# Operational Audit Overview

Introduction

This document outlines the Blue Prism product features that enable the audit of all changes within the platform. The comprehensive audit scope includes changes to the platform itself and also covers changes made to process automations.

User Access Control (UAC) and Environmental Context

It should first be noted that the ability to implement change within the platform is governed by comprehensive User Access Control, which gives System Administrators the ability to control user's roles and permissions within the platform down to a granular level.

This access is defined within the context of each environment - Development, UAT and Production - and is (optionally) governed centrally by means of integration with Microsoft Active Directory.
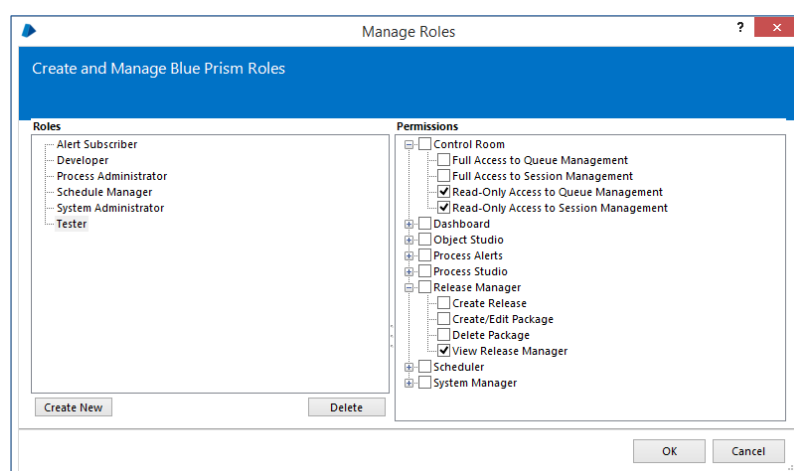
"UAC mechanisms facilitate IT control from a centralised point. This mirrors the central principle of the Blue Prism Framework: operational governance layered on top of architectural guardrails, creating a safe and managed environment for operational efficiency initiatives."

Platform Changes

Changes to the platform itself are audited as well as changes within it. Each event, as well as each change, is audited. This includes the mere action of logging in to the system; changes made to environment variables; changes to users' privileges; the importing and exporting of data; etc. In effect, this means that the System Administrator's behavior is subject to the same level of scrutiny as ordinary users.

Operational Audit

Work items are typically captured in a Blue Prism queue, (except perhaps where an external source is used for workflow). This provides Operations teams with immediate access to case status and outcomes as well as management information on case times, creation & completion dates, etc.

A detailed history of activity on a case by case basis is captured by runtime robots, who record all of their activity in a *session log*. This record includes - for example - every button pressed, every piece of data that is read, every decision made, etc. Where sensitive data is concerned, the logged information can be masked or omitted if necessary in order to comply with data standards such as PCI. The detail of the log relates directly back to the structure of the process diagram, making it easy to interpret by business users.

Process Change and Version Control

Users are required to document their changes each time they save a change to a process and a full version history is captured along with the date/time and identity of the person making each change.
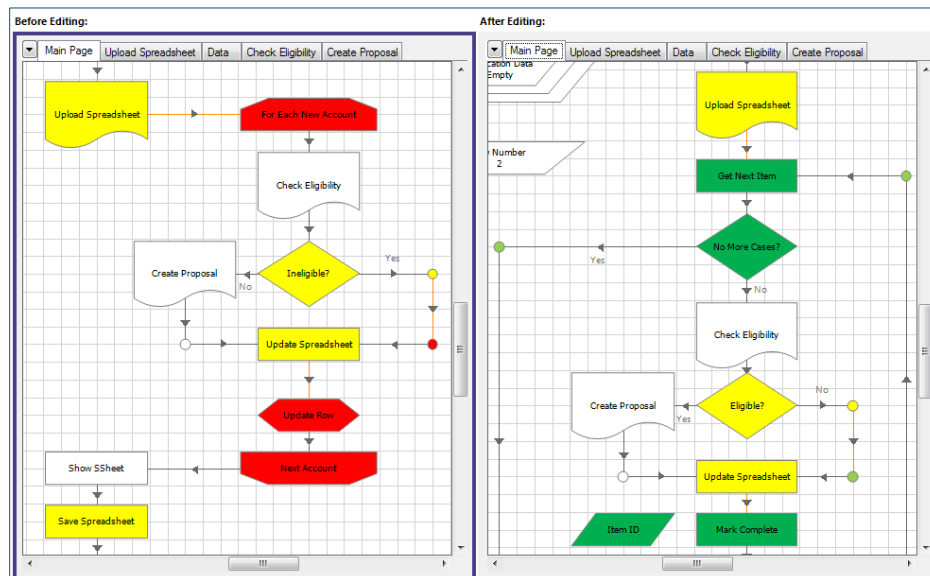
A full visual comparison can be made between any two versions in Blue Prism "Process History" and this uses a red/amber/green convention to highlight deleted/modified/new stages, respectively, as illustrated below.

Process History exists not only as an audit feature but also to facilitate rollback to old versions and to allow the correct interpretation of historic log files against the corresponding process, as it appeared at the time.

Change Management

Process changes are managed in line with the rules and procedures defined in the Agility Framework.

The platform facilitates the proper audit and governance of such changes through a combination of permissions (UAC) and the Blue Prism Release Manager, which provides a secure, audited and managed means of deploying changes from one environment to another – e.g. from Development to Production environments.

The Release Manager takes the form of an intelligent wizard that helps the user to wrap all of the components and dependencies of an automation into a single unit, allowing changes to be implemented atomically.

The resulting package is exported in an open xml-based file format which can be stored and versioned in independent repositories, if required.