Phillip Thoendel – **The Dangers of Change Approval Processes – Mod 8.2**

This week I will be discussing change approval processes and, more specifically, potential pitfalls when implementing these processes. The purpose of change approval processes is to control and manage changes made to an organization’s IT infrastructure. Change control/approval processes are a critical aspect of maintaining the security and functionality of an organization’s IT assets. In a world of constantly changing technologies and unintended consequences, special care should be taken to ensure all IT processes being changed are well organized, scrutinized, approved and carefully implemented. Failure to do **any** of these things can result in catastrophic consequences including but not limited to, data loss, data/identity theft, failure of organization-critical servers or loss of revenue and probably someone’s job.

Here is an outline of several best practices, with the help of my sources. (see sources at the bottom of the page).

1. **Submit Change Request**

* The first step in the process is to identify the need for a change and submit a thorough request explaining the need for this change as well as any resources they will require to implement this change. Also, the person submitting the request should have an understanding of the potential impacts this change may have.

1. **Create Change Advisory Board – Assess Change Request**

* A team of technical experts should be assembled to review change requests and analyze the validity and feasibility of the request. This acts as a “first pass”. Basically, you want to weed out any potentially frivolous changes.

1. **Deep Dive Risk Assessment**

* At this point the change advisory board will closely examine any potential risks in implementing this change. What other processes could this interfere with? Are we introducing a new security risk? What are the financial costs associated with this change? What staff will be involved with implementation? These are the kinds of questions the Change Advisory Board should have in mind when further analyzing a change request.

1. **Implementation**

* Once it has been determined that the change can occur with minimal risk the change can be implemented. Attempts should be made to have a “soft implementation” in a sandbox environment. Protocols should be established for the planning, preparation, back-up and disaster recovery aspects of the implementation before the implementation itself occurs.

1. **Verification**

* Following the implementation of the change there will be follow up that occurs ensuring that the implementation went smoothly and there were no unintended consequences. If there are any consequences, a quick assessment should be made based on the severity of the consequences to determine if it is something that can be fixed/patched easily or, in more severe cases, does the change need to be reversed?

In conclusion, implementing changes to an organization's IT infrastructure is a very high-risk venture. But, not implementing changes to keep up with modern technology standards creates a ticking time bomb of technical debt. It is better to expect changes and have experienced technical experts in your organization, to assess and mitigate the risks.

**Sources**

<https://dora.dev/capabilities/streamlining-change-approval/>

<https://changemanagementinsight.com/change-approval-process-in-itil-change-management/>

<https://www.prosci.com/blog/avoid-these-change-management-obstacles?utm_term=&utm_campaign=SEARCH+DSA+-+Blog+-+TOFU+-+US&utm_source=google&utm_medium=cpc&hsa_acc=5529787200&hsa_cam=11452601506&hsa_grp=108788490901&hsa_ad=475020570218&hsa_src=g&hsa_tgt=dsa-1460075494969&hsa_kw=&hsa_mt=&hsa_net=adwords&hsa_ver=3&gad_source=1&gclid=EAIaIQobChMInNKCnPCIhwMV8UpvBB281gEXEAMYASAAEgJdx_D_BwE>

<https://www.atlassian.com/itsm/change-management>