ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 10, Issue 3, pp: (81-85), Month: July - September 2022, Available at: www.researchpublish.com

An Approach to Control Information Technology Changes

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

Dhahran, The Kingdom of Saudi Arabia

DOI: https://doi.org/10.5281/zenodo.7092060

Published Date: 19-September-2022

Abstract: **Information Technology (IT) services plays a significant role to preform day-to-day operations in all organizations. Any unexpected outages in IT services may cause major financial loss due to business disruption. However, there are mandatory alterations executed frequently in IT infrastructure due to introducing, enhancing, modifying, replacing, or removing assets/services. Controlling the lifecycle of all alterations in the IT infrastructure is the responsibility of IT Change Management (ITCM). This is essential to ensure the security, availability, and reliability of the IT Infrastructure by eliminating the disruption of business and maximize IT services readiness towards customer satisfaction. This paper describes the process of storing, tracking, preventing and detecting configuration changes implemented in the IT infrastructure as part of IT change management process and in alignment with security standards and policies.**

Keywords: **Information Technology, IT Change Management, Infrastructure, Controls, Configuration, Tracking.**

I. INTRODUCTION

As information technology (IT) services are essential for all business operations, the ability to control the changes implemented in the IT infrastructure is significant in order to maintain the IT availability, reliability and security. The most important key to have a secure and well-defined structure is to have a mechanism to maintain a record and trace all changes implemented in the IT infrastructure despite the change type wither its authorized or unauthorized. Several issues encountered without having a tool to detect/ trace IT changes, which might exploit a vulnerability to breach security and thus cause huge impact such as system failure, higher cost, business impact, security threats, undocumented changes and loss of revenue. This paper intends to provide the process of IT change management configuration controls for storing, tracking, and detecting changes implementing in the IT infrastructure along with preventing unauthorized changes. The paper is organized into multiple sections as follows: IT change management controls process, configuration controls tools evaluation and lastly, the performance and validation process which covers testing procedure, Key Performance Indicator (KPI) and compliance.

II. CHANGE MANAGEMENT CONTROLS PROCESS

IT change management (ITCM) controls process demonstrates an end to end solution of storing, tracking, detecting and preventing changes in the IT infrastructure. There are multiple solutions and tools to control changes on IT systems such as Privileged Account Management (PAM) and configuration changes tracking tools as follow;

A. Privileged Account Management (PAM)

Privileged access management (PAM) is a technology used to control, protect and monitor access to an organization's information. PAM subclasses consist of shared access password management, privileged session management, vendor privileged access management (VPAM) and application access management.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 10, Issue 3, pp: (81-85), Month: July - September 2022, Available at: www.researchpublish.com

PAM system implementation will effectively help organizations to monitor the entire infrastructure and provides insight into users access what data as it's considered one of the best ways to protect organizations against external threats by preventing unauthorized activities and controlling/managing the access of sensitive corporate data through internal accounts.

Privileged user accounts have special access to confidential information, elevated permissions which make it a significant target for attacks.

The privileged session account control mandates a valid change request to activate IT admin accounts within the approved time frame, taking into consideration admin users who are required to perform daily operations or health checks that doesn't alter any component within IT infrastructure.

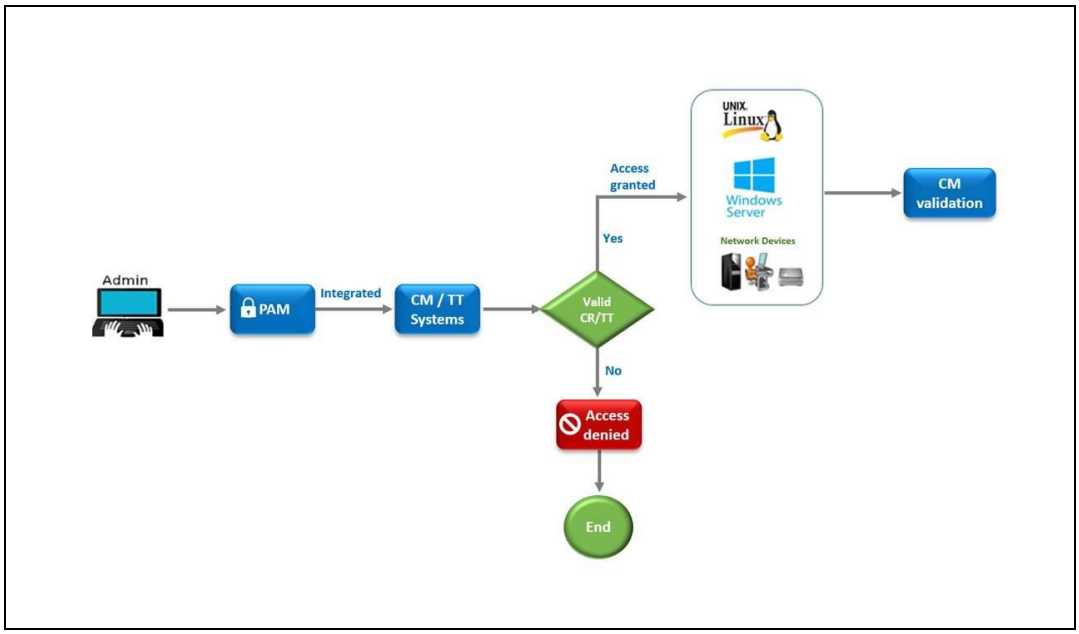

Figure 1: Privileged Account and Session Management Process

Figure 1 describes the privileged account and session management process to prevent unauthorized access to IT systems. This proactive control minimizes unauthorized change activities on the IT Infrastructure and eliminate unplanned interruption to the business as follow;

1. Admin user will select the type of account to be activated based on the environment (Windows, Linux or Communication).

2. Admin user will select the reason for activating the account:

2.1 Change Request (CR)/Trouble Ticket (TT): This option will mandate entering change request or trouble ticket number to automatically check the validity of the entered requests with the following conditions:

a. Valid task in an authorized change request is assigned to the requester or,

b. Valid trouble ticket is assigned to the requester.

2.2 Monitoring & Health Check: This option is utilized for daily operation such as systems monitoring and health check where the requester will not alter any component within IT infrastructure. Justification is mandated for this option.

3. Admin account will be activated if above requirements are fulfilled. Otherwise, account will not be activated and error message will be displayed accordingly.

4. Change management (CM) will perform a periodical review on enabled accounts to verify if all activated accounts where utilized in an authorized manner as part of the quality assurance process.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 10, Issue 3, pp: (81-85), Month: July - September 2022, Available at: www.researchpublish.com

B. Configuration Changes Tracking Tool

The best approach to automate detecting changes is through configuration changes tracking tools. The main functions of these tools are to trace unauthorized changes within the IT infrastructure, validate compliance and store configuration changes. The ultimate goal is to have a well-controlled and secured IT environment with emphasis on availability, security and compliance covering designing, implementing and validating stages through tracking and configuration tools.

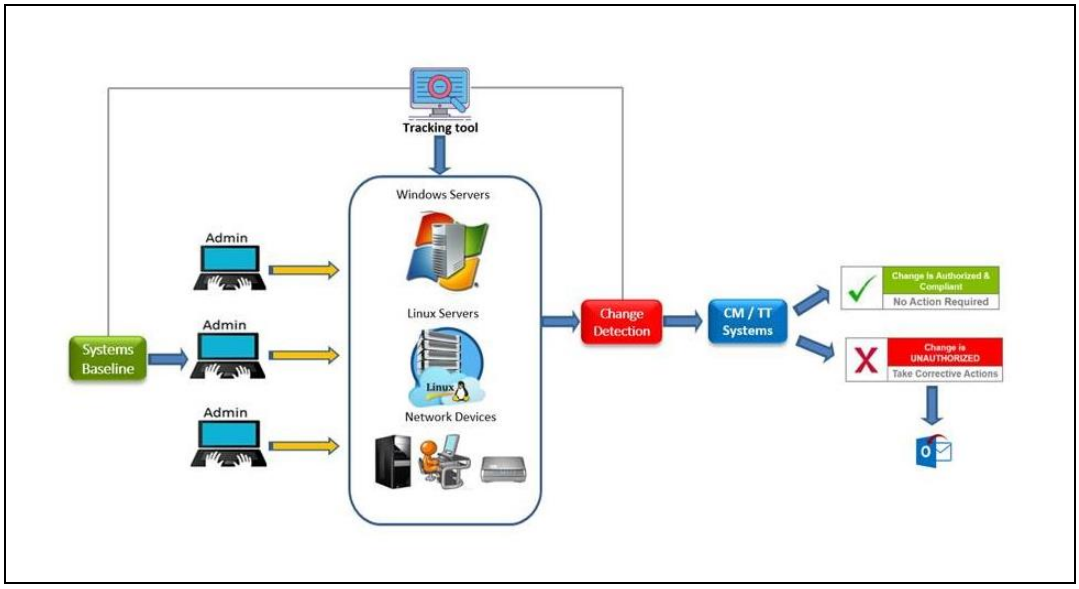

Figure 2: Tracking Tool Process

Figure 2 illustrate tracking tool process. The Configuration changes tracking tool will detect, track and store all changes implemented on IT infrastructure as follow;

1. The tool will capture data/configuration within IT infrastructure components and store it in a file as a baseline for that component.

2. 24 hours after storing the baseline, the tool will automatically check the components data/configuration and compare it with the baselines.

3. If there was any modification to the baseline configuration (add, remove, or change), tracking solution will check if there is an authorize change request or trouble ticket related to this component within the same period. The applied modification is considered authorized change if a valid change request or incident ticket exists. Otherwise, the change is considered as unauthorized.

4. Tracking tool will send an automated email to the task implementer, in order to justify the unauthorized changes during the specified period for the modified listed devices.

5. ITCM should assess and evaluate the case to take the proper action according to the compliance process.

III. CONFIGURATION CONTROLS TOOLS EVALUATION

Feasibility study is essential in order to determine the most appropriate tool based on change management requirements. The following are the steps for configuration changes tracking tools evaluation:

- Identify the scope of IT Infrastructure components.
- Define solution evaluation criteria (minimum requirements) such as:

o Real time tracking and alert: new solution should provide real time alerts mechanism once an improper change occurs (Immediate Alert).

o Integrated with ITCM documentation tool: the key criterion is the integration with ITCM documentation system where it should be capable to check the compliance status of each change.

o Compatible with most industrial systems and devices in IT infrastructure: solution must be suited with most industrial system and devices in IT infrastructure covering network devices, applications, databases and servers.

o Reporting feature: the solution requires reporting feature in order to document all devices information such as name, number, and owner...etc. Also, generate a report for all changes implemented on IT infrastructure components and be able to demonstrate the previous information and compare it with the updated one to identify who made the changes, what changes were made, when the changes were made, and where the information is available.

o Life dashboard mechanism: dashboard mechanism is essential in order to provide real-time views of changes and color-coded by priority and even pinpointed on maps to know where to focus attention first.

- Develop general and technical evaluation criteria such as:

o System bandwidth utilization

o User friendly system

o Availability of local vendor and support

o Availability of system training documentations/materials

o List of reference organization

o Report functionality

o Cost of running the system

o License type

o System roadmap

o Conduct Proof of Concept (PoC) to demonstrate the capabilities of the solution

- Evaluate on/off premise solutions

IV. PERFORMANCE AND VALIDATION PROCESS

This section elaborates on the performance and validation process for testing prior to the changes execution, measuring the performance and validate the compliance of change management process and policies.

A. Testing

Proper testing and validation are crucial to demonstrate that product meets the needed requirements and fits the purpose as follow:

- Develop multiple testing case scenarios
- Test basic functionality
- Test reporting functionality
- Test notification accuracy
- Include stakeholders as part of the testing

B. Key Performance Indicator (KPI)

KPIs plays a major role in measuring the efficiency, effectiveness, quality, and reliability of the process as follow:

- Change success rate: Number of changes successfully implemented relative to the total number of changes authorized in a given time period. This KPI measures the process effectiveness

- Process incompliance rate: Number of unauthorized changes implemented relative to the total number of changes authorized in a given time period. This KPI track and record unauthorized changes by the departments/employee.

C. Compliance

This section demonstrates the disciplinary actions and escalation process for non-compliant acts/behaviors related to change management process, policies, and/or controls as follow:

1. Violation will be issued when not complying with ITCM process with the following escalation as below:

1.1 First three (3) Department violations within a calendar year. For each committed violation, a violation report will be sent to the Head of the violating Department.

1.2 Four (4) or more Department violations within a calendar year:

1.2.1 For each committed violation, a violation report will be sent to the IT Admin Area Head copying the proponent's department Head.

2. The annual violation, counters for departments/employees will be reset to zero (0) at the end of each calendar year.

3. Any post violation feedback can only be communicated by the relevant Department Head.

4. As part of the investigation of any change related cases, all process participants are subject to this compliance process, including change coordinator, task implementer, technical change coordinator and change manager.

5. Compliance reported to IT management on a weekly/monthly basis.

V. CONCLUSION

In conclusion, clear organization requirements along with conducting a benchmark study to determine the best practice and validate the historical record are essentials in order to apply and enforce the suitable process of storing, tracking, preventing and detecting configuration changes.

REFERENCES

[1] How to Implement a Modern IT Change Management Practice, Published 15 April 2020 - Gartner ID G00720845 - 69 min read, by Steve White, pp. 45 – 53.

[2] Magic Quadrant for Enterprise Agile Planning Tools, Published 21 April 2020, Gartner ID G00394014, By Keith Mann, Mike West, Bill Blosen, Akis Sklavounakis, Deacon D.K Wan.