25 Point Change Management Process Checklist	√	×
1. Clarify what Change Management will accomplish in the enterprise. Change Management focuses on the oversight and approval aspects of the process, ensuring that only authorized changes are being worked on. It is more related to business impact than to IT operations. The ITIL definition of Change Management is that it is a process of controlling changes to the infrastructure or any aspect of services, in a controlled manner, enabling approved changes with minimum disruption.		
2. Define what a Change is. All Installs, Moves, Adds, Changes and Decommission (IMACD's) of the infrastructure. Software and hardware changes should fall under the control of Change Management. Even the most seemingly innocuous changes can cause major disruptions and outages if they are done under the radar. This is often the case when implementing Change Management in an immature, silo-structured enterprise.		
3. Make all levels of the enterprise aware of the benefits of Change Management. Stakeholders need to understand the benefits on an individual and at team level. Clearly defining and presenting to each stakeholder what those benefits will be, and conversely, establishing and enforcing policies that address the penalties and repercussions for bypassing the process is essential.		
4. Establish clear roles and responsibilities for the Change Advisory Board (CAB) and Change Manager. An effective and successful Change Manager is one who proactively ensures that the right resources, both technical and business, attend the CAB and present viable, justifiable changes. The Change Manager can be the final arbiter in resolving disputes over classifications and prioritisations. In extremes, this can be escalated to executive level. Attendees at the CAB who are representing changes should be well-informed and can speak to their items when challenged. Their role is to present the change justification, the impact analysis, the resource plan and execution plan for each change.		
5. The CAB should not be the exclusive domain of IT. A successful CAB will have a wide rotating mix of attendees from the IT and the business.		
6. Establish and stabilize the Change Management process before introducing tools. Ask not what you can do for the tool, but what the tool can do for you?		
7. Define Key Performance Indicators (KPIs) and Critical Success Factors (CSFs). KPI's: Reduction of unauthorized changes. Reduction in change related outages. Reduction in emergency changes. Actual cost of a change vs. budgeted cost. CSFs: A repeatable process that can make changes quickly and accurately. Protecting the integrity of the		

service when making those changes. Delivering process efficiency and effectiveness.		
8. Ensure back-out plans are documented and realistic. These should be tested and timing should be understood. Impact analysis is crucial to the back-out plan.		
9. Highlight the positive by building on successes and leveraging lessons learnt. Distribute success stories and integrate lessons learned into plans for future roll-outs.		
10. Use the Change Management initiative to promote other ITIL processes. When Release and Configuration Management processes are absent, consider combining all three into a centralized function. The three processes have many close links to each other and together can stabilize an enterprise's production environment.		
11. Create standardized processes and time frames to support Change Management. Have senior members of CAB sign off on the criteria to reduce the noise level. Define the boundaries around priorities and have them implemented. Apply consistently. Standard change processes will result in fewer circumventions of the system and greater efficiency and effectiveness.		

12. Change request types

Change Request	Description	Authorised by	Example
Standard	Common, accepted procedure	Pre-approved	Resetting passwords, adding a security patch to a server
Minor	Low impact, small amount of resources needed	Senior team members, Managers	Fixing a minor bug in an application
Significant	Possible adverse impact, some risk, more resources needed to implement	Managers	Installing a new software application requested by Business Users
Major	Risk of change adversely affecting users or infrastructure, major effort required to build and implement	Business Unit heads	Replacement of a production server running applications
Emergency	Significant impact if not implemented immediately, requires quick decision making	Team leader	A core router is malfunctioning and must be replaced

13. Request for change: Change requester initiates process and role players in change identified, Standards and quality criteria established for the raising of changes.

14. Change evaluation and assessment process: All upgrades or growth procedures should be fully validated in the lab environment prior to first application in the field, where possible. Collect all data necessary for further evaluation of RFC, develop Deployment Plan, Deployment Manager initiates process for testing change.

15. Configuration Management Database: Extend CMDB by new Configuration Items (CI) & relations that are inherent to the new

change, defines relevant CIs and their relation to other CIs (logical and physical interdependencies).		
16. Impact and risk assessment: Assessment of impact and risk on technical level, assessment of Impact and risk on business level.		
17. Change Advisory Board (CAB): Functions & purpose of change management has been communicated within the enterprise, Approval of change, conduct final assessment of requested change and issue approval/denial/deferral		
18. Installation in testing: Pre-installation Meeting, performs installation as described in Deployment Plan, attend and support the installation. Decide back-out plan/s and scenarios.		
19. Test installation review: Review installation of testing, feedback on testing installation, formal declaration of testing phase. Test back-out plan.		
20. Testing in progress: Conduct a pre-defined set of basic integration tests (as defined by Deployment Management), conduct functional test, and conduct user acceptance testing. Prevention of interference with existing live systems.		
21. Operational acceptance phase: Acceptance testing checklist and operations readiness signoff, service integrated into existing productive environment, review test results.		
22. Ready for live: Verify all tests completed, Service Desk informed and trained, operational support teams trained to support, Business Unit users informed, Formal declaration of live service. Integration with Service Desk: Integration with incident management, Integration with problem management.		
23. Implementation in live environment: Implementation performed as described in deployment plan, support and supervision of implementation.		
24. Go live acceptance: Successful integration in live environment, review back-out strategies, Quality Assurance, review implementation.		
25. Live: Services provided to Business Unit user, SLA measured and achieved.		