT Compliance is scalable. Build controls once and use them again and again into the future.

Take the next step to more efficient, cost-effective controls management. **Schedule a demo today**.

For more information or to request a demo:

Email: info@diligent.com | Visit: diligent.com