
Control Design

During our client work over the past year, we have noticed a trend that has caused some concern. We are seeing great focus and testing being done around the operating effectiveness of controls, but not as much focus on design testing. While ensuring the controls established by management are operating effectively is an essential part of the risk management process, focusing on the design of those controls is as important, if not more important. If a control is not well written and designed to mitigate the identified risk, it could be useless even in a situation where it is operating effectively. Let's take a real world example related to user access reviews:

Risk – Users' access rights are inappropriate based on job responsibilities leading to data being misused or modified both intentionally and unintentionally.

Control in Place – On an annual basis, users' access to all key systems will be reviewed by managers to ensure access is appropriate.

On the surface, this control seems to be properly designed to mitigate the risk of inappropriate access to key systems. Let's add more context to the situation:

Additional Fact – 85% of the users of key systems are in a rotational program where they switch departments and business units on a quarterly basis to gain exposure to different areas of the company.

This fact changes the situation of our control being designed to mitigate the risk. If these users are changing departments that frequently, their access to key systems most likely needs to be changed as well. In our experience, even the best change management, provisioning and deprovisioning programs miss items from time to time. Having the proper mitigating controls in place is what helps reduce the risk in these situations to an acceptable level. With the additional facts, our control design should be changed to read as follows:

New Control Verbiage – On a quarterly basis, users' access to all key systems will be reviewed by managers to ensure access is appropriate.

The example above is a simple one, but it does a great job of demonstrating the importance of designing controls properly. Proper process walkthroughs should be performed to gain an understanding of how the business operates, what the risks really are and what controls need to be in place to mitigate those risks. Once you have your controls designed properly, you can move on to testing the operating effectiveness of them, but do not let the design phase slip through the cracks. In a world where the risk landscape is growing and evolving every second, companies will be happy they thought through these issues in the right way.

At The Mako Group, we can assist you with designing controls that address your risks. We can also review your current controls to evaluate if they are properly meeting your needs. We are here to help and be your trusted partner.

Shane M. O'Donnell, CISA, CPA, MSA
Chief Audit Executive
March 2014