ITSM Enterprise Change and Release Management

Policy and Process Documentation

Document Ownership

Document Owner	ITSM Role, Department
Maury Collins	Service Transition Owner, Digital

Revision History

Version #	Revision Date	Revision Author	Revision Summary	Approvers
1	9/23/2016	Paul Censullo	New document, based on previous version from CompuCom	
2	12/13/2017	Paul Censullo	Reviewed	
3	2/14/2018	Paul Censullo	Update for consistency between process documentation	
4	5/3/2019	Paul Censullo	Updated for new section on governance and new definitions for Key Terms	
5	7/24/2019	Paul Censullo	Updates to policies for Change Type, Change Freezes, and Unauthorized Changes	
6	8/13/2020	Paul Censullo	Updates to policies and workflow diagrams, including swim lanes. Also added vendor expectations and consolidated workflows for all change types.	
7	9/10/2020	Paul Censullo	Edit to vendor expectation document	
8	10/30/2020	Paul Censullo	Clarified policy for Pre-Approved Changes.	
9	11/11/2020	Paul Censullo	Updated policy for Change Manager review of CRs for "CI Not Found."	
10	12/29/2020	Paul Censullo	Updated for rebranding MGB, CCB, and vendor supply team additions	
11	2/11/2021	Paul Censullo	Updates throughout for enhancements in January 7 release of ServiceNow application	
12	4/26/2021	Paul Censullo	Updates to workflows due to Emergency Minor Changes no longer requiring CCB	

13	7/15/2021	Paul Censullo	Updates throughout for enhancements in July 8 release of ServiceNow application	
14	10/28/2021	Paul Censullo	Added policy for Compliance, and miscellaneous updates for PIR and leadership approval.	
15	3/18/2022	Paul Censullo	New policy regarding application maintenance schedules.	
16	12/21/2022	Paul Censullo	Clarified policies regarding CCB attendance and communication of outages	
17	3/30/2023	Paul Censullo	Miscellaneous updates for branding and update references for Crisis incidents	
18	8/25/2023	Paul Censullo	Updates to policies for Compliant and Emergency Changes to be associated with Incidents/Major Incidents	
19	11/17/2023	Paul Censullo	Updates to incorporate Release Management best practices	
20	2/12/2023	Rob Smith	Added Release management grid, comparison with a release and without	

Contents

Introduction

Purpose

This document provides a high-level overview of the Change and Release Management process used to manage Changes and Releases within the Digital department at Mass General Brigham (MGB). It documents the workflow, roles, procedures, best practices, and policies needed to implement a high-quality process and ensure that the processes are effective in supporting Mass General Brigham. The Change and Release Management process is geared to ensuring adequate review, communication, and analysis of all Changes and Releases affecting the organization, as well as a mechanism for reviewing the overall Change and Release Management strategy.

Scope

The Change and Release Management process applies to all Mass General Brigham employees, contracted vendors, and organizations that introduce or implement Changes and Releases in the MGB environment. Changes include the addition, modification, or removal of a supported service or a modification to an application or hardware. A Release is a collection of one or more Changes to the production environment. Other service management areas are detailed in separate documentation.

Value

A well-defined and maintained Change and Release Management process will provide numerous benefits to Mass General Brigham users. For example:

- Standardizes and optimizes Change and Release process with a prescribed method of governance.
- Provides a structured process for planning, scheduling, communicating, and implementing Changes and Releases required by the Mass General Brigham business, thereby minimizing conflicts.
- Enforces a required level of technical and management accountability for every Change and Release.
- Ensures that Changes and Releases are made with minimum disruption to the services Digital has committed to its users.
- Minimizes downtime resulting from unapproved, unscheduled, or unsuccessful Changes and Releases, thereby increasing productivity of Digital staff and availability of systems and applications
- Supports Change and Release owners with a streamlined process to facilitate the successful implementation of Changes and Releases to the Mass General Brigham Digital environment.
- Improves alignment of IT services to the actual Mass General Brigham business and user requirements.
- Provides a source for information regarding every Change and Release to assist in problem resolution and continuous improvement.

Well-planned and implemented Change and Release and Management will make a significant difference to an MGB's service costs. A poorly designed Change or Release will, at best, force MGB staff to spend significant amounts of time troubleshooting problems and managing complexity. At worst, it can cripple the environment and degrade live services.

Goals

- Ensure Mass General Brigham Digital can effectively deal with change in a way that ensures the maximum value from our resources.
- Streamline procedures to reduce the negative impact on Digital staff and end users. This should result in increased productivity of users through fewer disruptions (higher service availability) and higher quality services.
- Adapt the Change and Release Management process to the Mass General Brigham culture
- Allow our Change and Release Management process to scale to our future needs

Governance

This section describes how we implement policies and technology. The intent is to ensure collaboration with all stakeholders to ensure updates are fully vetted before implementation. For each activity, steps include review, provide guidance and approve. If deny from any activity, then send back to the submitter for adjustments and resubmit based on changes.

Note: For Change Management governance, the Change Advisory Board (CAB) provides a forum for policy and process update discussions. The CAB consists of permanent CCB members.
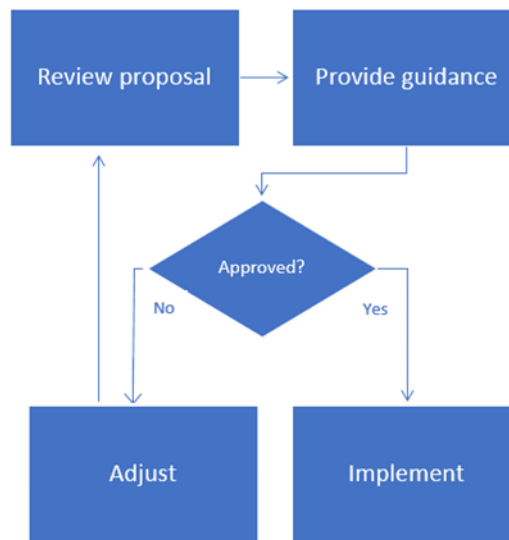
For Policy and process, the activities are as follows:

1. Process Owner and Manager agree on proposal
2. Process Owner presents risks/benefits to ITSM Program Senior Manager
3. Discuss proposal with CCB members. This typically occurs during CAB meetings
4. ITSM Program Senior Manager presents proposal to Office of CIO
5. ITSM Program Senior Manager presents proposal to Digital Leadership
6. ITSM Program Senior Manager reviews outcome with Process Owner
7. Process Owner and Manager implement

For Technology, the activities are as follows:

1. Process Owner and Manager agree on proposal
2. Process Owner presents risks/benefits to ITSM Program Senior Manager
3. ITSM Management team reviews enhancement to determine level of effort and scheduling
4. ServiceNow team develops
5. Process Owner and Manager validate technology
6. ITSM Program Technical Writer documents technology change in Knowledgebase (KB)
7. ServiceNow team implements using Change Management

Change Management vs Release Management

Change Management and Release Management at MGB are different but related functions within the Digital organization. At a high level, Change activities relate to the process of requesting, assessing, authorizing, and reviewing Changes. Release activities include planning, designing, configuration, rollout planning, testing, communication and deployment. Release Management provides the schedule and execution while the Change Control Board authorizes significant and major Changes to controlled environments.

While Change Management is strategic in nature, Release Management is more operational. Put another way, Change Management is the gatekeeper, protecting the Production environment, while Release Management is the doer, building, testing, and deploying Changes as a whole or in batch.

Change Management is an authorization process. Release Management is a build-test-and-implement process, with activities managed largely within individual teams.

Change Management involves pre- and post-deployment activities, while Release Management is focused on deployment activities.

While Change Management culminates in a post-implementation review, Release Management concludes with the successful versioning of a release. Example, major release 2.0 to 3.0, Minor release 1.1 to 1.2.

Note that Release Management activities are primarily conducted in pre-production environments, which fall outside the control of Change Management at MGB Digital. However, MGB Digital encourages the use of Release Management best practices.

Release Management Best Practices

Release Management best practices include the following:

- Have a system for planning each release and be sure that plan is communicated and approved by all stakeholders and be sure that this plan is maintained throughout the release cycle.
- Have a system for source control and be sure to indicate the interdependencies between each release component.
- Have staging areas to fully test the release in pre-production environments.
- Have a backout plan to roll back to the last known good state in the event the release fails. This plan must be tested and include actionable steps.
- And be sure to compile lessons learned during the Post Implementation Review. More details on the Post Implementation Review will be provided later in this document.

Change that Includes a Release vs. No Release

A Change is determined to include a release from Digital teams when the following are attributes of the Change hold true. *Note: Not exhaustive, nor in order	A Change is determined **not** to include a release from Digital teams when the following are attributes of the Change hold true. *Note: Not exhaustive, nor in order
- Routine throughout the lifecycle of the product or service - Well-coordinated amongst stakeholders - Planned well in advance of implementation (Major Change) - Risk is astutely managed as the impact is extensive due to the nature of - Plans (implementation, test, comms, backout plans) are robust - Inclusion of multiple customer requests to be bundled to deliver enhancements - As per the policy, product version will either be either major or minor upgrade number. Example major release: 1.0 to 2.0, example minor: 1.1 to 1.2 (Page 7 in policy) - Scheduled on a routine throughout the product lifecycle - Pre testing in non-prod & post Change validation testing is accomplished.	- An update to restore services in expedited or emergency timeframes - Update to a product that is at, or near end of life - An update to maintain services that do not increment the product version - Risk is not high - Impact could be broad due to nature to restore services or maintain service health - As per the policy, pre testing in non-prod & post change validation testing is accomplished (Page 24 in policy) - Change does not list a release in the change description, impact or justification fields on the change - Backout plan does not include a version update or down grade.

Policies

1. Change Policy Compliance	
Objective	To provide a consistent set of processes and procedures required to minimize and measure the impact of Change-related incidents and stabilize day-to-day operations.
Policy Scope	This policy covers all departments and customers involved with making changes to the IT infrastructure. The policy includes all IT changes to hardware, software, applications and services associated with the running, support, and maintenance of Mass General Brigham production and nonproduction environments. The policy applies to all employees, contractors, and subcontractors (vendors) who perform duties or deliver services within a Mass General Brigham controlled environment or who use a MGB-owned asset. This policy applies to all equipment owned, managed, leased or contracted by Mass General Brigham. Compliance with this policy is mandatory. Failure to comply may result in disciplinary action, up to and including termination of employment or contract.
Functional Policy	All employees and suppliers must comply with the policies and procedures developed by the Change Management Process Owner. Any exception requires written approval by Change Management and any other parties involved (such as Business Owners). All employees must complete Change Management training as assigned by the organization. New hires are automatically assigned to complete Change Management training upon joining the organization.
Enforcement	Manual

2. Change Manager Responsibilities Policy	
Objective	To provide consistent expectations and review of Changes and to ensure that Change Requesters are managing their Change requirements effectively and efficiently.
Policy Scope	This policy covers all Supervising Managers within all departments involved with reviewing and approving Changes to the IT infrastructure.
Functional Policy	All Supervisors and Supervising Manager must comply with the policies and procedures developed by the Change Management Process Owner. He/she will be responsible for the review of all Changes submitted by their staff and ensuring that the Changes and associated Requester adheres to all defined Change Policies. *Note: If "CI Not Found" is indicated for any Change, the Change Manager contacts the requester to ensure that a ServiceNow request has been initiated. The existence of this request demonstrates that the requester has begun working with ITSM Configuration Management-phs to have the CI or CIs added to the CMDB, as needed, so that "CI Not Found" will not be used again for this CI.*
Enforcement	Manual

3. Change Lead Time Policy	
Objective	To provide adequate time to properly evaluate and plan for authorization, approval, and implementation of a Change, while minimizing Emergency and Expedited Changes and the impact on the organization.
Policy Scope	This policy covers all departments and customers involved with making changes to the IT infrastructure. The policy includes all IT changes to hardware, software, applications and services associated with the running, support, and maintenance of Mass General Brigham production and nonproduction environments.
Functional Policy	A Request for Change (RFC) or Change must be submitted in time for appropriate assessment prior to authorization and implementation. Lead times are dependent on the categorization of a Change. To ensure that a Change is processed as a Normal Change (not Emergency or Expedited), the following minimum lead times are required: • Major Change – At least 30 days • Significant Change – At least 7 days • Minor Change – At least 2 days *Note: The only exception to this is for Pre-Approved Changes, which do not require any lead time.*
Enforcement	Technological (ServiceNow)

4. Change Type Policy	
Objective	To ensure that a Change is assigned a Change Type. This will provide the information to define the level of authorization and priority.
Policy Scope	This policy covers all Changes.
Details – Functional Policy	The Change Type process examines the impact of all approved Changes on the organization. All Changes will be assigned a Change Type of Normal, Expedited, Emergency, or Pre-Approved. ServiceNow assigns a Change Type of Pre-approved to a Change when the user selects the Pre-approved Change check box and specifies a valid entry. Otherwise, ServiceNow assigns the Change Type by calculating the available lead-time for your request (the Submit date/time vs the Start date/time) for each Change Subtype as follows:

Subtype…	… with Lead Time…	results in Change Type…
Minor*	>= 2 days	Normal
	< 2 days, > 30 minutes	Expedited
	<= 30 minutes, or in the past	Emergency
Significant	>= 7 days	Normal
	< 7 days, > 30 minutes	Expedited
	<= 30 minutes, or in the past	Emergency
Major	>= 30 days	Normal
	< 30 days, > 30 minutes	Expedited
	<= 30 minutes, or in the past	Emergency

All Changes with a Change Type of Major or Significant are reviewed by the Change Control Board (CCB) or Emergency Change Control Board (eCCB).

    * Minor Changes should not include outages unless the associated app CI includes a maintenance schedule.

Enforcement	Technological (ServiceNow) ServiceNow also provides a suggested Change Subtype based on information the requester provides for information related to risk and impact for the Change.

5. Change Authorization Policy	
Objective	To ensure that all Changes are authorized by appropriate parties.
Policy Scope	This policy covers all Changes.
Functional Policy	All Changes must be properly authorized at the appropriate time during the life of the Change. The following table shows the approvers that are required based on the Change Type:

Change Category	Minor	Significant	Major
Approval	• Supervising Manager • Configuration Item Owner	• Supervising Manager • Configuration Item Owner • Change Management • Digital VP	• Supervising Manager • Configuration Item Owner • Change Management • Digital VP

Note: During Change Freezes, all Changes require Leadership approval. Minor Changes also require Change Management approval.

Change Management reviews all Significant and Major Changes for compliance before they are scheduled for a Change Control Board meeting as well as after implementation. A compliant Change is a well-prepared and executed Change. It is one that clarifies what, why, and how the Change is being executed and one that is reviewed by the requester after implementation. It includes specific requirements for the following fields:

- Configuration Items
- Change Description
- Justification
- Dates and Times
- Planning Fields (Testing, Implementation, and Backout Plans)

The workflow state **Awaiting CCB** indicates when a Change has received all approvals other than Change Control Board (when required). A Change should only be implemented when it is in the **Awaiting Implementation** state (except for Emergency Changes).

Enforcement	Technological (ServiceNow)

6. Change Compliance Policy	
Objective	To ensure Changes meet specific requirements for proper preparation and execution.
Policy Scope	This policy covers all Changes.
Functional Policy	A compliant Change is a well-prepared and executed Change. It is one that clarifies what, why, and how the Change is being executed and one that is reviewed by the requester after implementation. It includes specific requirements for the following fields:

Field	Requirement
Configuration Items (CIs)	• Include CI or CIs to which the Change is to be applied. • Ensure all CIs have all recommended and required fields completed.
Change Description	• Fully identify what is being changed, using text that is clear and understandable by anyone outside of your team. • Changes required to resolve an incident must be associated with the incident. • For Emergency and Expedited Changes that include the words "break/fix," must include the parent MI number.
Justification	Fully identify why the Change is being made.
Dates and Times	• Change is submitted and approved by Tuesday at noon before the targeted CCB meeting. • Allow sufficient lead time for a Normal Change. • Be sure any Service Outage falls within the Change window.
Testing, Implementation, and Backout Plans	• Include actionable and detailed steps. • If there is a Service Outage, include the communication plan detailing the business impact to all stakeholders. • If using an attachment or link, be sure that it is valid. • If no Backout Plan exists (such as if the Change is implemented by a vendor), provide the initial remediation steps or escalation procedure.

Change Management reviews all Significant and Major Changes for compliance before they are scheduled for a Change Control Board meeting as well as after implementation.

	For Pre-Compliance, Change Management reviews Changes for each of the previously identified fields. Any Normal or Expedited (Significant & Major) Changes that are submitted by Tuesday at noon prior to the targeted CCB meeting is considered "Submitted for on-time review." During Change Freezes, Minor Changes must also adhere to this timing. If any field does not meet the specified requirement, the Change is deemed not Pre-Compliant. For Post-Compliance, Change Management assesses Changes for the following requirements following implementation: • PIR complete – The requester manually identified the Change as successful, successful with issues, or canceled following implementation. • Authorized prior to implementation – Except for Emergency Changes, all required approvals were granted before the implementation date. Changes that do not meet both requirements are deemed not Post-Compliant. The ITSM Change Management Dashboard reports the Compliance status for all Changes.
Enforcement	Manual and Data Entry (ServiceNow)

7. Change Control Board Policy	
Objective	To provide the standards required for the Change Control Board (CCB) to function.
Policy Scope	This policy covers all Changes that require assessment, approval, and review by the Change Control Board (CCB).
Functional Policy	A Change Control Board (CCB) is a group of people who can give expert advice to Change Management on the implementation of Changes. This board is made up of Site Administrators from all sites within MGB Digital and representatives from the business units to help determine business impact. CCB responsibilities include: • Approving of Changes – Changes rejected by the CCB will be noted by the CCB scribe. • Reviewing the Change Management process, including any amendments made to it during the period under discussion. • Reviewing Change Management wins/accomplishments for the period under discussion, for example, a review of the business benefits accrued by way of the Change Management process. • The CCB will meet on a regularly scheduled basis to be established by the Change Manager.
Enforcement	Manual

8. Unauthorized Change Policy	
Objective	To ensure that no unauthorized Changes occur within the environment, all Changes should adhere to the Change Management policies and procedures.
Policy Scope	This policy covers Changes that are being implemented.
Functional Policy	Changes that have not obtained the required approvals as stated within the Change Authorization Policy are considered unauthorized Changes. Unauthorized Changes are tracked and reported to senior management.
	An unauthorized Change results from any of the following:
	• A Change not submitted for the associated Change.
	• A Change does not follow the Change Authorization Policy, such as the required approval was not given at the workflow states defined within the Change Management procedures.
	• The Change implementation started outside the scheduled deployment window.
	Note: Changes with implementation windows greater than 24 hours should include Change tasks for each calendar day associated with the Change.
Enforcement	Manual

9. Emergency Change Policy	
Objective	To enable Change Management to deal with Emergency Changes quickly, without having to sacrifice normal management controls.
Policy Scope	This policy covers all departments, customers, and vendors involved with making Changes to the IT infrastructure. The policy includes all IT changes to hardware, software, applications and services associated with the running, support, and maintenance of Mass General Brigham production and nonproduction environments.
Functional Policy	A Change will be considered to be a valid Emergency Change if one or more of the following applies: • The Change is required to resolve a Major incident/Crisis • The Change is required to prevent a Major incident/Crisis *Note: The system automatically assigns a subtype of Emergency to any Change with less than 30 minutes or less of lead time (submittal time vs implementation time) or in the past.* *Emergency Changes are reviewed by the eCCB, a subset of the Change Control Board.* Any Changes required to resolve a Major incident or Crisis must be submitted by the SME (subject matter expert) within 2 hours after resolution. Every Change must note the parent Major Incident ticket number (obtained from the Major Incident Manager). For Major and Significant Changes, approvals include: • CI Owner • Manager • Digital VP • eCCB For Minor Changes, approvals include: • CI Owner • Manager • Digital VP (email notification) • eCCB (email notification) *Note: During Freezes, all Changes also require Leadership approval. Minor Changes are subsequently reviewed by Change Management.*
Enforcement	Technological (ServiceNow)

10. Expedited Change Policy	
Objective	To enable Change Management to deal with Expedited Changes quickly, without having to sacrifice normal management controls.
Policy Scope	This policy covers all departments, customers, and vendors involved with making changes to the IT infrastructure. The policy includes all IT changes to hardware, software, applications and services associated with the running, support, and maintenance of Mass General Brigham production and nonproduction environments.
Functional Policy	- A Change will be considered to be an Expedited Change if the Change submission does not comply with the Change Lead Time Policy and requirements for Normal Change submission as stated within that policy. - Major or Significant Major Changes that require implementation prior to the next Change Control Board (CCB) meeting are reviewed by the Emergency Control Board (eCCB).
Enforcement	Technological (ServiceNow)

11. Pre-Approved Change Policy	
Objective	To ensure that a Pre-Approved Change process is defined to enable that such Changes are efficiently and effectively processed to support the organization's business needs.
Policy Scope	Pre-Approved Changes that are defined by the Change Management process.
Functional Policy	A Pre-Approved Change is a Change that follows an established path, that is low risk, routine, and is the accepted solution to a specific requirement or set of requirements. The crucial elements of a Pre-Approved Change are: • The Change is routine, low-risk, and can easily be backed out • No outage occurs during the implementation • The Pre-Approved Change template must be approved prior to use • The Change Subtype is Minor *Note: Changes based on Pre-Approved Change templates use a streamlined process, and are approved only at first use. Other Minor Changes that are not associated with Pre-Approved Changes must be reviewed and approved using our full Change Management process.*
Enforcement	Manual

12. Change Communication Policy	
Objective	To ensure that all planned Changes have been communicated to the business/users, implementation team, and related process areas that may be potentially impacted by the Change.
Policy Scope	This policy covers all Significant and Major Changes that occur.
Functional Policy	Changes categorized as Significant or Major that are under the control of Change Management will be communicated to the necessary businesses/users. Implementation teams, and related process areas.
Enforcement	Technological (ServiceNow)

13. Change Freeze Policy	
Objective	To ensure that required freezes to the production environment are requested, documented, and approved appropriately to ensure that no Changes will occur on a specific entity or facility during a specified period of time.
Policy Scope	This policy covers all requested Freezes within the environment.
Functional Policy	A Change Freeze represents a block on Production Changes impacting the same entities or facilities, applications, and resources during the major event window. Change Freezes can be: • Enterprise – No Changes for the entire enterprise • Site Specific – No Changes for the associated site or any Enterprise Change that affects that site A Change Freeze are typically implemented as a result of a specific event. This can include an inspection from a regulatory agency or major additions to the Mass General Brigham environment, such as new affiliates, major hardware or software implementations, or facilities maintenance which temporarily removes desired redundancy. All Changes* for the Change Freeze period require Leadership approval and are given added scrutiny, particularly those impacting the same entities as the major planned event. Whenever possible, Changes are rescheduled outside the major event window. *Except Cache Dev/QA and Pre-Approved Changes
Enforcement	Technological (ServiceNow)

14. Forward Schedule of Change Policy	
Objective	To ensure that all planned Changes have been identified and any associated conflicts to rains awareness of possible impact and risk.
Policy Scope	This policy covers all areas involved in making changes to the IT infrastructure and all areas affected by the Change.
Functional Policy	The Service Desk communicates to the User community at large any planned additional downtime arising from implementing the Changes using the most effective methods available.
Enforcement	Manual

15. Change Testing Policy	
Objective	To ensure that all Changes are tested, for which testing capabilities exist, prior to being implemented within the production environment.
Policy Scope	This policy covers that all changes that require pre-testing in non-prod & post change validation testing is accomplished.
Functional Policy	A Change requires successful completion and sign-off of testing before being implemented into the production environment, where environments allow. Immediately after implementation in the production environment, the Change must be retested to ensure the expected outcome has been achieved. If any issues were encountered, they must be specifically spelled out in the results of the Change on the Post-Implementation Review, as required, to close the Change. *Note: Changes are automatically closed after 5 days if the Post-Implementation Review is not completed, and the Change is deemed not Post-Compliant.*
Enforcement	Manual

16. Change Success Criteria Policy	
Objective	To ensure that all Changes follow a standardized evaluation of success in order to protect the stability of the infrastructure.
Policy Scope	This policy covers all Changes that are being implemented.

Functional Policy	A change is considered successful based on the following criteria:
	
	• No Change Related Incidents - As a result of the release being implemented into the production environment, there have been no incidents that are directly related to the release.
	• No Other Failures – Following the release into the production environment, there are no other failures to any other components or configuration items (CIs) related to the release.
	• Change has been Satisfied - Within the Change, an outline of the specific Change has been detailed, including a timeline for the Change to take place, and any other information pertaining to the accuracy of the Change has been confirmed to be successful.
	• Deemed as such by Change Manager
	    o This can be the agreement or approval of the individuals who have been outlined in the Change (that is, the specific roles involved), indicating that the release into production does what it is expected to do.
	    o Further, there can be confirmation of any additional requirements as outlined by the CCB (such as timelines, activities completed, etc).
	• Release has Occurred – If the Change was meant to repair a CI component or application's functionality, the symptoms that had previously occurred within the environment no longer occur.
	• Post-Implementation Review (PIR)
	    o To be conducted by the Change Requester.
	    o Will ensure that within the PIR, a checklist of all or mandatory items have been confirmed.

Enforcement	Manual

17. Failed Change Policy	
Objective	To minimize failed Changes and related impacts to business.
Policy Scope	This policy covers Changes that are being implemented.
Functional Policy	Failure of a Change is deemed as such if the results of the Change are not successful and the Change Requester and implementors of the Change deem it as failed. A failed Change may result from any of the following: • One or more incidents related to the Change • The Change must be backed out for any reason • The Change deployment goes past the required implementation date (for example, started within the scheduled deployment window, but completed outside the scheduled deployment window) • The state Change objective was not achieved • A Change was found to have been unauthorized
Enforcement	Manual

18. Change Post-Implementation Review Policy	
Objective	To maximize and continually improve the benefits of the Change Management process and reduce costs and to gain information and understanding with which to improve based on reviewing changes. A successfully completed Post-Implementation Review (PIR) will be used in process evaluation and continuous process and service improvement. The overall intent of the review is to ensure that all standardized and repeatable methods and techniques are used to achieve effective and efficient handling of al Changes in order to prevent future Change related incidents.
Policy Scope	This policy covers all Changes including Emergency and Expedited Changes.
Functional Policy	The Post-Implementation Review (PIR) process is designed to collect and utilize the knowledge learned throughout an implementation to optimize the delivery and outputs of implementations in the future. The content of this review will vary depending on the success factor for the Change, problems that may have been encountered because of the Change, and the category of the Change.
Enforcement	Technological (ServiceNow)

19. Application Maintenance Schedule Policy	
Objective	To ensure that critical applications include a process that allows them to be routinely inspected, adjusted, and repaired. Also ensures that Changes affecting these applications are scheduled in a consistent timeframe.
Policy Scope	This policy covers all Changes including Emergency and Expedited Changes.
Functional Policy	All applications with the Impact to HealthCare Operations field set to High must include a maintenance schedule in ServiceNow.
Enforcement	Change Control

Key Terms and Definitions

Backout Plan: A contingency plan of step-by-step instructions to minimize any disruption of service if a Change implementation does not go as planned. The Backout Plan is required entry for every Change. The plan should include sufficient details to allow an individual with similar skills to execute the plan and clear enough to be understood by all approvers.

Change: The addition, modification, or removal of a supported service or a modification to an application or hardware.

Change Advisory Board (CAB): This group meets on a regular basis to provide a forum for policy and process update discussions. It is responsible for giving expert advice regarding Change Management governance. It consists of the permanent members of the Change Control Board (CCB).

Change Control Board (CCB): The group responsible for giving expert advice to Change Management on the implementation of Changes. It includes representatives from all areas within Mass General Brigham, including site leadership, configuration owners, application owners, technical leadership, as well as any individual with stakeholder interest. It meets on a weekly basis to review Major and Significant Changes prior to implementation to be sure they are sufficiently researched, planned, communicated, coordinated, and executed. Some CCB members also serve on the Change Advisory Board.

Change Manager: Responsible for setting the CCB agenda and for reviewing Changes for completeness and potential conflicts prior to weekly meetings. The Change Manager has the authority to defer any change that is deemed to represent a potential problem to Mass General Brigham system availability or network integrity.

Change: A record containing details of a Change. Each Change documents the lifecycle of a single Change. Changes can be created directly by users with ITIL access in ServiceNow or may also be created when an RFC is approved by the group identified as the Assigned Group on the RFC.

Change Subtype: A categorization of a Change based on its risk and impact. ServiceNow suggests a Change subtype based on information associated with the risk and impact of the Change.

Risk Impact Matrix

		Impact		
		Low	Medium	High
Risk	Low	Minor	Minor	Minor
	Medium	Minor	Significant	Significant
	High	Minor	Major	Major

- **Major –** Enterprise-wide impact and high risk.
- **Significant –** Multiple-site impact and medium risk.
- **Minor –** Single department impact and low risk.

Level of Risk: The caution to implement a change successfully. When assessing risk is calculated based on following factors:

* Number of teams to implement

* Prior change success

* Incident history

* Time to back out

* Implementation window

* Risk to the business

* If redundancy, then risk goes down. If no redundancy, then risk goes up.

*If known impact during change window, then risk goes down. If impact not known/educated guess, then risk goes up

Note: At the current time, business risk is not calculated within the Change form nor documented unless by the requester within description and/or impact of the Change. However, please consider the risk to the business, of not implementing the change. Some common types of business risks include strategic, financial, clinical operations, compliance, and any other contributing factors that could have a negative impact on the business.

Change Type: A system-calculated categorization of a Change, based on its lead-time and Change Subtype. The Change Type is calculated by ServiceNow by comparing the lead time to the current time for a Change based on the Change Subtype. Options are:

- **Normal –** Used to introduce a new service or to improve or retire a service.
- **Expedited –** Used to resolve degradation of a service. Other Changes categorized as Expedited due to improper lead time are perceived as lacking proper planning.
- **Emergency –** Used to resolve a service interruption (Incident, Major Incident, or Crisis).
- **Pre-Approved –** Used to streamline the process for making normal, routine Changes that can easily be backed out. Assigned based on selection of the associated check box.

Change Freeze: A block on Production Changes impacting entities or facilities, applications, and resources during the major event window. Can be either Enterprise or Site Specific. Freezes can be the result of an inspection from a regulatory agency or major additions to the Mass General

Brigham environment, such as new affiliates, major hardware implementations, or facilities maintenance which temporarily removes desired redundancy.

Leadership Approval: An additional level of approval required to implement a Change during a Change freeze. Includes sign off by S. Flammini (Vice President and CTO, Digital) and T. White (Vice President, Infrastructure Technology Services, Digital).

Compliance: A compliant Change is a well-prepared and executed Change. It clarifies what, why, and how the Change is being executed and is reviewed by the requester after implementation. Change Management reviews all Significant and Major Changes for compliance before they are scheduled for a Change Control Board meeting as well as after implementation.

Configuration Item (CI): Any component that needs to be managed in order to deliver a service. CIs are controlled through the Change process and stored in the Configuration Management Data Base (CMDB).

Crisis: An incident of significant enough disruption to the business that Leadership deems it a Crisis.

Emergency Change Control Board (eCCB): A subset of the Change Control Board for reviewing Expedited and Emergency Changes, as needed.

End User: This person uses IT Services on a day-to-day basis in order to achieve their desired business outcomes.

Incident: An unplanned interruption to a service or a reduction in the quality of a service.

Major Incident: An incident of significant enough disruption to the business that Leadership deems it a Major Incident.

Maintenance Schedule (Window): A designated time period when maintenance-related Changes are scheduled to be made to a specified Configuration Item (CI).

Post Implementation Review (PIR): Review of a completed Change. The PIR should note any issues or steps taken. A PIR is required to be completed within 5 days after implementation of any Major, Significant, or Emergency Change.

Release Management: The flow of Changes through various pre-production environments, culminating in the successful deployment to production in the least disruptive manner.

Request for Change (RFC): An RFC can be entered in ServiceNow or via the Service Desk home page by any Mass General Brigham user to initiate a Change. RFCs can be entered by business users who do not have all of the required information or who may not even know what his or her specific needs might be. It can also be used between Digital groups or even within a single group, if required by team policy. If approved by the Assigned Group identified on the RFC, ServiceNow automatically generates a Change, transferring applicable information.

ITSM Process Roles

ITSM Process Roles are defined by the set of responsibilities, activities and authorities granted to a designated person, team or group. One person can be accountable for multiple roles. The identified roles within the Process are defined below:

Process Owner

Profile	This role is accountable for ensuring that the process is being performed according to the agreed and documented process and is meeting the aims of the process documentation.
Responsibilities	• Primary designer of the ITSM Process • Define appropriate standards to be employed throughout the process • Define and approve KPIs to evaluate the effectiveness and efficiency of the process and design reporting specification • Ensure that quality reports are produced, distributed and utilized • Review KPIs and take action required following the analysis • Address any issues with the running of the process • Review opportunities for process enhancements and for improving the efficiency and effectiveness of the process • Ensure that all relevant staff have the required technical and business understanding; and process knowledge, training and understanding and are aware of their role in the process • Ensure that the process, roles, responsibilities and documentation are regularly reviewed and maintained • Communicate process information or changes as appropriate to ensure awareness • Review integration issues between the various processes • Integrate the process into the organization • Promote the Service Management vision to top-level/ senior management • Function as a point of escalation when required • Ensure that there is optimal fit between people, process, technology/tool and steering • Ensure that the process is fit for purpose
Key Outputs	• Ensures the process is available, accurate, and meets organizational needs. • Obtains End User feedback. • Promotes the process within Mass General Brigham
Authority	• Approves changes to process • To escalate any breaches of the Process to higher management levels • To take action as a result of any process non-compliance • To organize training for IT employees and nominate staff for training. • To escalate to management remedial training needs • To negotiate with the relevant Process Owner if there is a conflict between processes

Change Manager

Profile	Manages the activities of the Change Management process for the Mass General Brigham Digital organization. This individual focuses on the process as a whole and not on any individual Change. However, the Change Manager is involved in every step of the process – from receipt of the RFC or Change to the implementation of the Change.
Responsibilities	- Ensure Changes and RFCs are properly recorded in the ServiceNow Change Management application. - Issue an agenda of RFCs and Changes to be reviewed, discussed, and approved to CCB members in advance of meetings. - Review all Changes for compliance. - Present all RFCs and Changes at CCB meetings. - Chair all CCB meetings. - Review and evaluate the Change process.

CCB (Change Control Board) Members

Profile	Provides expert advice to Change Management on the implementation of Changes. It includes representatives from all areas within Mass General Brigham, including site leadership, configuration owners, application owners, technical leadership, as well as any individual with stakeholder interest.
Responsibilities	- Review submitted RFCs and Changes prior to weekly meetings. Work with the Change Manager or Change Requester with any questions or issues prior to the meeting when possible. - Assess, approve, or reject Changes. Provide guidance requiring any technical questions that need to be considered prior to approval. - Assist in the coordination of Change schedules to avoid conflicts with other established events. *Note: Prior to February 2021, the "CCB" was labeled the "CAB."*

eCCB (Emergency Change Control Board) Members

Profile	Provides expert advice to Change Management on the implementation of Emergency and Expedited Changes that cannot be reviewed by the CCB. A subset of the full CCB.
Responsibilities	- Assess, approve, or reject Changes. Provide guidance requiring any technical questions that need to be considered prior to approval. - Assist in the coordination of Change schedules to avoid conflicts with other established events. - Be available for consultation should any Emergency or Expedited Changes be required.

CAB (Change Advisory Board) Members

Profile	Provides expert advice regarding Change Management governance.
Responsibilities	- Strategic oversight of the Change Management process. - Consists of permanent CCB members. - Meets on a regular basis to provide a forum for policy and process update discussions.

Change Owner

Profile	The individual stakeholder ultimately responsible for the end result of the Change, seeing it through its lifecycle. For example, a network engineer may be the Change owner for a router upgrade.
Responsibilities	- Provide details, as required or known, to complete the RFC or Change. - Attend the CCB to answer any possible questions regarding this Change or timing. - Communicate details regarding the Change to appropriate parties, and keep the Change Manager informed throughout the release cycle. - Provide details, as required or known, to complete the post implementation review for Changes.

Change Requester

Profile	The individual asking for the Change to be made. May or may not be the Change owner.
Responsibilities	- Sponsor or advocate for the Change, usually from a Mass General Brigham business perspective. - Provide details, as required or known, to complete the RFC or Change.

Release Manager

Profile	Manages the activities of the Release Management process for the Mass General Brigham Digital organization. This individual focuses on the process as a whole and not on any individual Release.
Responsibilities	Review and evaluate the Release Management process.

Process Activities – Change Management

The following section describes major procedures of the Change Management process. Note that there are two different potential workflows, depending on how a Change is initiated: by Request for Change (RFC) or by manual entry of the Change.

The RFC process is used by business users as well as Digital to request that a change be made. It is used when the requester does not have all of the required information or may be a required per team policy.

The Change process is used by licensed ServiceNow users to directly enter a Change, bypassing the request activities (Request and Assignment Group Approval).

- If initiated via a Request for Change (RFC):

Request → Assignment Group Approval → Draft → Awaiting Approvals → Awaiting CCB → Awaiting Implementation → Implement → Support → Close
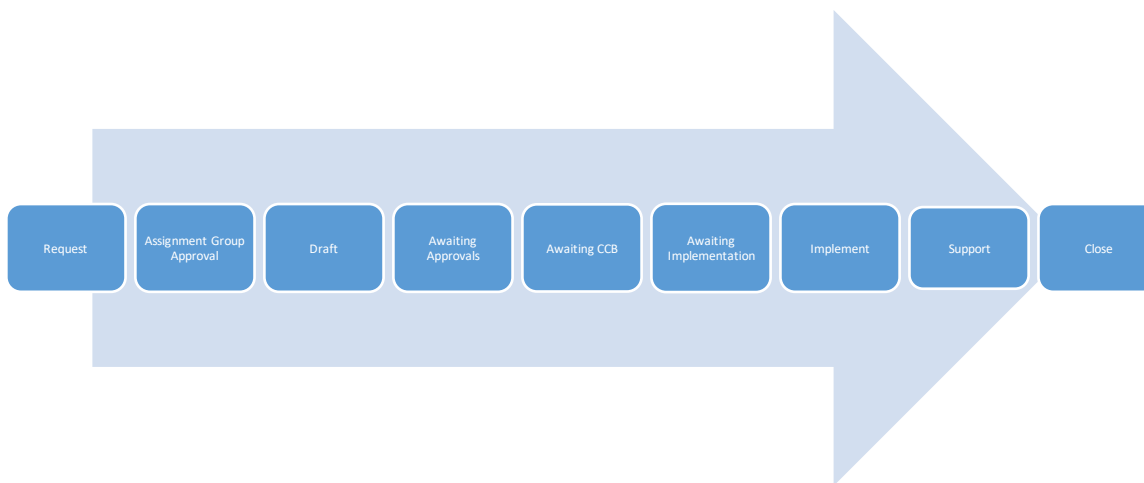
- If initiated via a Change:

Draft → Awaiting Approval → Awaiting CCB → Awaiting Implementation → Implement → Support → Closed
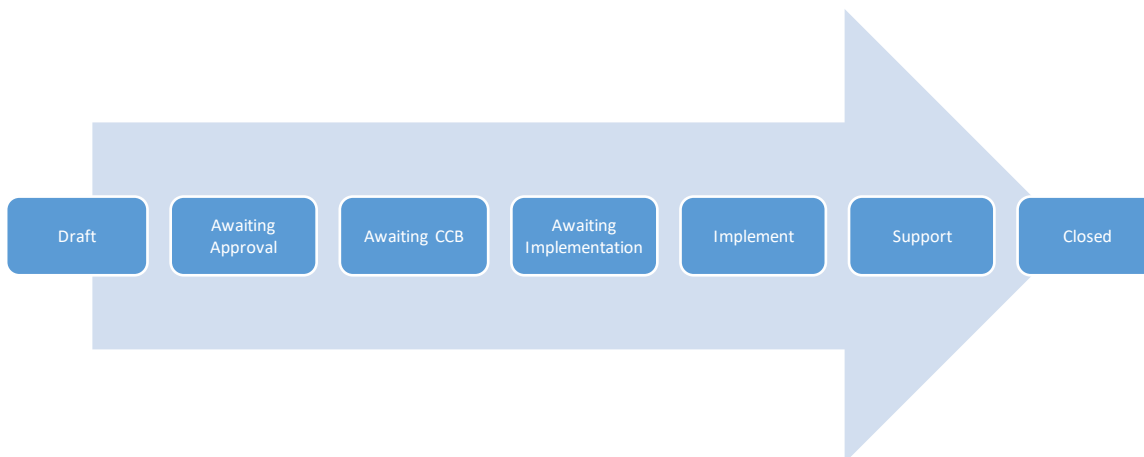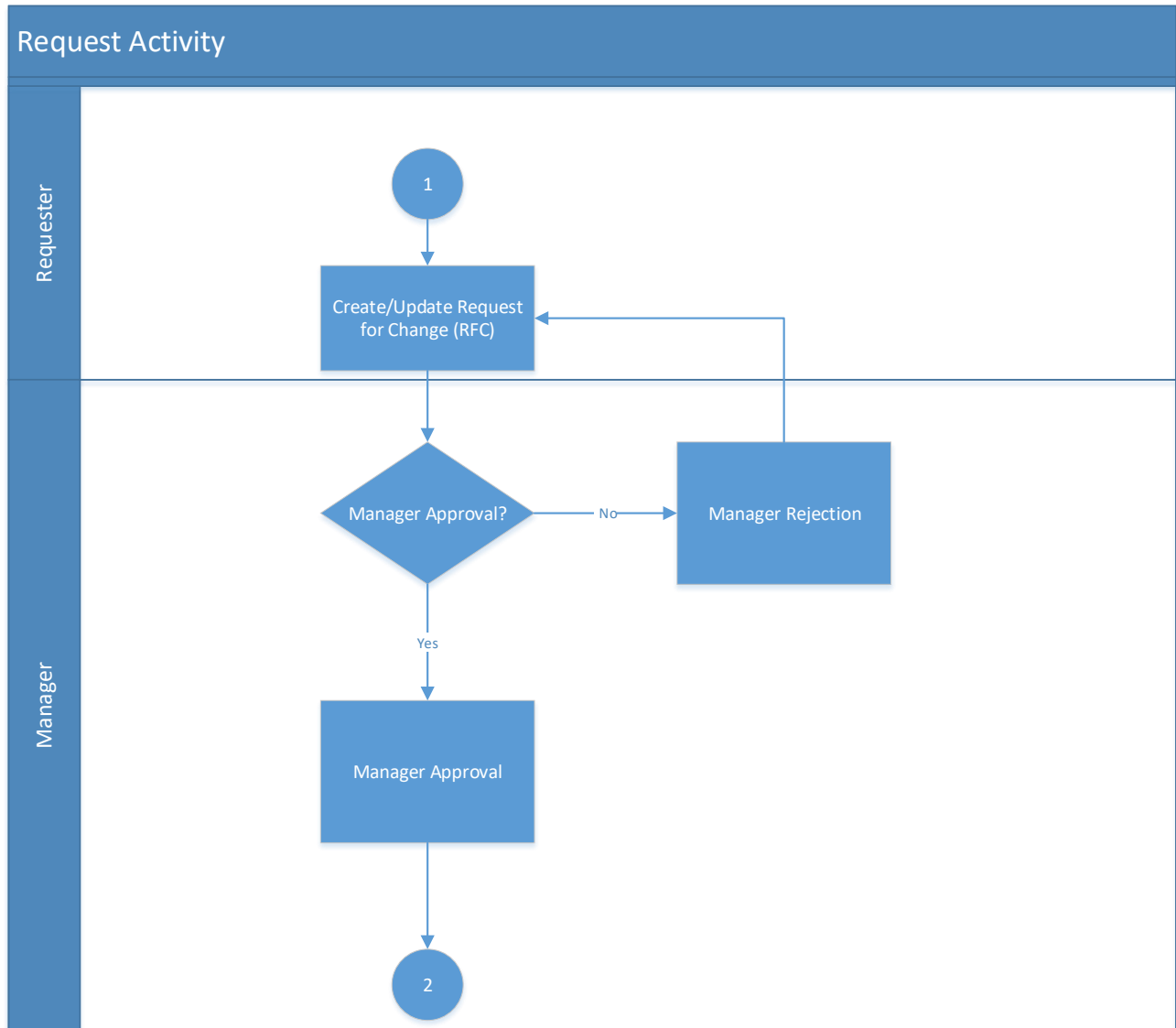
Request Activity

Activity	Request
Purpose	Provides business users and Digital with a process for requesting a Change.
Outcome	Provides a process within ITSM to respond to the needs of the business.
Triggers and Inputs	Identification of a business or technology need.

Procedure Steps	● Requester uses the Request for Change option in ServiceNow to initiate an RFC. ● Requester completes all fields, including "To which group is this to be assigned" (Assignment Group), and clicks to submit the request. ● The Requester's Manager accepts or rejects the RFC.
State	Requested
Owner	Requester
Outputs	If approved by the Requester's Manager, the RFC is sent to the Assignment Group for review.

Activity	Requester	Requester's Manager	Change Process Owner	Change Manager
Request	R	A	I	I

Assignment Group Approval Activity

Assignment Group Approval Activity

Requester

Update and resubmit

Assignment Group

2

Assignment Group Review of RFC

Approve Request?

No → Assignment Group Rejection

Yes

Assignment Group Acceptance

3
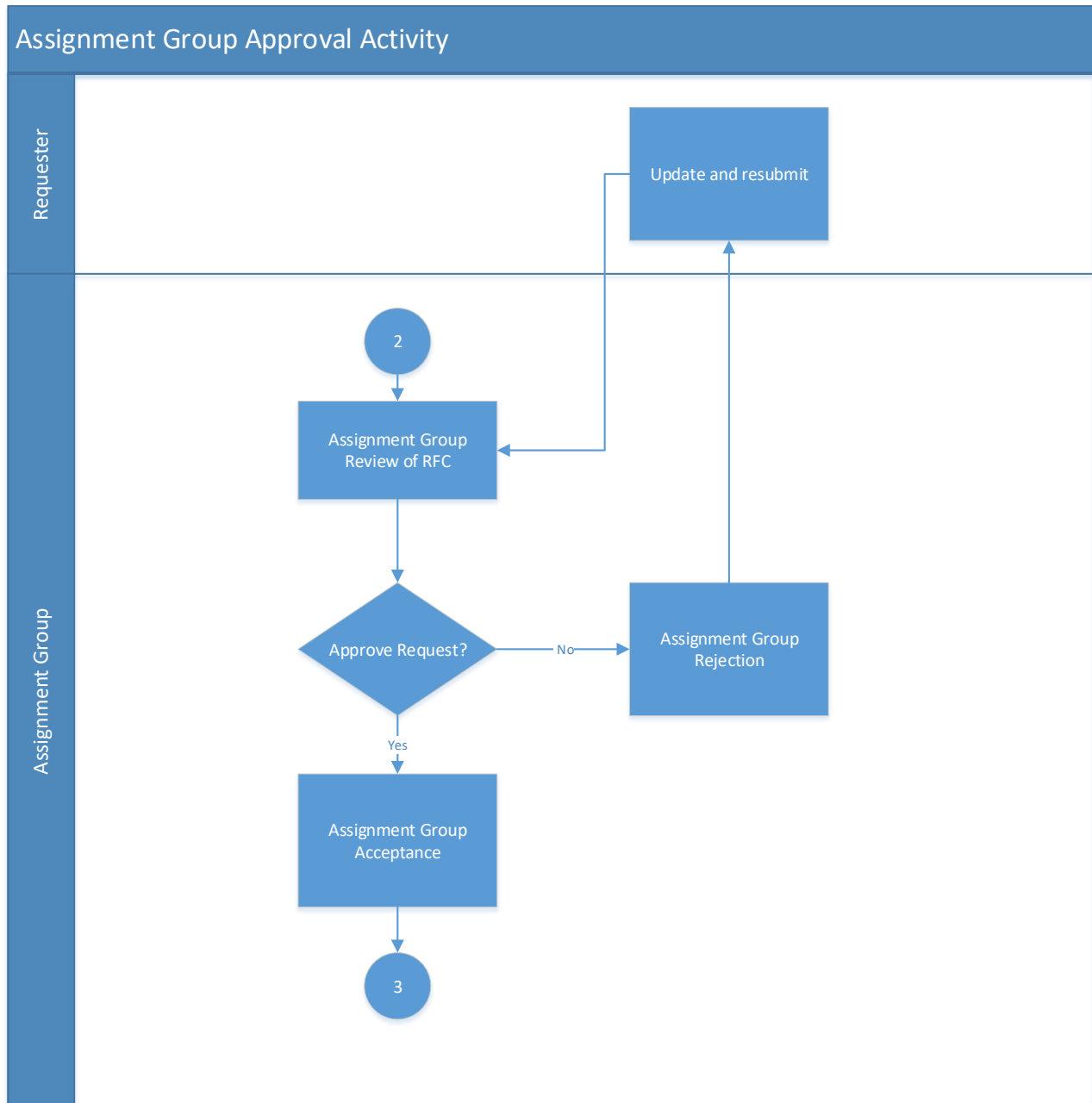
Activity	Assignment Group Approval
Purpose	Provides business with a technical review of a request prior to initiating a Change.
Outcome	Business dedicates resources to Changes deemed appropriate to pursue.

Triggers and Inputs	Submittal of an RFC to a designated Assignment Group.
Procedure Steps	● An email notification is sent to a Digital group identified as the Assignment Group in an RFC. ● User from the Assignment Group uses the My Open Changes option in ServiceNow to access the associated Change. ● User from the Assignment Group either accepts the Change (assuming the role of the Requester) or rejects the Change.
State	Approved
Owner	Assignment Group
Outputs	If approved by the Assignment Group, ServiceNow transfers information from the RFC to a Change. The Assignment Group assumes the role of the Requester.

Activity	Requester	Assignment Group	Change Process Owner	Change Manager
Assignment Group Approval	A	R	I	I

Draft Change Activity

Important: For Changes entered directly by ServiceNow users, the Draft activity may represent the starting point. For Digital teams with ServiceNow authorization, the previous activities (Request and Assignment Group Approval) are left to the discretion of internal team policy.

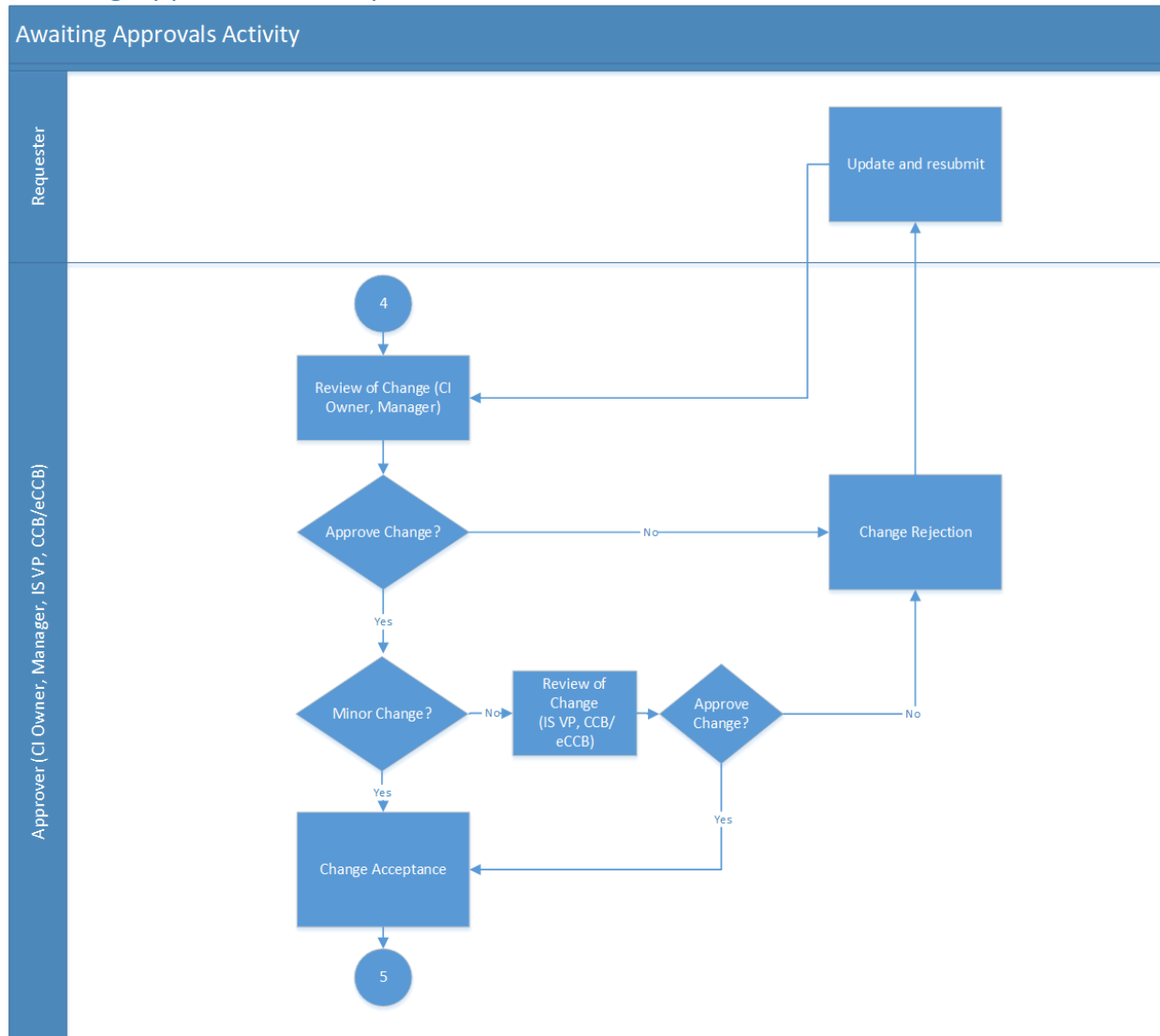| Activity	Draft Change
Purpose	To provide a method for documenting changes to the Mass General Brigham environment. Changes can either be directly submitted by authorized users or generated from previously accepted RFCs.
Outcome	Documented Changes are either submitted directly for implementation or sent for review and approval.
Triggers and Inputs	Direct input into ServiceNow by an authorized user or Assignment Group acceptance of an RFC.
Work Instruction Steps	● If an RFC is accepted by the Assignment Group, the Change is generated automatically by ServiceNow, with information from the RFC transferred to the Change. Otherwise, the requester uses the Create Change option in ServiceNow to initiate the Change. ● Requester completes all required fields, including the Start/End Date and time and Change Subtype. ServiceNow uses this information to assign the Change Type. ● Requester clicks to submit the Change.
State	Draft
Owner	Requester
Outputs	Depending on the Change Type assigned to a Change, it may be submitted for implementation or sent to the CCB/eCCB for approval. Minor Changes proceed to the Implement activity (except during freezes).

Activity	Requester	Requester's Manager	Change Process Owner	Change Manager
Draft Change Request	RA	I	I	I

Awaiting Approvals Activity

Activity	**Awaiting Approvals**
Purpose	Provides business with a comprehensive review and communication of all aspects of a Change.
Outcome	Avoid inefficient use of resources due to inadequate technical review, conflicts with other scheduled events, lack of coordination with other interested stakeholders (business and technical), improper testing and planning; ensure Changes conform to business standards and policies.
Triggers and Inputs	Submittal of a Change for review.

Procedure Steps	• Submittal of a Change request in ServiceNow generates notification of Change to all responsible reviewers. This includes, but is not limited to the Requester's supervisor; Configuration Item Owners and interested parties, and others noted on the Change; and – for Major and Significant Changes - the associated Digital VP, and the CCB/eCCB. • Reviewers work with the Change Manager or Requester with any questions or issues prior to CCB meetings when possible. • For Changes sent to the CCB, reviewers meet every Wednesday to assess Changes for Major and Significant Changes. Change Manager reviews all Changes scheduled for the CCB for Pre-Compliance. • Assess, approve, or reject Changes. Provide guidance requiring any technical questions that need to be considered prior to approval. • Update the Change, as appropriate.
State	Awaiting Approval
Owner	Reviewer
Outputs	If approved by all reviewers, the Change moves from Awaiting Approvals to Awaiting Implementation activity. If rejected, an email notification is sent to the Requester for remediation.

Activity	Requester	Reviewer (Digital VP, CCB, CI Owner, Requester's Manager, Other)	Change Process Owner	Change Manager
Awaiting Approvals	A	R	I	R

Implement Activity
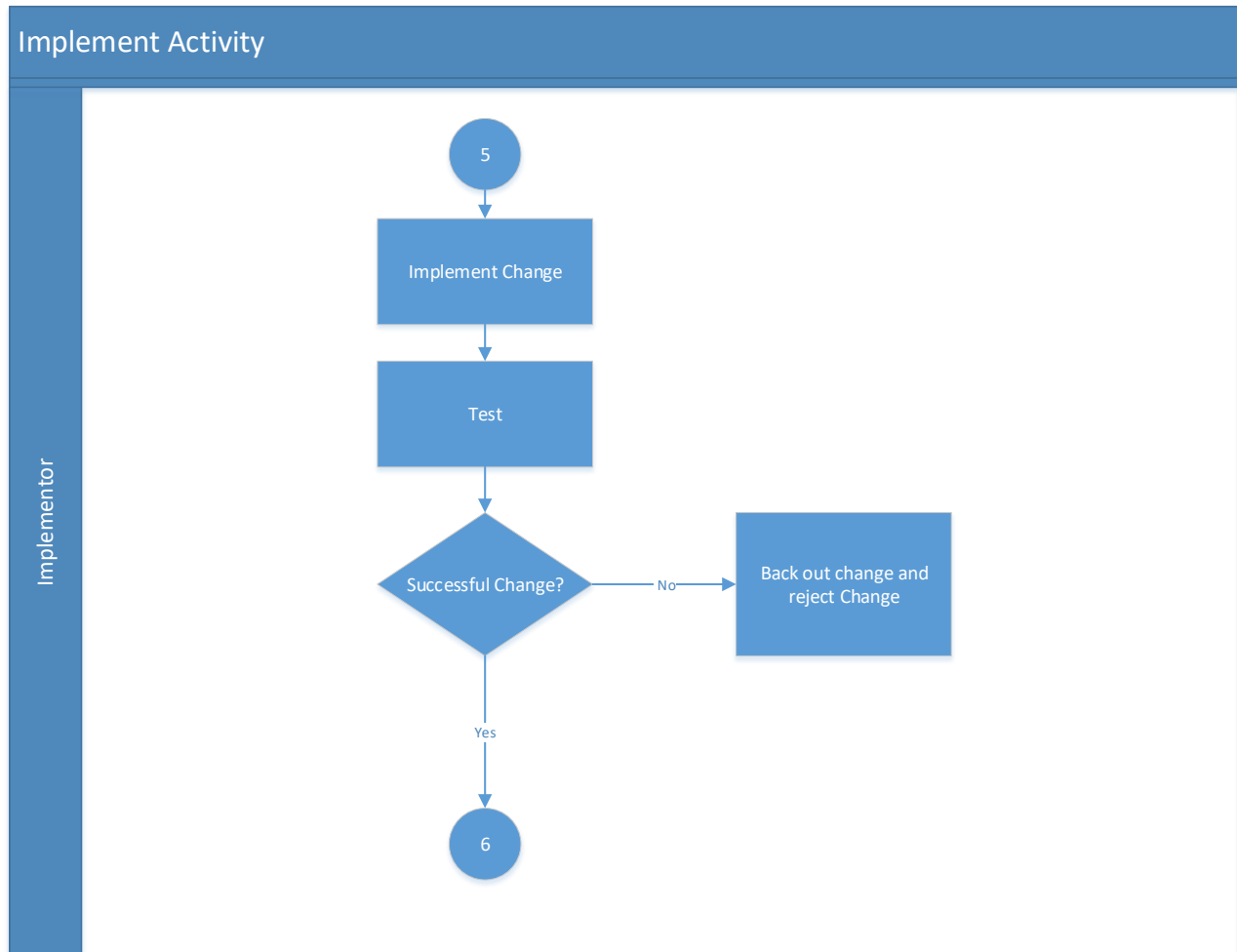
Activity	Implement
Purpose	Ensures that all activities associated with a Change have been completed and the Change can be implemented as scheduled.
Outcome	Change is properly built and tested.
Triggers and Inputs	Approval by all reviewers.
Procedure Steps	- Complete all tasks to build and test the Change. - Update Change, as appropriate.
State	Awaiting Implementation
Owner	Implementor

Outputs	If successful, Change is implemented as scheduled. If not, backout plan for the Change is completed.

Activity	Requester	Implementor	Reviewer (CCB, CI Owner, Requester's Manager, Other)	Change Process Owner	Change Manager
Implement	A	R	I	I	A

Close Activity

Activity	**Close**
Purpose	To examine how the Change was handled throughout its entire lifecycle, and whether it produced the desired results.
Outcome	All follow-up activities for a Change are completed. Opportunities to improve the implementation of similar Changes in the future are tabled and action items assigned accordingly.
Triggers and Inputs	Successful implementation of a Change.
Procedure Steps	● An email notification is sent 3 days after the end date of the Change to request completion of the PIR (Post-Implementation Review) tab. ● Requester completes the PIR tab. ● If not completed within 5 days, the Change is automatically closed, noting missing PIR information. ● Change Manager reviews Changes for Post-Compliance.
State	Closed

Owner	Requester
Outputs	A fully documented Change.

Activity	Requester	Implementor	Reviewer (CCB, CI Owner, Requester's Manager, Other)	Change Process Owner	Change Manager
Close	R	I	I	I	A

Process Activities – Release Management

For Release Management, core activities are focused on the testing that we perform both before and after the release is deployed into our production environment.

Pre-Deployment

A successful Release starts during development. Accordingly, best practice Release Management includes rigorous testing activities:

- Testing should be run in environments that are as close as possible to the production environment
- This includes unit testing (low-level testing of specific functionality), user acceptance testing (testing by and for end users), security testing (to uncover any potential vulnerabilities), and performance testing (to ensure that the Release can hold up under a given workload)
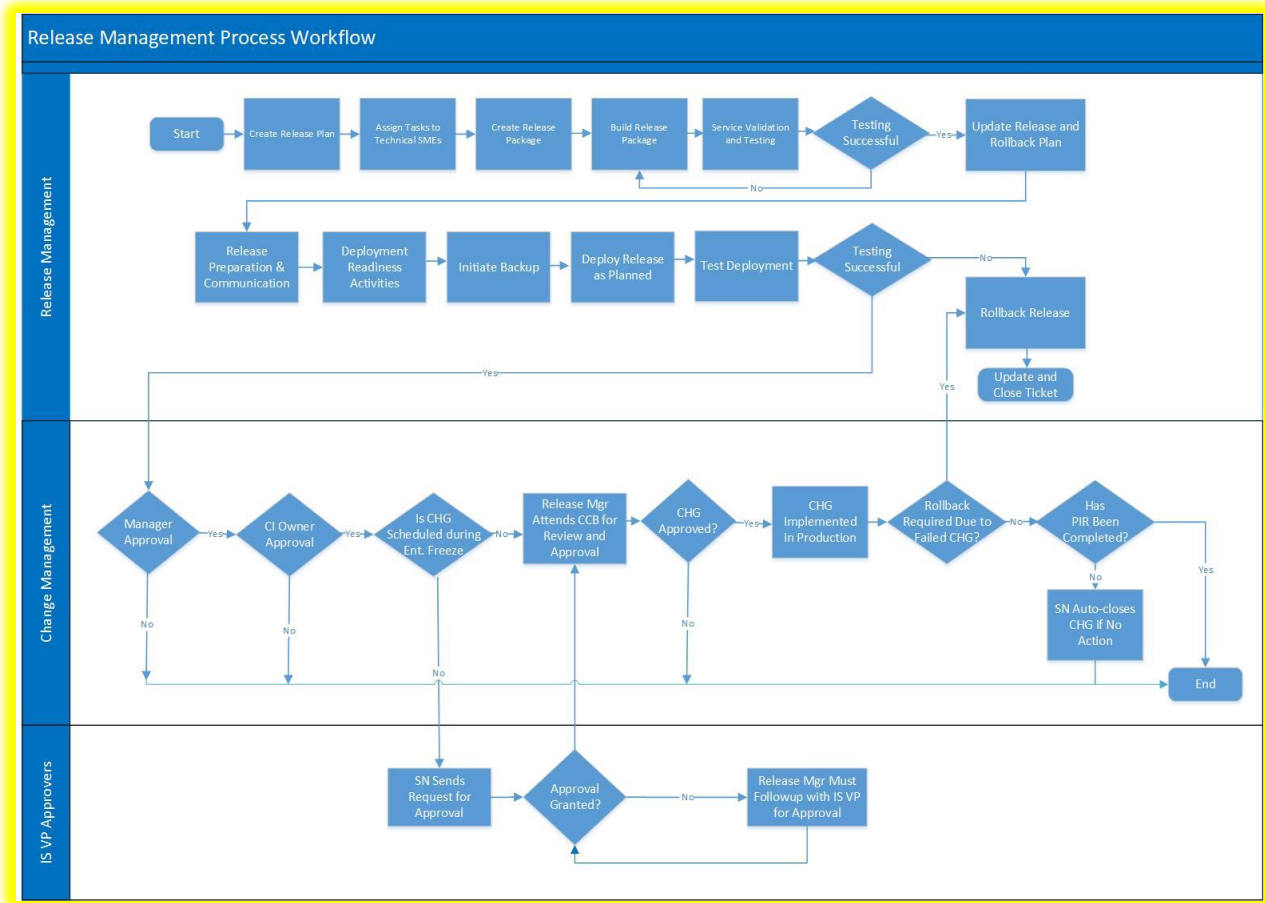
Post-Deployment

As previously defined, successful Release Management ensures resiliency once in production. This is facilitated by effective post-deployment testing:

- For application releases, testing validates that the services work as expected by our business users
- For infrastructure releases, testing is coordinated with all teams that are dependent on that infrastructure to ensure critical services are not disrupted
- Testing includes smoke testing (a basic test of the most important features of the Release) and regression testing (to ensure that existing functionality still works) to ensure the release does what is designed to do. Often overlooked functionality such as printing is a good example of what an effective regression test should include.

Release Management Phases

There are three phases to release and deployment management:
- **Release build and test -** The release package is built, tested and checked into the DML. This phase starts with change management authorization to build the release and ends with change management authorization for the baselined release package to be checked into the DML by service asset and configuration management. This phase only happens once for each release.
- **Deployment -** The release package is deployed to the live environment. This phase starts with change management authorization to deploy the release package to one or more target environments and ends with handover to the service operation functions and early life support. There may be many separate deployment phases for each release, depending on the planned deployment options.
- **Review and close -** Experience and feedback are captured, performance targets and achievements are reviewed and lessons are learned.

Release Management Process Workflow

Release Management

Start → Create Release Plan → Assign Tasks to Technical SMEs → Create Release Package → Build Release Package → Service Validation and Testing → Testing Successful

Testing Successful —Yes→ Update Release and Rollback Plan

Testing Successful —No→ (back to Build Release Package)

Release Preparation & Communication → Deployment Readiness Activities → Initiate Backup → Deploy Release as Planned → Test Deployment → Testing Successful

Testing Successful —No→ Rollback Release → Update and Close Ticket

Testing Successful —Yes→ (down)

Change Management

Manager Approval —Yes→ CI Owner Approval —Yes→ Is CHG Scheduled during Ent. Freeze —No→ Release Mgr Attends CCB for Review and Approval → CHG Approved? —Yes→ CHG Implemented in Production → Rollback Required Due to Failed CHG? —No→ Has PIR Been Completed?

Manager Approval —No→ (down to End)

CI Owner Approval —No→ (down to End)

Is CHG Scheduled during Ent. Freeze —No→ (down)

CHG Approved? —No→ (down)

Has PIR Been Completed? —No→ SN Auto-closes CHG if No Action → End

Has PIR Been Completed? —Yes→ End

IS VP Approvers

SN Sends Request for Approval → Approval Granted? —No→ Release Mgr Must Followup with IS VP for Approval

Critical Success Factors, Key Performance Indicators (KPIs) and Metrics

Change

- Percentage of Successful Changes

- Percentage of Changes Closed by the System

- Number of Changes Awaiting Approval

- Number of Expedited Changes

- Number of Emergency Changes

- Number of Emergency Changes Not Related to Major Incidents

- Number of Major Incidents Caused by a Change

Release

- Number of EPIC Releases that Caused an Incident

- Percentage of EPIC Releases that Were Rolled Back

Supplemental Information

This section includes expectations for vendors working with Mass General Brigham. The Mass General Brigham Supply Chain team includes the following information for contracts related to High Risk Templates:

xx. DIGITAL CHANGE MANAGEMENT:

In the event that Business's software or hardware are utilized as part of Customer's production environment or other environments critical to Customer's technology infrastructure, Business hereby agrees to comply with all applicable Mass General Brigham Digital Change Management requirements found at: https://massgeneralbrigham.org/Vendors/ChangeManagement

This section also includes consolidated workflows for Normal, Emergency, Expedited, and Pre-approved Change Types as well as processing of Changes during freezes.

Vendor Expectations

Importance of Digital Change Management at Mass General Brigham

Digital Change Management is a process based on IT Infrastructure Library (ITIL) principals. This process was designed and put in place to ensure that all technology changes are recorded, tested, accurately scheduled, reviewed, and properly approved prior to implementation. This process is critical to Mass General Brigham. Most of our technology changes could have a direct impact on the safety, security and well-being of our patients, our training programs and medical research that sustain the advancement of medicine, and in our community. If there is an issue with the change when implemented, our Major Incident process can pinpoint what changed and when, and then begin immediate resolution to restore service.

Vendor Responsibilities Making Changes to Our Production Environment

- Vendors must adhere to all Mass General Brigham Digital Change Management processes and procedures when their software and hardware are utilized as part of our production environment, or other environments deemed to be critical to the infrastructure in our technology space. Vendors should work with their respective Digital contact to ensure all Digital Change Management processes and procedures are properly followed. If a Digital contact is not yet identified, please contact changemanagement@partners.org.
- Vendors must work with Mass General Brigham Digital personnel to notify them when maintenance or modifications of any kind are required in our enterprise or site-specific computing environments, so that our personnel can properly coordinate the work and communications, if necessary, per our operational processes and procedures.
- All changes required on vendor-owned hardware and software will be scheduled, reviewed, and approved by our Change Advisory Board and covered on our morning calls on Changes of the Day (COD).
- Vendor changes are expected to be scheduled during off-peak hours; in most cases, peak hours are defined as between 7 am and 6 pm (Eastern Standard Time), Monday through Friday. Issues adhering to this requirement should be escalated to our Change Advisory Board.

Scope

For the purpose of this document, changes include the addition, modification, or removal of a supported service or a modification to any software application or associated hardware.
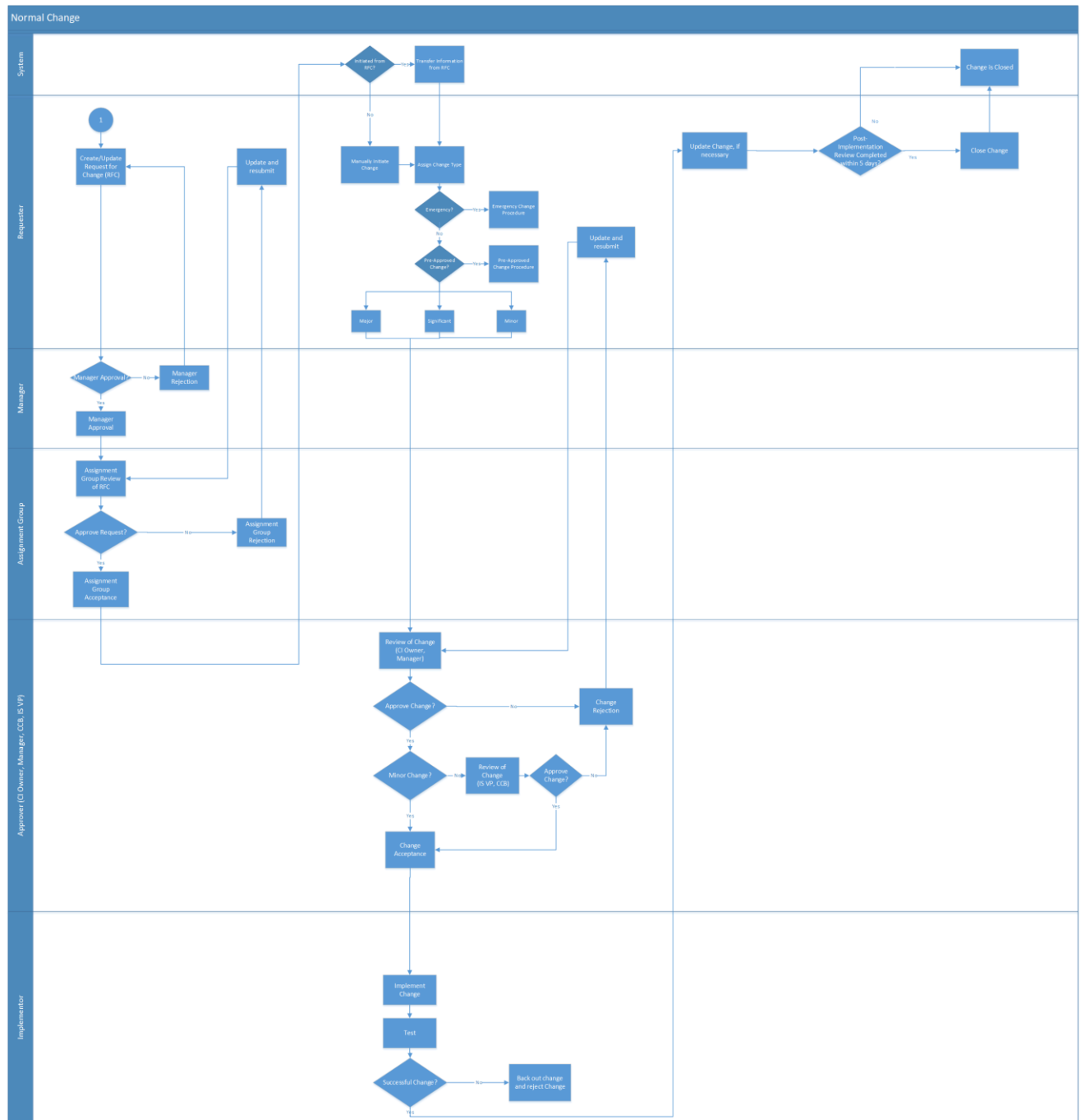
Documentation

Our Digital Change Management process and procedure documentation can be provided to each vendor that makes such a request. This can include information on our process software solution, ServiceNow.
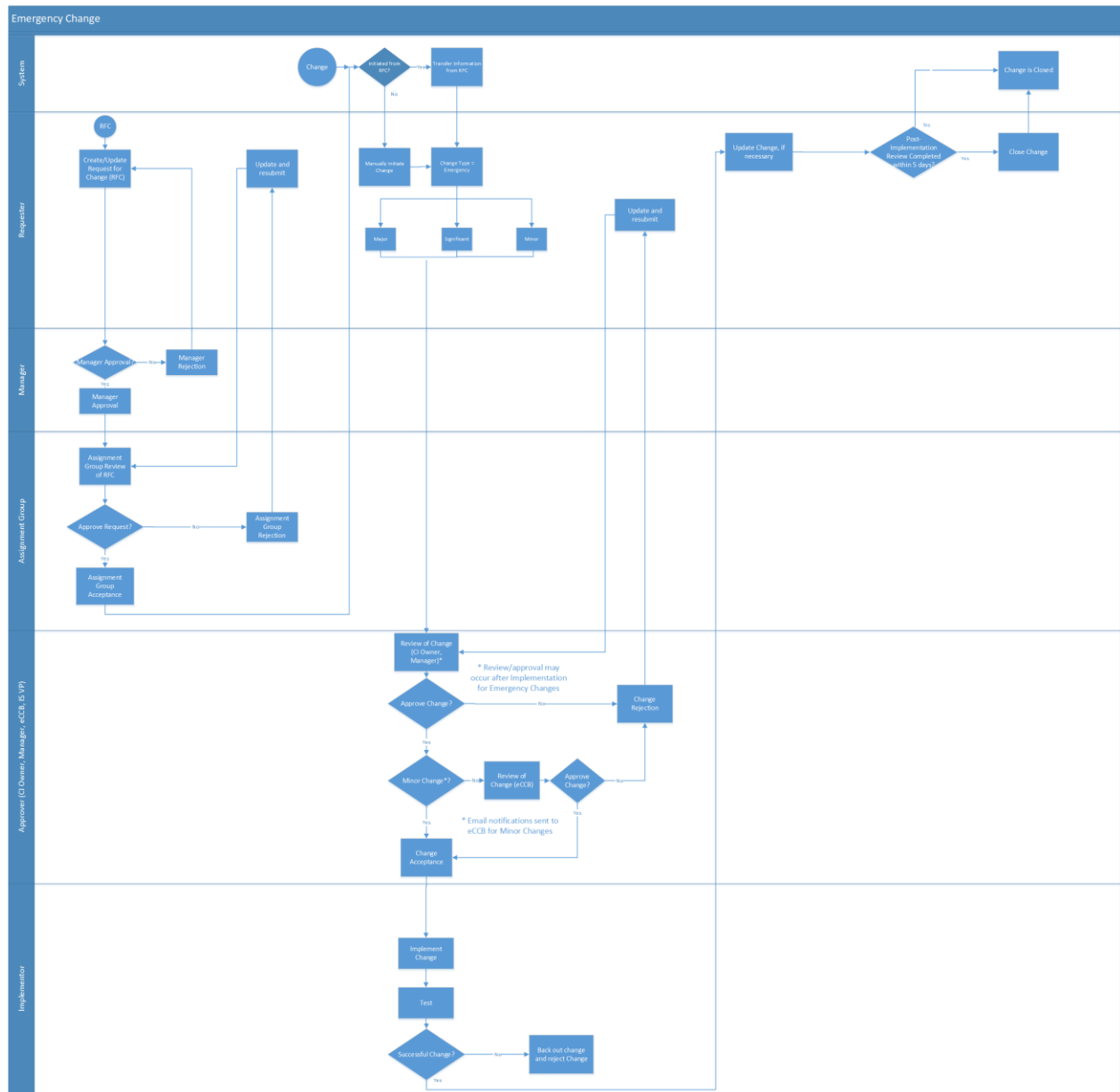
Failure to Comply with Digital Change Management Process

Failure to comply will be reviewed on a case-by-case basis, and in the context of contractual agreements between the vendor and Mass General Brigham.
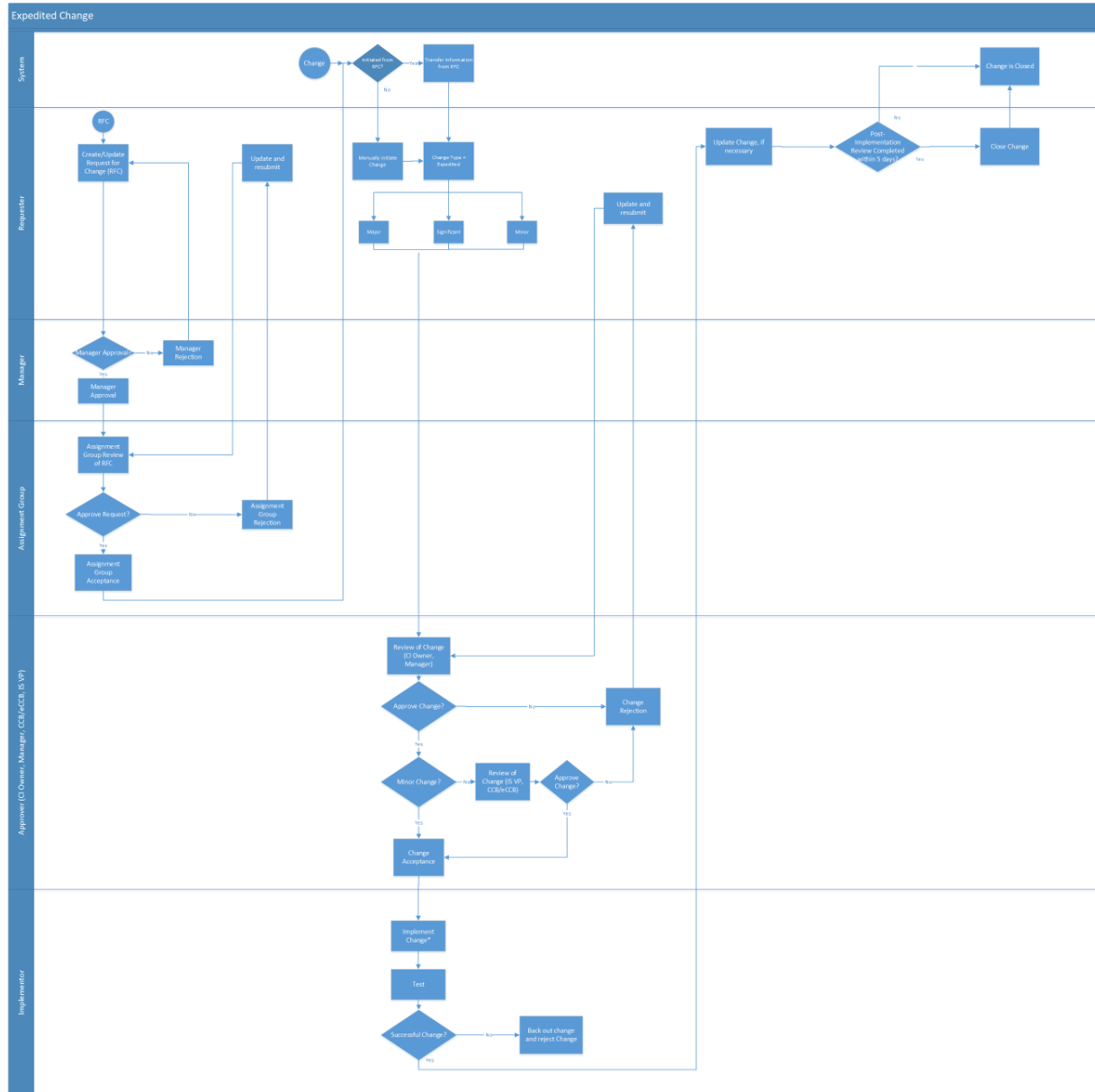
Normal Change

Emergency Change