



Management Environment Software Change Procedure

Managed Environment Software Change Procedure

Overview

This procedure describes the change management procedures applied to software components in managed environments as described in the Hardware & Software Standards & System Owner Schedule.

Procedure

All changes to software components delivered to Eyecon managed environments must be requested via a Release Installation request in the Eyecon Service Desk project of Eyecon's Task and Bug Tracking System as described in the Hardware & Software Standards & System Owner Schedule.

Release Installation change requests must identify:

- The release version of all changed components (including configuration releases)
- The target environment, for example "EAL Production".
- A customer impact statement identifying if any change will impact a customer's system environment and require coordination (for example "Modified game launch URL for Gamesys game launches"). This information may be used to describe the change to customers and coordinate any updates required prior to installation.
- A regulatory impact statement specifying if a release contains changes which are considered by the AGCC technical standards as a "Routine Change", "New Game", or "Game Update". This information may be used to describe via the AGCC change management system (EDNA) the nature and details of the change for approval prior to installation.
- The release contents either as a text summary, a reference to the individual tasks or to a filter within Eyecon's Task and Bug tracking system which is detailed in the Hardware & Software Standards & System Owner Schedule. This content must identify all software systems, information, database entities, data and hardware that will be changed.
- A change classification of Major or Minor according to the guidelines described in this procedure.
- A justification for the selection of the change classification.
- A risk classification according to the guidelines described in this procedure.
- Any other information deemed necessary to describe the change such as specific installation instructions.

All software builds which update game components must generate a game signature compliant with the requirements specified in the Game Identification Standard.

A description of the workflow steps including approvals and signoffs for software change requests are described in the workflow section of this procedure. Games are not released with the same issues as previous games.

The Delivery Manager must sign off each new game design on the wiki page and send it to the compliance team before providing the game to the test house.

All new games are finalised, have QA signoff and all open issues are resolved prior to delivery to the testing house.

All changes must receive approvals and signoffs prior to installation to a managed environment. Where a change requires certification, this must be verified as part of approving a change.

Controls

The following controls are in place to enforce the above process:

- Access to all source code repositories and JIRA projects must be granted in compliance with Eyecon's Software Development Policy and Information Security Policy.
- All projects must use the Change Management Template setup in JIRA for issues, workflows and screens.
- Change classification and change justification are mandatory on Product Change and Product Bug issue types.
- Each source code repository must enable the Eyecon Bitbucket pre-commit hook add-on to validate commits. The plugin will ensure that:
 - The commit comment matches a specific format (ie Regex: ([A-Z0-9-]*): (.*)), for example "CMT-9:Valid commit comment"
 - The JIRA issue referred to in the comment exists on the specified project.

Certified Changes

Any change which is classified as a 'New Game' or 'Major Change' and has been tested and certified by an approved independent testing laboratory is referred to as a certified change.

Change Classification

All changes to software components must be classified as Minor or Major according to the following guidelines:

- All changes to critical components that do not impact game fairness are considered to be Minor updates.
- All changes to non-critical components are considered to be Minor updates.
- All other changes are considered to be Major updates and must be tested by an approved external Test House.

A non-exhaustive list of example changes and their accompanying change classification is provided in an Example Change Classifications page in the Eyecon wiki.

Change Classification Mapping

Eyecon's operations are governed by the conditions of numerous regulatory licenses with potentially differing requirements and terminology. The following table clarifies the mapping from Eyecon's change management procedures to specific regulatory terms.

Change Type	Potential Impact to Game Fairness	AGCC	UK Gaming Commission	Eyecon Change Classification	Internal Testing Required?	Third Party Testing Required?
New Game	Yes	New Game	New Game	New Game	Yes	Yes
Game Update	Yes	Game Update	Major Change	Major Change: Game update – potential impact to game fairness	Yes	Yes
Game Update	No	Routine Change	Minor Change	Minor Change: Game Update – no impact to game fairness	Yes	No
Platform or Environment Update	Yes	Routine Change	Minor Change	Minor Change: Non game update – potential update to game fairness	Yes	Yes, Sample of Games
Platform or Environment Update	No	Routine Change	Minor Change	Minor Change: Non game update – no impact to game fairness	Yes	No
New RNG	Yes	Game Update	New RNG	New RNG	Yes	Yes. RNG and Sample of Games
RNG Update	Yes	Game Update	Major Change	Major Change: RNG Update	Yes	Yes, RNG and Sample of Games
New or Updated, Non-Critical, Warehouse Component	No	Routine Change	Minor Change	Minor Change: Non game update – no impact to game fairness	No – Check contents of release only	No

Critical Components

Games Team

Backend Components

- Game Server
- Pool Server (Jackpot Engine)
- Carbine Game Engine
- Superbus Game Rules
- Feed Server
- RNG

Frontend Components

- Orion Framework
- Orion Games
- Tamborine Games
- Lamington Games

Distributions Team

- Integration Server
- Bonusing Server

Business Insights Team

- Management Server
- Configuration Server
- Authentication Server

QA Team

- None

Change Authorisations

All Role/Owner and Environment values are references to the System Owner Schedule.

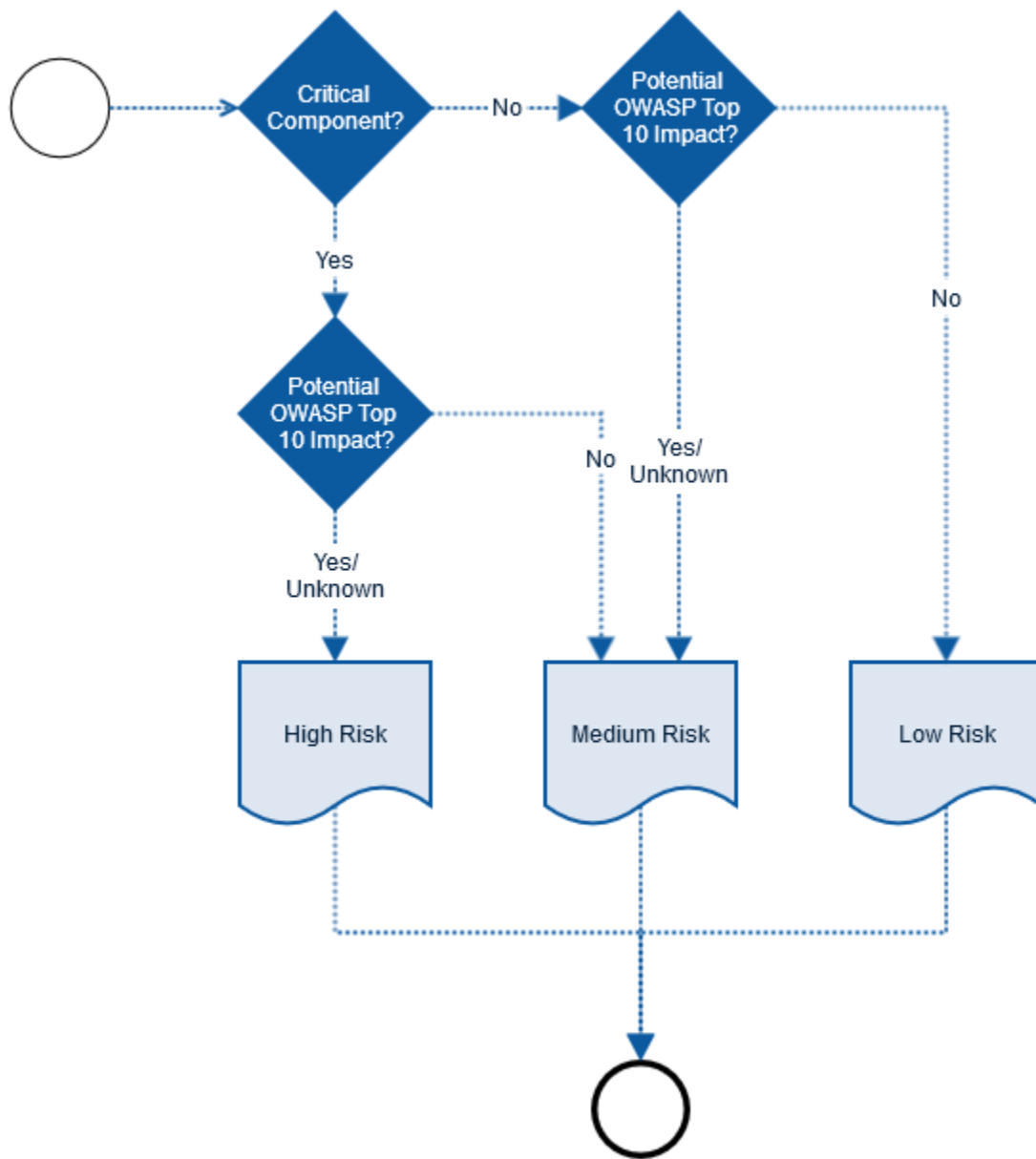
Activity/Approval	Area/Environment	Role/Owner
Request Change	All	Delivery Manager Product Support Manager Technical Principle Development Team Member
Approve Change	QA	QA Lead
Implement Change	QA	QA Team
Approve Change	Compliance Testing	Compliance Officer
Approve Change	All managed environments	System Owner or Delegate
Implement Change	All managed environments	IT Operations Team Member
Approve Change	Development Environment	System Owner

Risk Assessment

This field will inform the QA, Compliance and IT Operations teams of the impact of changes to influence the approval gates defined in this procedure.

A more complex methodology for selecting an appropriate value for this field and the appropriate risk treatment will be developed and made available in this procedure.

Selecting a value for Risk Assessment:



Release Planning

The implementation of all change requests which potentially impact business as usual for all aspects of the business should be coordinated so as to minimise the operational impact of the change. For example, for a

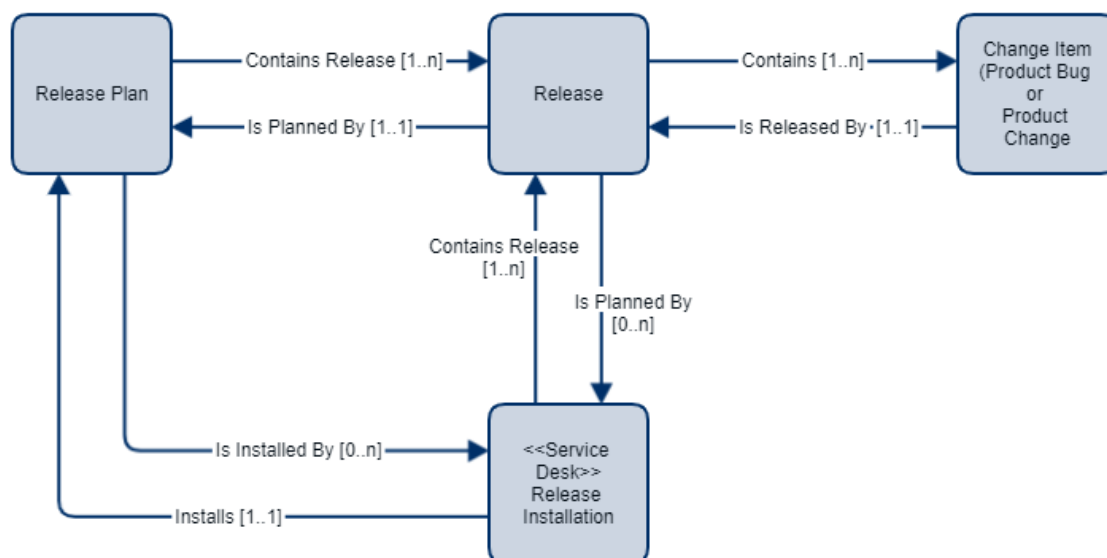
managed environment which operates 24/7/365 this may mean implementing changes during the lowest transaction volume time of day.

A formal release plan will be documented and will contain a reference to all of the changes contained with a particular change.

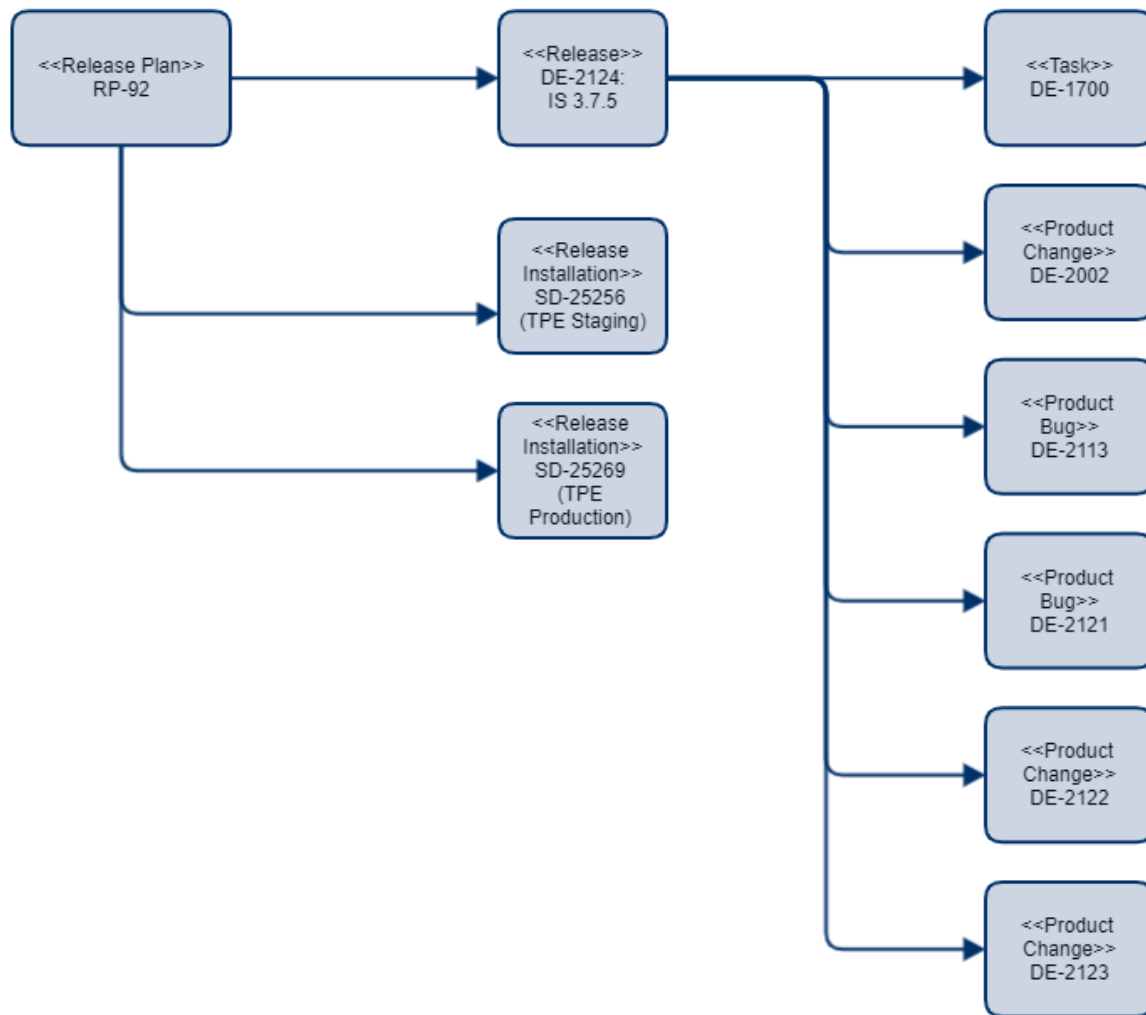
All changes to software will be done with a “Product Bug” or ‘Product Change’ issue type in JIRA. Configuration changes may be completed with a Task type JIRA issue. The release of software versions which contain these changes will be described in a Release issue type. The release plan must contain:

- Implementation Date – Set as the first installation date to a managed environment
- Change Classification – One of the values outlined in the Change Classification section above, selected from available values in dropdown
- Regulatory Reference – The game/multiple games, RNG, etc. which are impacted by either Minor or Major changes contained within the release plan, selected from available values in dropdown (select multiple where appropriate)
- RTS Test Case – Where required under this procedure the results of the RTS Checklist test case attached.

The relationships between a Release Plan, it’s contents (Product Bugs and Product Changes) and the Release Installation requests are described in the following diagram.



Release plan example



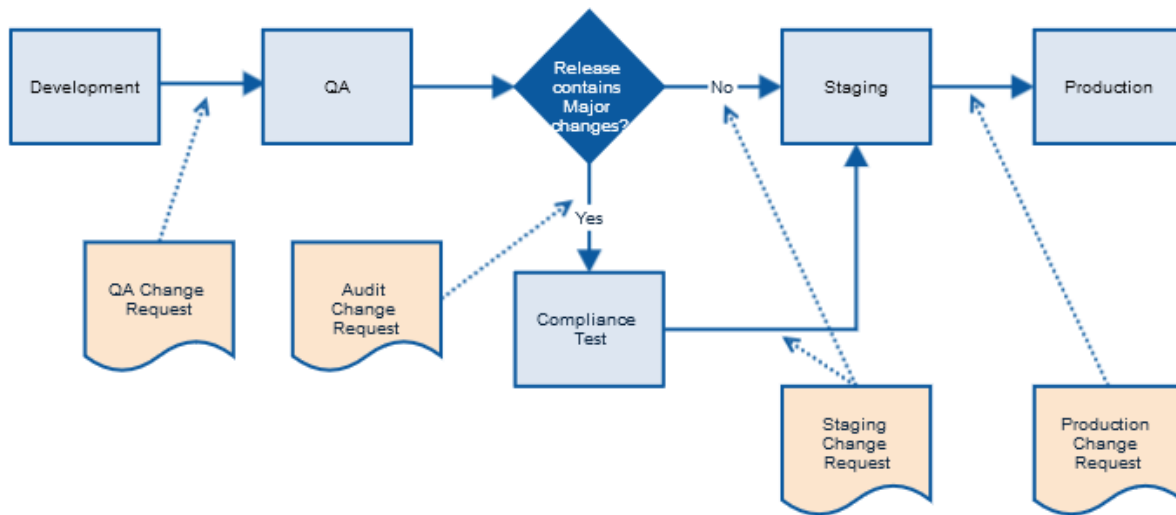
Workflows

The following workflow describes the steps including signoff gates for Eyecon's change requests.

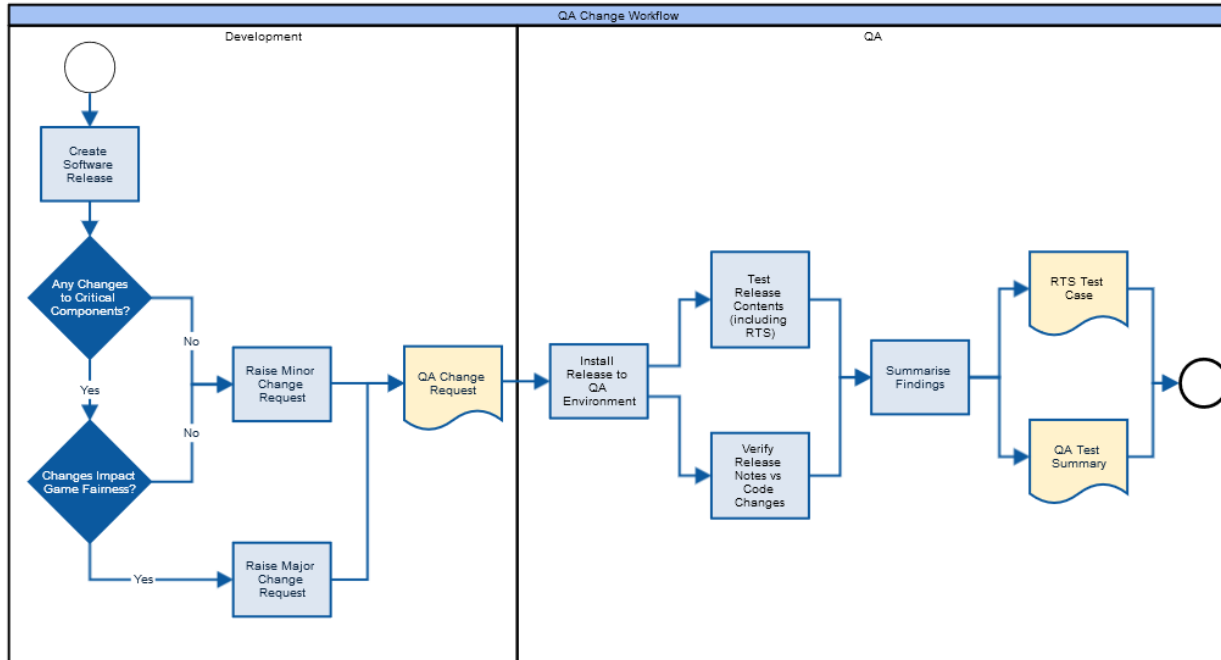
General Lifecycle Phases

A number of change requests are created during the software development lifecycle phases. Eyecon considers an installation of new or updated application servers to a managed environment as defined in the Hardware & Software Standards & System Owner Schedule to be a change. The following diagram highlights the points during the major lifecycle phases where change requests are raised. Eyecon maintains a register of all change requests to managed environments on the Release Tracking section of the Wiki.

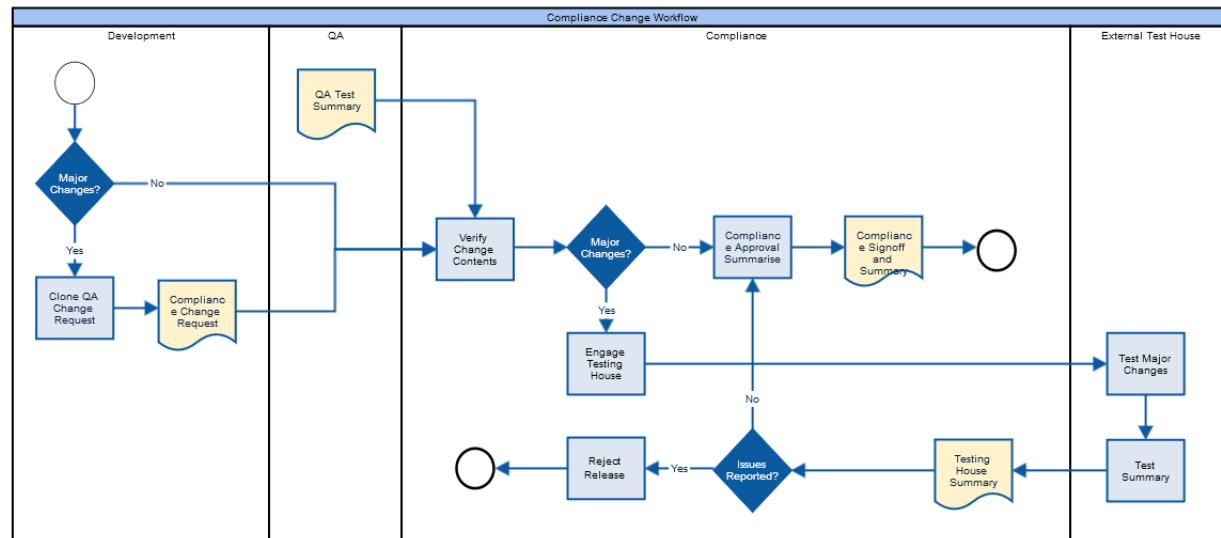
Note: While new change records are created for each development phase the initial QA request is cloned and all details are carried over to subsequent phase change requests.



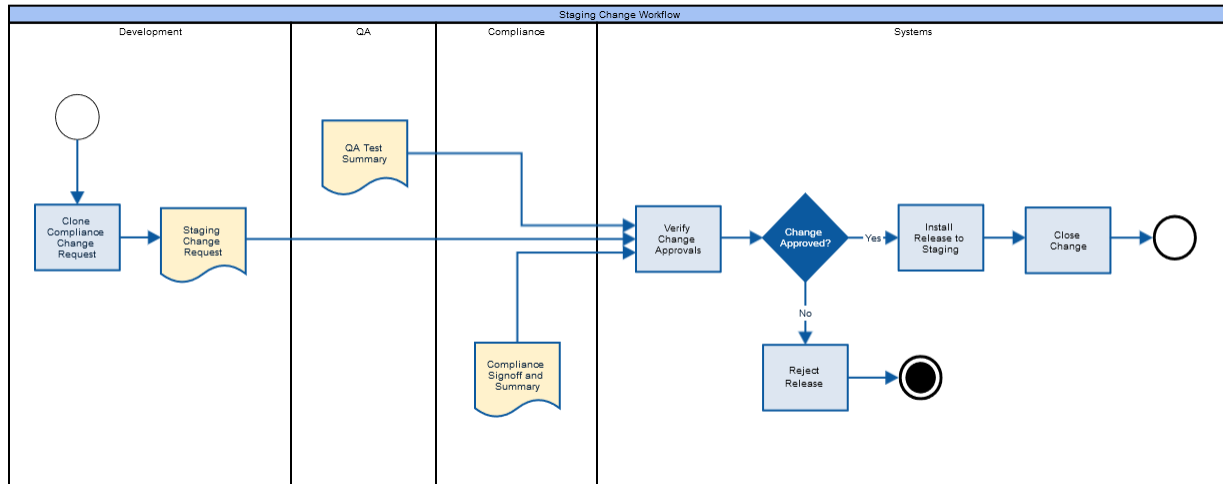
QA Change Workflow



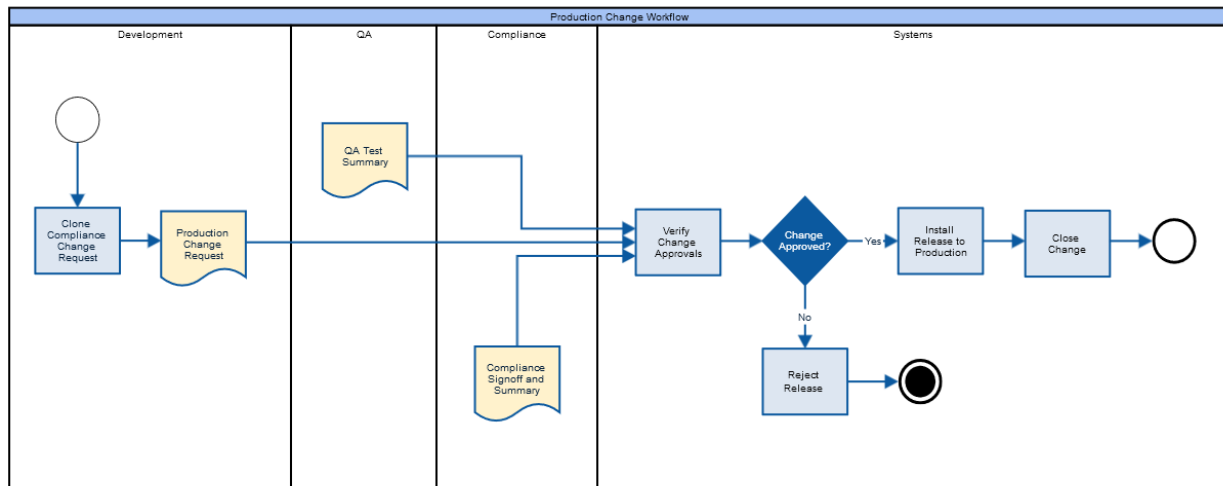
Compliance Change Workflow



Staging Change Workflow



Production Change Workflow



Exceptions:

There will be no exceptions permitted under this Policy.

Consequence for Non-Compliance:

The Company reserves the right to take disciplinary action for a breach of this Policy.

Refer to Eyecon Code of Conduct for guidance regarding disciplinary actions.

References	
Internal References	<ul style="list-style-type: none">• Change Management Policy• Game Identification Standard• Hardware and Software Standards Policy• System Owner Schedule• Example Change Classifications
External References	

Policy Management Section	
Owner	Robert Black
Author	Paul Clarkson
Effective Date	September 2014
Last Review	04.03.2024
Proposed Date of Review	February 2025
Revision	9

Document Revision History			
Date	Revision	Author	Description of Change

12.04.2019	1	DS	Previously approved revision
12.08.2019	2	DS	Migrated standalone policies
14.04.2020	3	DS	Reviewed for accuracy
26.03.2021	4	DS	Reviewed for accuracy
02.03.2022	5	LC	Reviewed for accuracy
19.05.2022	6	PC	Amended change procedure for non-critical warehouse components
03.03.2023	7	LC	Reviewed for accuracy
27.02.2024	8	LC	Reviewed for accuracy
04.03.2024	9	PC	Added 'certified changes' section