IT Change Control Procedure

2018

Edward Aractingi Phd. PMP CISSP

Marshall University

4/1/2018

TABLE OF CONTENTS

1. INTRODUCTION

The purpose of change management is to increase awareness and understanding of proposed changes across Marshall University Information Technology. Additionally, the change management procedure should ensure that all changes are made in a way that minimizes negative impact to services and customers.

2. CHANGE CONTROL PROCESS

The change control process defines the steps required to perform a change to the production environment or services that are defined as "In Scope".

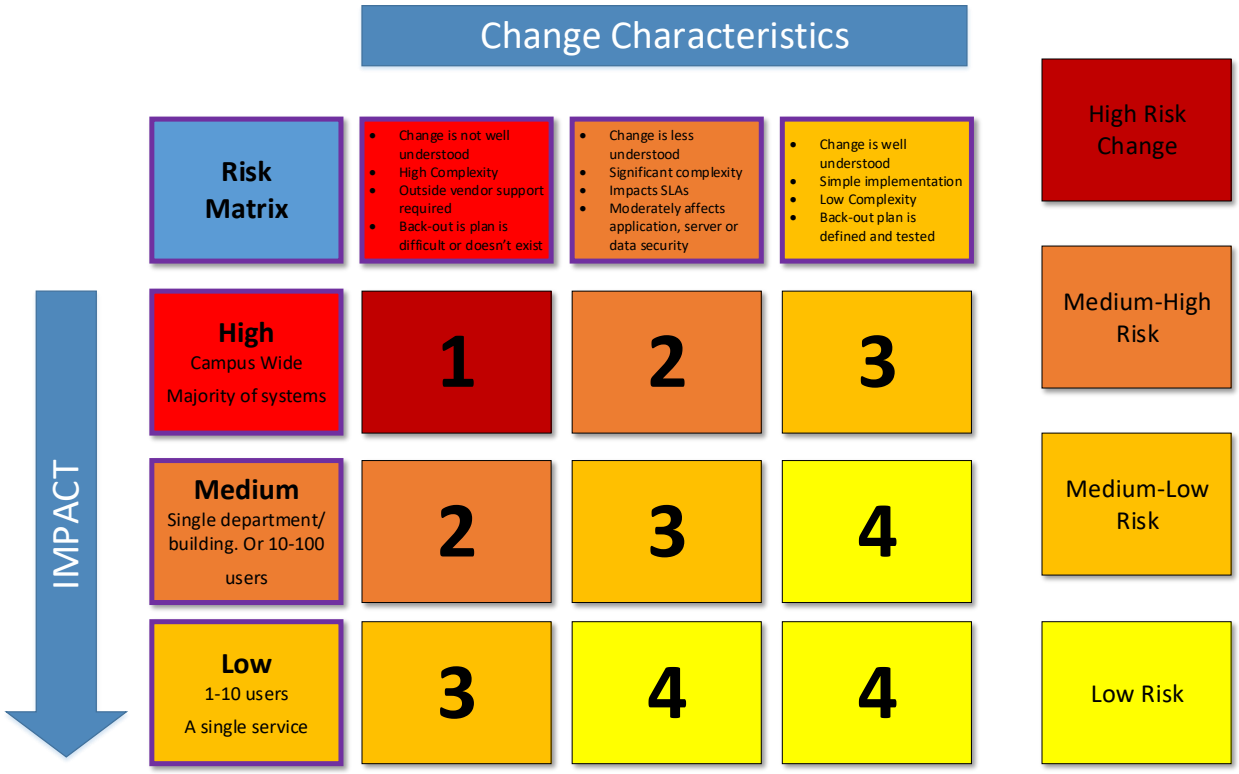
2.1. CREATE A CHANGE REQUEST

Once the need to implement a change to a production service has been identified, a change request is created in the current IT Ticketing System. Refer to Appendix B – IT Ticket Documentation Process .

- Technical Assessment – the change implementer and their line manager review the feasibility of the change from a technical perspective and analyze the technical risks associated with the change. The analysis should take place for any steps required to reach the desired outcome. Vendor documentation, user communities and peer reviews should all be used to complete this assessment.

- Business Impact – The line manager, working with the change implementer, the director of their department and the service owner (or the business unit impacted by the change) should review the possible impact on the business operation during and after the change.

- Risk Assessment – the change implementer and their line manager should review the risk associated with performing the change. Risk can be evaluated on the following table by evaluating the impact and urgency of the change.



2.2. RISK LEVELS

- Low – For standard/routine changes, the risk is low. Low risk levels tend to have the following characteristics:
  - Involves IT resources from only one functional team within Information Technology.
  - Low complexity, i.e., no technical coordination required.
  - Low risk to service availability.
  - Simple implementation and simple back-out plans.
  - No impacts to service level agreements.
  - The change is well understood and has been tested.
  - Back-out plan is defined and tested.
- Medium – Significant changes are medium to high-risk. Characteristics of medium-risk include:
  - Involves IT resources from more than one functional team.
  - Significant complexity – technical coordination required from one or more functional teams.
  - Moderate risk to service availability.
  - Some complexity to implementation and back-out plans, back-out not expected to extend the implementation timeframe.
  - Moderately affects application, data or server security

  - Impacts service level agreements
  - Change is less understood
  - The change has been partially tested including the back-out plan or cannot be tested but back-out plan is well defined.
- High – The risk level of a change is considered to be high if any of the following criteria apply:
  - Involves IT resources from more than two functional teams.
  - High Complexity – complex technical coordination required with one or more functional teams.
  - High risk to service availability
  - Complex implementation and back-out plan. The back-out likely to extend beyond the planned change window.
  - Affects the security of data.
  - Impacts the service level agreements.
  - Outside vendor support is required.
  - The change is not well understood
  - Back-out is difficult or does not exist.

2.3. APPROVAL

The type of change being made determines the level of approval required.

- Standard Changes – Standard changes are pre-approved and are conducted as part of the normal course of business.

- Significant Changes – Must be submitted for review and approval to the IT Executive Committee that meets Monday mornings and the effected business unit(s) or committee (i.e. Banner Oversight Committee) if applicable. A significant change should have a minimum of 5 business days of lead time prior to the change.

- Emergency Changes – Must be approved by the service owner when possible and the Chief Information Officer or their designate.

2.4. SCHEDULING

All significant changes should be entered as Scheduled Maintenance at https://itservicestatus.marshall.edu.

2.5. PRODUCTION CHANGE-FREEZE SCHEDULE

During the course of the year, there are certain periods that are considered production change-freeze dates. During these periods, no significant changes should be made to the infrastructure or services without approval from the CIO or delegate. Some examples of production change freeze dates are:

- Start of the semester – 7 days prior to the start of the semester and extending to the end of the first week of classes.
- Dead Week – The week prior to exams/finals.
- Finals Week – The week of finals through the end of the grading period.

For the complete list of the current production freeze dates, go to http://www.marshall.edu/it/productionfreeze .

2.6. COMMUNICATION

All significant and emergency changes require a posting in the chronological list of changes (aka a CLOC posting) pre- and post-change notification. Currently change notification services are located at https://itservicestatus.marshall.edu. However, depending on impact and determined by the IT Executive team, additional communications, such as an email, may be required.

2.7. IMPLEMENTATION

Implementation of the change should be completed during the scheduled service window. Any changes to the planned implementation should be updated on https://itservicestatus.marshall.edu, including when the change takes longer than expected.

2.8. TESTING AND VALIDATION

After implementing the change, the change administrator's team under the leadership of their manager must validate that the change was completed successfully and achieved its goals.

The IT Service Desk must test that the impacted systems are functioning as expected and send notification if there are any issues.

2.9. ACCEPTANCE

Once the testing and validation is completed and it confirmed that change was successful, the manager of the group implementing the change will update the ticket with a note that the change is accepted and close it.

3. POST CHANGE COMMUNICATION AND DOCUMENTATION

3.1. CLOC UPDATES

The change implementer is responsible for updating chronological list of changes (CLOC) postings at https://itservicestatus.marshall.edu with the post change status of the service.

3.2. EMAIL UPDATES

If an email was sent out prior to the change to notify the Marshall University community then a post change status email is required when services are restored or if any outages will last longer than planned.

4. SCOPE AND EXCEPTIONS

4.1. IN SCOPE

The intended scope of the Marshall University Information Technology change management procedure is to cover all of MU IT's services and platforms except for those defined as out of scope.

4.2. OUT OF SCOPE

There are many services and tasks that performed by Marshall University Information Technology that are considered out of scope of the change management procedure but do still require an *operational process* such as requiring a support ticket (i.e. Footprints, ServiceNow ..etc.).

- Disaster Recovery
- Non-production changes
- Daily administrative tasks
    - Password resets
    - File permission changes
    - User desktop support
    - Single network port configurations such as port security and VLAN changes
    - Single user/small group VOIP changes such as moves, adds, changes to a single telephone or administering team call groups
    - Changes that affect a single user

5. APPENDIX A – KEY TERMS AND DEFINITIONS

- Standard Change – A low risk routine change with well-understood outcomes that is made during the course of business. A standard change follows pre-determined processes, is pre-approved and may be made at the discretion of an individual employee.

- Significant Change – Significant changes have medium to high-risk, involve critical services, outcomes that are less predictable and/or are not made during the normal course of business. Significant changes must follow the change control procedure and require approval based on risk and impact.

- Emergency Change – Emergency changes are similar to significant changes but must be executed as soon as possible. Examples of emergency changes included, changes to correct or prevent an imminent outage or urgent security threat. Emergency changes follow fewer steps but must be approved by the Chief Information Officer or two members of the IT Executive team. Emergency changes must be reviewed at the next IT Executive Meeting.

- Change Owner – The person responsible for documenting, planning, coordinating and implementing or assigning an implementer. The change owner will make sure any IT Ticketing issues are updated as well as updating the CLOC notification service.

- Change Driver – This is the source of the change such as a security update, software patch or functionality improvement.

- Risk – is determined by a combination of the assurance that a change will happen as expected and the potential impact of a change should it not go as expected

- Impact – Determined by potential disruption to customers and dependent systems.

- CLOC – Chronological List Of Change

6. APPENDIX B – IT TICKET DOCUMENTATION PROCESS

The following items are included in any change request submitted via the ticketing system (e.g. Footprints or FP for short) for approval.

- Urgency
- Change Owner
- Change Driver/Source
- Risk/Impact Level
- Status – (Not necessarily the same as the support ticket status – e.g. open, closed – but needed in order to maintain the final status of the change after the issue is closed.)

  - New
  - Approved
  - On Hold
  - Completed without Issues
  - Completed with Issues (include details in update)
  - Unsuccessful
  - Cancelled
- Type of Change
- Implementation Plan
- Dependencies
- Impacted Services
- Back-Out Plan
- Proposed Date/Time of change
- Estimated Time to Complete

7. APPENDIX C – CLOC POSTING PROCESS

1. Login to Cachet at https://itservicestatus.marshall.edu/dashboard
2. If you are reporting an unscheduled outage/incident
    i. Click the blue "Report an Incident" button to the left of the screen.
    ii. At a minimum, fill out all of the fields that are not labeled as optional to complete the incident. Be sure to designate the component when available.
    iii. Ensure "Notify subscribers" is checked then click add
    iv. Be sure to update the status of the incident as it changes.
3. If you are scheduling a change ahead of time
    i. Click "Maintenance" located on the sidebar menu on the left of the screen
    ii. Select "Add Maintenance" on the top right of the screen
    iii. Fill out all fields to fully complete the maintenance form. Be sure to select the correct time and date when answering when the maintenance is schedule. Cachet will use this information to automatically update the IT Maintenance calendar.

1. Impact – estimated impact of the maintenance on the affected environment (outage, partial outage, degraded performance, etc.…)
2. Affected – Any and all anticipated applications, services and systems that may be directly impacted by the maintenance.

iv. Click the green "Add" button at the bottom of the screen to submit the maintenance.