Getting Started
25 Key Requirements of a Change Management Solution

Presented By:

SunView Software Inc.

Getting Started:

25 Key Requirements of a Change Management Solution

Our goal is to take you through twenty-five of the most important criteria that a Change Management solution should include.

Finding a Change Management Solution

Behind every successful IT project are two key criteria that create success, and inversely, determine the potential for failure. Essentially, when processes and tools come together, they can either make magic, or leave bitter regrets for an IT organization. We want to put you on the path to the former, and in this guide will show you how to select the right tool that will blend with your team's processes.

Of course, always remember having both good processes and an incredible tool is a requirement as well. No tool can fill a gap where processes are absent or lacking. To the same affect, if processes are paired with a tool that works against you, you will find yourself writing yourself around those limitations. Once that happens, organizations tend to shift more to reaction than prevention. Unfortunately, managing change like this also works against best practice recommendations such as those found in ITIL. That said though, what other criteria should a solution have?

Well, that's where this Getting Started guide will help. Our goal is to take you through twenty-five of the most important criteria that a Change Management solution should include.

How to Use This Guide

- Read through the list of twenty-five key requirements.
- Starting with a score of 100, subtract 4 points for each requirement you are missing.

Threat Level	Score	Description
Warning	92-99	Your solution is incomplete.
Elevated	80-91	Your solution lacks major functionality.
Imminent	< 80	Your solution prevents visibility to your IT infrastructure.

Getting Started:

25 Key Requirements of a Change Management Solution

25 Key Requirements

A Change Management Solution Should…

1. Use ITIL terms and definitions, making sure that workflows and processes are based on ITIL best practices.

2. Allow users to be differentiated based on license and role, including a range of customizable access from requestors (customers) to IT Staff.

3. Provide a mechanism for requiring specific fields.

4. Report details down to the record detail including items such as: total number of Changes over any given period, status (active/closed), by category, or Configuration Item.

5. Provide a wide range of reports out-of-the-box, as well as, options for creation, design, and customization of reports based on any field. In addition, there should be an ability to create specific reports for management.

6. Record an audit log of all Change updates and resolution notes. Be sure it also attaches the account that made the change. Finally, very advanced systems will have an ability to record both the previous and current contents of any fields that have been changed.

7. Allow users to manually escalate Requests for Change (RFCs) with the ability to create and modify automatic notification rules, or create Business Policy Automations (BPAs) to escalate an RFC or to notify recipients based on other criteria.

8. Generate unique IDs per RFC.

9. Automatically apply date and time stamps to any new or updated change records, as well as when

any subsequent actions performed on the RFC in the History tab.

10. Record the date and time when an RFC is closed, and record it to a reportable, historical record.

11. Support an administrator's ability to create BPAs and automated reports to monitor and track RFCs.

12. Provide easily accessible options for workflows based on the type and/or necessity of a change selected.

13. Allow the designation of approvers, such that only users who have the privilege to approve can be selected. In addition there should be an option for the creation of approval groups which contain all the approvers necessary for a specific change type or for specific criteria.

14. Present easily accessible and identifiable rejection options for those users with the corresponding privilege.

15. Enable administrators to assign CAB members to different roles within the solution. Taking that a step further, the solution should also allow administrators to add all CAB members to a role, if all members need the same privileges, or to various security teams if there need to be specific CAB member roles within the team.

16. Extend functionality to administrators allowing them to configure BPAs that will automatically change the priority based on impact and urgency.

17. Allow users to view the status of the approval process in an easily accessible and intuitive area within the application. In addition, approvals should be recorded for historical purposes.

18. Provide a mechanism that allows users to easily add impacted resources, users, and business services to RFCs. Furthermore, administrative staff should also have the ability to create new fields and modify the form to more fully articulate assessment needs.

19. Include a centralized location for users to view scheduled changes and outages. Of course, options for administrators to modify role privileges such that, only the Change Manager can create announcements, is necessary as well.

20. Ensure the necessity and indicate when applicable any rollback plan, and in turn, attach the rollback plan to the RFC.

21. Prompt users to provide comments when an RFC is submitted for validation or when an RFC is validated.

22. Allow users to link Incident Reports to RFCs.

23. Enable users to easily add business services and impacted resources to an RFC.

24. Integrate seamlessly with a CMDB module.

25. Record and track release and deployment activities. Additionally, administrators should have access to a tool that utilizes different processes for each RFC.