Change Control Policy

Pieter Smith

SECURITY EXCELLENCE | Bidvest PROTEA COIN

Contents

1.1 Introduction

The purpose of this document is to establish the BPC IT's change management policy and procedures. This policy ensures that any changes to the operating environment are managed through a process that reflects best practices for the implementation of change management within the IT environment in a manner that safeguards the confidentiality, integrity and availability of BPC's information systems.

1.2 Document Location

This document is amended by the distribution of new revisions of all or part of the document to the named holders. The history of amendments is recorded below.

Revisions	Location	Authorised
Archived	IT – General\Policies\Policies and SoP\Archived	Pieter Smith
Current	IT – General\'Policies\Policies and SoP\Change Control	Pieter Smith

Copies of this document other than those listed above will not be revised; such copies are marked as UNCONTROLLED.

1.3 Scope

This policy applies to all changes in the BPC IT environment. Whether being implemented by BPC employees or contractors (collectively referred to as personnel in this document).

1.4 Roles and responsibilities

1.4.1 Group IT Manager

- Approve BPC's IT change management policies and procedures.
- Appointing members to the CAB.
- Approve all change requests in the IT environment.
- Ensuring the CAB adheres to change management procedures.

1.4.2 CAB members

- Review all changes throughout the development and operational lifecycle of products and systems after ensuring the changes are held to approved criteria before implementation.
- Ensuring that changes are processed in an orderly and consistent manner.
- Overseeing how proposed changes could affect the functionality and secure state of the information systems.
- Providing subject matter expertise to the Group IT Manager as required to assist with performing the Security Impact Analysis.

1.4.3 Change requestors

- Owning the RFC from creation to closure, which includes
    - Generating and submitting the RFC to start the process.
    - Providing all the details that must be included in the RFC (see Appendix A).
    - Attending CAB meetings as necessary to assist the CAB with deliberation on the change.
    - and shepherding the authorized RFC through implementation and validation post-CAB.

1.5 Compliance

For BPC employees, failure to comply with the procedures identified in this plan may result in progressive discipline up to and including dismissal. For non-employees and contractors, failure to comply may result

in removal of the individual's ability to access and use BPC data and systems. Employers of non-BPC employees will be notified of any violations.

1.6 Procedures

The following change management procedures apply to all changes to the IT infrastructure and production environments.

1.7 RFC classification

All documentation associated with change management is maintained in the ticketing system. The change requestor must provide all the required documentation within the ticketing system for an RFC to be considered complete and the change request may only initiate RFCs on those components of the information system for which they are qualified and authorized to access for purposes of initiating such changes, including upgrades and modifications.

There are three types of RFCs:

1.7.1 Normal change

A normal change is one that meets the defined lead time for testing and validation and is assigned a risk level of no, low, medium or high. A normal change is an RFC that is not an expedited or emergency change and is subject to the full change management review process, including review and authorization by the CAB and is typically implemented in regular predefined maintenance windows.

1.7.2 Expedited change

An expedited change does not meet the lead time requirement for a normal change but is not an emergency change. Service is at risk, although service might not be down and the RFC needs to be authorized because of a client request that has been validated by SME/technical expert or an executive, who has determined that that the change needs to go in without waiting for the recommended lead-time/maintenance window. The same 'normal' change request information is provided in the ticketing system to implement the change, including the reason for expediting the RFC (risk level, back-out plans, scheduled time and downtime required), but lead times are much shorter. Authorization by a CAB member is required, and expedited changes are subject to retroactive review by the CAB.

1.7.3 Emergency change

An emergency change is one that must be implemented as soon as possible to correct, or prevent, a high priority incident, or that must be introduced as soon as possible due to likely negative service impacts or situations where the impact to a service is imminent if action is not taken. These changes do not follow the complete lifecycle of a normal change due to the speed with which they must be implemented and authorized. All emergency changes are authorized by the Group IT Manager and documented and entered in the ticketing system prior to implementation, or as soon as possible after the change has been implemented depending on the nature of the emergency. Emergency changes are subject to a post implementation review process by the CAB.

1.8 Process

1.8.1 Normal change - Infrastructure

Change requestors must use the latest template (see Appendix A) and complete it in full. This document is then submitted for approval via the ticketing system. Approvals via email is also accepted if it is recorded in the ticket. The change requestor's divisional executive or executive's designee must sign off on the RFC as a normal change. Once an RFC has been signed off by the divisional executive, it is considered pre-authorized and will be reviewed by the CAB for comment and send for approval by the Group IT Manager.

If an objection to the RFC is raised by the CAB, the RFC will be removed from the implementation schedule list and returned to the requestor for discussion.
If no objection is raised, the change is implemented on the scheduled date. The ticket is only closed once the change has been implemented and verified by the CAB.

1.8.2 Normal change - DevOps

A change request is initiated by the drafting of a URS, in the event of new development. The URS must be signed off as new development by the CAB. Bug reports are tracked through a normal ticket.

If an objection to the RFC is raised by the CAB, the change request will be removed from the development list and returned to the requestor for discussion.

If no objection is raised a technical document will be drawn up to determine a development timeframe that must be approved by the CAB. Once the technical document has been approved it will be added to the development schedule on a first come first served basis.

Once development has been completed before the changes are moved to production, they must first be tested end-to-end in a QA environment. QA testing include internal testing using existing test cases or with the creation of a new test case. The change is then passed on to the system owner for UAT once it passes internal testing. Only when the development passed initial UAT in the QA environment is it moved to production during the next maintenance window. After it has been successfully deployed the RFC ticket can be closed.

1.8.3 Expedited change - Infrastructure

The change control follows the same process and approval flow as a normal change RFC for infrastructure, but lead times are shorter. Expedited change RFCs must demonstrate that service is at risk, although service might not be down, and the RFC needs to be authorized because of a client request that has been validated by SME/technical expert or an executive, who has determined that that the change needs to go in without waiting for the recommended lead-time. The same normal change request information is provided in the ticketing system to implement the change, including the reason for expediting the RFC (risk, back-out plans, scheduled time and downtime required). It is the responsibility of the change requestor to shepherd the expedited change through the approval process. All expedited RFCs must be preauthorized by the Group IT Manager. Retroactive CAB approval is required.

1.8.4 Expedited change - DevOps

The change control follows the same process and approval flow as a normal change RFC for DevOps, but lead times are shorter by allowing the development to jump the queue and not enter it at the bottom but the top. The same normal change request information is provided in the ticketing system, including the reason for expediting the RFC. All expedited RFCs must be preauthorized by the Group IT Manager.

1.8.5 Emergency change - Infrastructure

E-RFCs for infrastructure do not follow the complete lifecycle of a normal change due to the speed with which they must be implemented. E-RFCs must meet the criteria that they are necessary to correct, or prevent a high priority incident, or likely negative service impacts/situations where the impact to a service is imminent if action is not taken. All E-RFCs are authorized by a member of the CAB and documented and entered the ticketing system prior to implementation, or as soon as possible after the change has been implemented depending on the nature of the emergency. The E-RFC is discussed at the earliest CAB meeting and are subject to a post implementation review.

1.8.6 Emergency change - DevOps

E-RFCs for DevOps are typically only done for reported critical bugs. They do not follow the complete lifecycle of a normal change due to the speed with which they must be implemented. E-RFCs must meet

the criteria that they are necessary to correct, or prevent a high priority incident, or likely negative service impacts/situations where the impact to a service is imminent if action is not taken. All E-RFCs are authorized by a member of the CAB and documented and entered into the ticketing system prior to implementation, or as soon as possible after the change has been implemented depending on the nature of the emergency. The E-RFC is discussed at the earliest CAB meeting and are subject to a post implementation review.

1.9 Notice requirement

All normal RFCs require a minimum two-week notice to impacted stakeholders unless the stakeholders have agreed to waive this requirement.

1.10 CAB meeting

CAB sittings happens weekly. Once for infrastructure and once for DevOps. The facilitator confirms that all the requests that were planned for the previous week have been implemented, if any request was not implemented the reasons are noted and the implementation is carried over to the new schedule. All E-RFCs implemented since the previous meeting are also discussed and confirmed that the post implementation review has been completed. Any new requests are discussed and added to the schedule once approved. It is possible for the CAB to request to delay an implementation.

It is imperative that the CAB agree during this meeting that all the preconditions have been met before approving the implementation.

1.10.1 Post Implementation reviews

Once the change has been implemented the implementor has the responsibility to verify that the changes are implemented correctly, operating as intended and meet the security requirements. The implementor must update any system documentation to reflect the changes for review during the next CAB sitting.

Change requests that cannot be implemented follows the planned back out procedures. The reasons for the failure are noted to be discussed during the next CAB sitting.

1.11 Security Impact Analysis

Potential Impact				
Security Objective	**No**	**Low**	**Moderate**	**High**
Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	No adverse effect	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity: Guarding against improper information modification or destruction and includes ensuring information nonrepudiation and authenticity.	No adverse effect	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations,	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations,	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations,

		organizational assets, or individuals.	organizational assets, or individuals.	organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information.	No adverse effect	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

1.12 Glossary

BPC	Bidvest Protea Coin
CAB	Change Advisory Board
E-RFC	Emergency Request for Change
QA	Quality Assurance
RFC	Request for Change
SME	Subject Matter Expert
UAT	User Acceptance Testing
URS	User Requirement Specification