COSMOS
Navigate the Compliance Universe

CEP Magazine - August 2020
Mitigate more risks with a change management program

By Henry Powell, MBA, CCEP, PMP

Henry Powell (hpowell@hjpowell.com) oversees training, reporting, and automation for a global financial institution in Dallas/Fort Worth, Texas, USA.

Nearly every compliance program is faced with finite resources, a wide-ranging scope, and ever-changing business and regulatory landscapes. In many companies, changes that occur—whether within the business, the compliance function, or the broader environment—are not centrally documented, uniformly analyzed, or tracked through disposition, which creates the very thing compliance is tasked with preventing: risk. Effectively managing system change is, therefore, paramount for any compliance management program. A comprehensive and effective change management program (CMP), in particular, is essential for timely identification, reporting, tracking, and remediation of compliance risk. It will also help to enhance your overall program's risk mitigation capabilities and advance its maturity.

When changes happen …

As the business and the regulatory landscapes evolve, compliance must update process documents and risk requirements, conduct additional risk assessments, and update second-line-of-defense controls (2LOD) (e.g., test procedures and reports) in tandem to ensure accurate understanding and effective governance of the overall control environment. An effective CMP lets organizations identify, communicate, and assess how a given change affects business operations, and it helps businesses determine whether they are subject to more, less, or different types of risk as a result. Once risks are known and properly assessed, appropriate first-line-of-defense controls (1LOD) and 2LOD controls can be added to prevent, detect, mitigate, and monitor these risks.

When a system management failure occurs due to a change, the control environment is weakened, rendering existing controls ineffective. When 1LOD controls become ineffective, they fail to prevent, detect, or mitigate risk; any 2LOD controls that augment, govern, or monitor the 1LOD controls become ineffective as well. When 2LOD controls become ineffective, they are either not executed or, if executed, return erroneous results (false positives or false negatives), making them unreliable tools for risk prevention/governance. 2LOD controls remain effective only so long as they accurately reflect the underlying systems, business processes, and the 1LOD controls they govern.

Compliance also uses its understanding of the business' processes and the 1LOD controls therein to establish monitoring and testing procedures for ongoing verification of control effectiveness. The more processes compliance reviews and the more controls it identifies, documents, and tests, the greater the "coverage" of compliance. When changes to business processes or 1LOD controls go undetected or unremediated, compliance coverage is reduced, because the number of processes and controls being tested and monitored are also reduced, leaving compliance unable to effectively monitor 1LOD risk mitigation in these areas. In fact, this may lead to a false sense of security, as compliance may believe it has more coverage than truly exists.

Finally, the absence of an effective CMP reduces a compliance program's maturity. Mature organizations are agile and proactive because they have access to metrics and data that allow for more informed decisions; they can understand the nature, scope, and impact of a change and the remediation options available. Ineffectively

managed system change, on the other hand, forces organizations to be reactive, making them less mature. Less mature organizations may not foresee the change nor understand its scope and impact and are, thus, unable to respond effectively.

Your CMP's policy

Companies should establish a change management policy that explains the purpose, scope, roles and responsibilities, end-to-end process, reporting requirements, training requirements, and the host of other elements necessary for a successful program. Many organizations may have some form of change management in place already, and your policy must provide guidance on how compliance requirements will inform, interact with, or alter these programs. One thing to avoid is introducing additional bureaucracy that impedes the business' ability to respond to change—this will be critical to buy-in and adoption.

Your policy should include a Purpose section that outlines why the policy exists, program goals, employee expectations, and benefits to the organization. The scope of the program should be defined in terms of geography, business units, and departments/functions. Small programs may be driven by compliance and limited to a single region, whereas large programs may be global and span the entire enterprise. Scope should also address how this policy interacts with, informs, or modifies other change management programs that may exist within the company. For example, this policy may require other change management programs, such as information technology change management, to notify compliance of approved changes exceeding certain thresholds (impacted users, dollar limits, number of processes or systems, etc.), or it may require compliance's approval in certain cases.

The policy owners should be defined, ideally by name and title, with contact information if possible. Roles and responsibilities must be defined and should include, at minimum, roles for the policy owner, program manager, and change owner. The actual number of roles and the corresponding responsibilities will depend on the size and scope of the program; examples of other possible roles include change coordinator, change review board, change identifier/requestor, and approver. Including a high-level, end-to-end process diagram that describes the interactions between actors and the process triggers, inputs, and outputs is also recommended, as it will aid in the understanding, implementation, and adoption of the policy.

Additionally, training requirements will facilitate common understanding of policy requirements and aid in adoption and execution. Training, at a minimum, should address the end-to-end process and roles and responsibilities. Reporting requirements should focus on monitoring compliance with the program and the program's effectiveness. Finally, the policy should include requirements for program governance, such as periodic policy reviews and revisions, routine updates of its effectiveness to the policy owners, opportunities for improvement and maturity, staffing and budget needs, etc.

A change management system is also key

A centralized change management system (CMS) is a principal component of an effective, scalable change management program. It serves as the intake mechanism for identified and proposed changes. The entry of a change into the CMS triggers a process (or processes) by which key stakeholders evaluate the change (its impact, scope, timing, etc.) and then determine and implement the required remediation. When integrated with other systems, the CMS can link/map changes to other objects, such as authoritative sources, controls, business processes, business units, issues, etc., as appropriate. And predefined workflows and checklists within the CMS can be created to support different categories or types of changes (e.g., regulatory, business process, organizational, product enhancements).