ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 9, Issue 3, pp: (48-50), Month: July - September 2021, Available at: www.researchpublish.com

Change Management Controls on Information Technology (IT) Systems

[1]Lamia T. AlSulaiman, [2]Khalid A. Al-Khathlan, [3]Jumana F. Alturairi

Dhahran, The Kingdom of Saudi Arabia

Abstract: **In most business environments, any business function is supported by several IT systems. Availability is the key metrics that demonstrates the overall performance of IT services. However, IT systems may encounter multiple outages/interruptions due to planned changes. As IT Change management (ITCM) is the highest authority responsible for controlling the lifecycle of all changes through standardized procedures for computing, network and application changes; enforcing controls on scheduled changes are significant in order to protect IT infrastructure.**

This article describes IT Change Management controls on IT systems changes, which aims to manage and implement changes on IT infrastructure in a way that minimizes risk and reduces corporate-wide impact.

Keyword: **Information Technology, IT Change Management, Controls, IT Systems, Critical Systems, Change Requests.**

I. INTRODUCTION

Information Technology systems may encounter outages due to systems changes such as installations, decommissioning, upgrade and fixes in the network, computing, applications, databases and facility environments. IT Change Management role is to enforce the required controls prior to implement any change in order to eliminate an unanticipated systems interruption and ensure the continuation of IT services availability. Moreover, systems outages are recorded through multiple processes such as change management, incident management and problem management. Therefore, engagement across IT organizations is required in order to define the required controls for each system.

This document covers Change Management controls on IT systems changes, which comprehensively highlight IT critical systems criteria along with the essential systems controls.

II. CHANGE MANAGEMENT CONTROLS

A. IT Critical Systems Criteria

As a first step, IT systems should be categorized based on selected criteria such as number/type of users, hosted services/applications, systems tiering and business criticality. Below are the criteria table:

TABLE I: IT Critical Systems Criteria

Criticality Classifications	Classification Criteria
Very High	Systems hosting corporate-wide services
High	Systems serving critical users and high management
Moderate	Systems hosting services for multiple groups of directly connected end-users.
Low	Systems hosting services for specific users

B. IT Systems Controls Samples

The following sample of controls applied for IT systems changes:

- All changes should be freeze during major high-profile events
- Submitting change requests should be ahead of time (i.e. Minimum 3 business days prior to the implementation)
- Approved Cybersecurity checklist is required for changes related to new commissioned systems or applications as well as major enhancements on the Intranet and Extranet zones
- Change Requests (CRs) should be coordinated/communicated with concerned entities across IT
- Secure proponent approval for service affecting changes targeting 24X7 users
- Relate targeted devices/systems from repository systems (i.e. Configuration Management Database "CMDB")
- Obtain task implementer group approval

C. *IT Critical Systems Samples*

Due to the high impact of the identified critical systems (very high and high), additional controls must be applied in order to mitigate the risk of causing wide outages by misconfiguring (either intentionally or unintentionally) a critical IT supported service.

The following sample of controls applied for IT critical systems changes:

- Assign one person to review the change and a different person to execute
- Assign a task to perform health check after the implementation in order to ensure service availability
- Perform extensive testing before deployment
- Follow phased approach deployment as applicable
- Changes should be implemented gradually starting with the least critical system/service
- Obtain critical service/system owner approval
- Assign task for critical service/system owner as applicable
- Schedule changes to be implemented after prime time (least utilization time)
- List the hosted services/users
- Send notification email to the impacted proponent/users

D. Specific IT Systems Controls

Along with the abovementioned controls that covers IT critical systems, additional controls may apply for specific systems as follow:

Mobility Devices Update Controls

In many organizations, mobility services are mandatory for day-to-day operation. However, mobile version update is required for some cases in order to avoid threats and hacking to IT systems. Thus, blocking mobility services is essential with the following steps:

- For zero-day vulnerability that require immediate action, the blocking should be implemented through emergency change request
- For other severity vulnerability changes, multiple CRs should be submitted for the blocking action with the following conditions:
  - Schedule CRs during weekdays only

- Post disconnection notifications sent to users highlighting the required action to regain the access, type of device and disconnect devices date
- Post disconnection notifications sent to users by SMS

Workstations Changes Controls

- Workstations CR should follow phased approach strategy:
- Pilot phase: Target 50 % of IT organizations + non-IT selected users
- Phase 1: 5%
- Phase 2: 20%
- Phase 3: 40%
- Phase 4: Remaining workstations to reach the 100%
- Send notification email (pop-up message or through email)
- No impact changes should be scheduled after working hours only and service affecting should be during the dedicated maintenance window
- Enforce snooze alert message for at least 6 hours prior to the reboot

Computing Servers Controls

Computing server's deployment should follow phase approach strategy:

- Phase 1: Quality Assurance servers
- Phase 2: Backup systems
- Phase 3: Tier-2 and Tier-3 servers
- Phase 4: Tier-1 servers

III. CONCLUSION

Change management controls are the key elements for success implementation of changes, which will be led to eliminating IT systems massive outages along with ensuring services availability especially for critical systems changes.

REFERENCES

[1] Information Technology Infrastructure Library® (ITIL) Foundation

[2] ITIL® Release, Control and Validation (RCV)