Configuration Management

Plan

Prepared for

Deloitte

16 January 2015

APPROVAL SIGNATURE

The D2C2 Configuration Management Plan was prepared for the exclusive use of the Deloitte.

Approved by & Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Information System Owner

**DOCUMENT CHANGE HISTORY**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Description |
| 1.0 |  | Deloitte | Initial draft |
|  |  |  |  |

Table of Contents

[1.0 INTRODUCTION 1](#_Toc70337402)

[1.1 System Identification and Description 1](#_Toc70337403)

[1.2 Purpose 1](#_Toc70337404)

[1.3 Scope 1](#_Toc70337405)

[1.4 Structure 1](#_Toc70337406)

[2.0 ROLES AND RESPONSIBILITIES 2](#_Toc70337407)

[3.0 Configuration Management 3](#_Toc70337408)

[4.0 COMMUNICATIONS 4](#_Toc70337409)

[5.0 CONFIGURATION CONTROL PROCESS 4](#_Toc70337410)

[5.1 Step 1: Establish System Configuration Baseline 5](#_Toc70337411)

[5.1.1 System Architecture 5](#_Toc70337412)

[5.1.2 System Characterization 6](#_Toc70337413)

[5.1.4 Software 6](#_Toc70337414)

[5.1.5 System Library 7](#_Toc70337415)

[5.3 Step 2: Identify Change and Complete Change Request Form 7](#_Toc70337416)

[5.3.1 Change Control Process 8](#_Toc70337417)

[5.4 Step 3: Submit Change Request Form 14](#_Toc70337418)

[5.5 Step 4: Perform Configuration Change Process 14](#_Toc70337419)

[5.6 Step 7: Perform Configuration Status Accounting 15](#_Toc70337420)

[5.7 Step 8: Conduct Configuration Verification and Audit 16](#_Toc70337421)

[6.0 Protection of Configuration Management Plan 16](#_Toc70337422)

[7.0 CONFIGURATION MANAGEMENT RESOURCES 16](#_Toc70337423)

[7.1 Facilities 17](#_Toc70337424)

[7.2 Tools 17](#_Toc70337425)

[7.3 Configuration Management Database (CMDB) 17](#_Toc70337426)

[8.0 REFERENCE DOCUMENTS 18](#_Toc70337427)

# INTRODUCTION

## 1.1 System Identification and Description

System Number: **[project ID not provided]**

System Name: Deloitte Digital Contact Center

System Abbreviation: D2C2

The system is in the following system operational status: Operational status

Deployment of D2C2 began in 2021 with a core set of applications. These applications will grow to become the premier Contact Center environment for Health, Federal, and beyond.

## 1.2 Purpose

An information system is typically in a constant state of migration, with upgrades to hardware, software, or firmware and possible modifications to the system environment. Documenting information system changes and assessing the potential impact on the security of the system on an ongoing basis is an essential aspect of maintaining the security accreditation. A good Configuration Management Plan (CMP) ensures that configuration and control changes to the system are monitored, evaluated, and impacts are assessed prior to implementation.

## 1.3 Scope

This Configuration Management Plan applies to the D2C2 managed by the Deloitte Organization. It applies to all levels of the organization and all users of the system.

As a management tool, the CMP ensures that system components, whether hardware or software, are properly identified and controlled during the day-to-day operations. Deloitte provides a disciplined set of techniques for controlling changes to identified baseline security configurations, and enhances consistency, compatibility, integrity, and security of Deloitte’s D2C2 systems.

## 1.4 Structure

This plan is organized into five major sections:

* Section 1 provides an introduction to the plan.
* Section 2 provides a description of the CMP roles and responsibilities.
* Section 3 describes the communication methods related to this CMP.
* Section 4 provides an overview of the configuration control process.
* Section 5 discusses CM resources.
* Section 6 provides a referenced forms list.

# 2.0 ROLES AND RESPONSIBILITIES

This section clearly identifies Configuration Management (CM) roles and responsibilities for the system, noting that all CM activities must be performed in accordance with the processes and procedures documented in the CMP. Some examples of CM roles and responsibilities in an organization are provided in the following table.

| Role | Responsibilities |
| --- | --- |
| Chief Information Officer | Setting forth policies regarding CM and implementing CM at the highest level for the Deloitte. |
| System Owner/Manager | Serves as the authority for all matters of CM for the system. Responsible for developing functional requirements and verifying that the requirements are implemented appropriately. May also play a role in establishing the Configuration Control Review Board (CAB) and may be involved in the selection of the CAB members. |
| CM Manager | Oversees all aspects of the CMP; responsible for all day-to-day activities necessary to support the CMP and may call on other personnel for assistance. Primary responsibilities are:  - Implement the CMP  - Provide operational support to the CAB  - Draft the CMP for CAB approval  - Provide the CAB with information to evaluate changes  and screen materials  - Arrange CAB meetings, provide agendas, and prepare  meeting minutes  - Coordinate implementation of CAB decisions  - Maintain CM Library and database  - Coordinate CMP with other security documentation, as  required |
| CM Librarian | The CM librarian is appointed by the CM manager and is responsible for storing, retrieving, and distributing CM library materials. |
| Change Advisory Board (CAB) | Governing body for CM policy and guidance affecting all GSs and MAs in the organization. A chairperson should be appointed by the CAB to oversee the activities of the Board. Primary responsibilities of the CAB include:  - Managing CM operations  - Reviewing and approving the CMP  - Evaluating, approving, or disapproving change requests  - Ensuring proposed changes are limited to those necessary  to correct deficiencies  - Satisfying changes in operational capability, personnel  safety, and logistics support requirements  - Effecting substantial life-cycle cost savings  - Maintaining security requirements  - Preventing slippages to approved schedules  - Ensuring proposed changes do not adversely affect external systems, subsystems, facilities, software, or services  - Establishing system baselines and authorizing changes to applications |
| System Users | Responsible for reporting any weaknesses identified in current versions of the hardware, software, and components. |
| Other | Other roles in the organization, such as the information system security officer (ISSO) and system administrator may also have specific CM responsibilities. Once the extent of these responsibilities is determined, they are documented in the CMP for the system. |

Table 2-1: Configuration Management Roles and Responsibilities

# 3.0 Configuration Management

Our configuration management process is designed to keep up-to-date information about our assets and the component parts of the IT services we manage. The process ensures that accurate and reliable information about our assets are available when and where it is needed. All configuration changes will go through our Change Management process. ServiceNow (SNOW) will be our repository for housing all our documentation. Patches that are applied will be stored in SNOW unless the file is greater than 100MB. Those patches will need to be stored in a secure cloud storage bucket. As part of our improvement efforts, we shall conduct quarterly reviews of all configuration changes made.

**Version control**

The version control process will enable our team to track and manage different versions (or drafts) of a document so that everyone is aware of its current iteration. Users editing a document are required to update the Revision History table at the beginning of the document. Please be sure to enter the necessary information in the required fields so that everyone is aware of the changes that were made. When saving a new document, please be sure to use the approved NOC-nomenclature. If saving an existing document, please update the version.

# 4.0 COMMUNICATIONS

The communications section discusses the methods used to share information regarding CM (such as upgrades, application changes, technical notices, version control, and so on) within the organization. This section addresses items such as who has access to the information and how, when, and what type of information is shared.

# 5.0 CONFIGURATION CONTROL PROCESS

This section identifies the processes/steps required to ensure that all changes to D2C2are properly requested, evaluated, and authorized. Processes provide detailed, step-by-step procedures for establishing, processing, tracking, and documenting changes.

The Configuration Control Process is critical to the D2C2because of the number of changes, revisions, upgrades, and modifications that it is expected to undergo throughout its life cycle. Thus, the effective management of changes requires a formal, documented, systematic process for requesting, evaluating, tracking, and approving changes to the system. The figure below is an illustration of the Configuration Control Process currently in place.



The following sections provide detailed descriptions of the eight minimum steps that are included as part of the Configuration Control Process.

## 5.1 Step 1: Establish System Configuration Baseline

The first step of the Configuration Control Process is to establish the System Configuration Baseline as a snapshot of the current design and functionality of the system, and to provide details regarding all software. The System Configuration Baseline includes identification of all software applications that are currently being used in the production environment, and the specific configuration settings for each. If the system is not yet operational, the System Configuration Baseline reflects the current status of the system within the System Development Cycle (SDC). Specifically, the following items describe and/or identify the System Configuration Baseline:

* System Architecture
* System Characterization
* Hardware
* Software
* System Library

This information may be collected from various system and/or security documentation. The amount of existing documentation may depend on where the system is within the SDC.

### 5.1.1 System Architecture

A detailed and explicit definition of the system authorization boundary diagram is represented in Figure 9‑1 Authorization Boundary Diagram below.

Diagram

Description automatically generated

Figure 9‑1 Authorization Boundary Diagram

### 5.1.2 System Characterization

Purpose and functionality of the system:

* Number of users: *5000+*
* System criticality and information sensitivity levels: *Moderate Level*
* System confidentiality, integrity, and availability levels: *Confidentiality- Moderate (M), Integrity (M), and Availability (M).*
* Type of data that is processed by or stored in the system: *Protected Health Information (PHI) and Personally identifiable information (PII).*

### 5.1.4 Software

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Title (including acronym or nickname) | Version Number | Build Number, if appropriate | Media (such as 4mm tape, 8mm tape, CD ROM, and so on) | Hardware requirements necessary to run the software (such as available disk space, random access memory (RAM), network connections, and so on) | Control parameters (such as password policy, account lockout policy, requirements to change existing passwords, audit policy, user rights assignments, event log policy, restricted groups, system services settings, file permissions settings, and so on) |
|  |  |  |  |  |  |

### 5.1.5 System Library

#### 5.1.5.1 System Documentation and Supporting Information

The following system documentation was used to establish the System Configuration Baseline:

|  |  |  |  |
| --- | --- | --- | --- |
| Title | Publication Date | Version Number | Revision Date |
|  |  |  |  |

#### 5.1.5.2 CM Library

The CM library contains all CM-related documentation (such as change request (CR) forms, security impact assessment forms, and CR status logs, and so on). The CM Manager is responsible for maintaining the CM library to ensure that all documents regarding system changes are stored in an orderly manner, and copies are provided to authorized persons, when necessary. Due to the complex nature of the D2C2 and frequency of updates and changes, the CM manager has delegated some responsibilities to a CM librarian, who is generally responsible for storing, retrieving, and distributing library materials.

## 5.3 Step 2: Identify Change and Complete Change Request Form

To initiate a change, the need for that change is identified and other relevant information such as what type of change it is, why the change is necessary, and how the change may be implementedis collected. A change ticket is opened in ServiceNow with the needed information in the ticket. The ticket is monitored through the process of development and Production. Changes to the D2C2are categorized as:

**Emergency** - any change that is required to address safety or security issues

**Major** - any change that requires more than 120 hours of development support

**Minor** - any change that requires less than 120 hours of development support

**Optional** - any change that is strictly "nice to have" but is not necessary to the function of the system

The CR form provides information such as title and description of the change, justification, timeframe, and the potential impact on security, including a signature from the approving security official.

The system owner or Chief Engineer ensures that all information on the form has been completed before submission.

A security impact assessment form is included with the CR form, describing in detail the possible impact that this change could have on system security.

See Section 6, Figures 1 and 2, for a sample change request form and sample security impact assessment form.

### 5.3.1 Change Control Process

The Change Control process will formally review all change requests to provide assessment and planning, in efforts to approve and implement changes. Standard, User Creation, Rollbacks, User Termination, Updates and Patches and Emergency changes will have its own procedure and approval protocols to follow. For continual improvement efforts, weekly change control meetings will be had.



**A Standard Change** request is classified as a simple, low-risk change, which may not require change management assessment, but only require the approval of the First Level Product SME.

**Description:** The Standard Change Request process will detail how every standard change request is handled through the Change Control Process.

**Prerequisites:**

**Targets:** Systems

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | Change request submitted through SNOW |  |
| 2. | Classified as a Standard change |  |
| 3. | Review to see if it is a preapproved change |  |
| 4. | Submit to the CAB |  |
| 5. | Schedule the release |  |
| 6. | Implement the requested change and update the CMDB |  |
| 7. | Post implementation review |  |
| 8. | Close the change |  |

**Emergency Change** requests are classified as a high priority and are time sensitive. These changes go directly to the Emergency Committee.

**Description:** The Emergency Change Request process will detail the steps involved in order expedite a change needed in the system.

**Prerequisites:**

1. Major event occurrence

**Targets:** System

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | Change request is submitted |  |
| 2. | Classified as an emergency |  |
| 3. | Submitted to the Emergency Review Committee | Committee consists of Chief Engineer, duty NOC manager, QA Lead, Customer Designate (for customer impacting changes) |
| 4. | Implement requested change |  |
| 5. | Post implementation review |  |
| 6. | Close the change |  |

**Configuration change** requests are classified as needed changes to IT components or assets.

**Description:** The Configuration Change process will detail the steps needed to approve any changes to our systems

**Prerequisites:**

1. Baselines
2. Latest version of system

**Targets:** Systems

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | Change request submitted |  |
| 2. | Classified as a configuration request |  |
| 3. | Is this an emergency change |  |
| 3.1 | If Yes: Submit to Emergency Committee for review  If No: Proceed to the CAB |  |
| 4. | Submitted to CAB for review |  |
| 5. | Change implemented in Development |  |
| 6. | Change is tested |  |
| 7. | Request to implement in Production |  |
| 7.1 | If request approved: Is this a major change?   * If Yes: Proceed to Customer Notification Process * If No: Proceed to Schedule Change   If denied: Go to Implement in Development | Customer Notification process will alert the customer of any major changes to the system. |
| 8. | Schedule change |  |
| 9. | Implement change |  |
| 10. | Perform Configuration Status Accounting |  |
| 11. | Conduct Configuration Verification and Audit |  |

**Rollback Change** requests occur when the actions of an associated change request need to be reversed. Rollback changes will need to go through the CAB.

**Description:** The Rollback Change Request process will detail the steps involved in order to revert the system back to a previous state before a change was implemented.

**Prerequisites:**

1. Previous change request

**Targets:** System

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | Change request submitted |  |
| 2. | Classified as a Rollback change |  |
| 3. | Submit to the CAB | Requires approval from the NOC manager and the Chief Engineer |
| 4. | Schedule the release |  |
| 5. | Implement the requested change |  |
| 6. | Post implementation review |  |
| 7. | Close the change |  |

**User Creation** requests allow for new accounts to be created. This request has its own approval process and does not go through the CAB.

**Description:** The GCP User Creation Change Request process will detail the steps involved to create a user into our systems.

**Prerequisites:**

1. New member joins the program.

**Targets:** GCP

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | Change request submitted |  |
| 2. | Classified as a User Creation request |  |
| 3. | Customer approves account creation request |  |
| 4. | Request is approved by the NOC Manager |  |
| 5. | Request is approved by PII Manager |  |
| 6. | Create account |  |
| 7. | Create GCP Account |  |
| 7.1 | Sign into your Google Admin Console |  |
| 7.2 | Go to Users from the Admin console Home Page |  |
| 7.3 | Select the organizational unit you wish to add the user to |  |
| 7.4 | Click Add New User |  |
| 7.5 | Add Account Information | * First and Last Name * Enter External after last name if they are a contractor. * Enter a C after their last name if they are a customer. |
| 7.6 | Create Password | It can be autogenerated or manually created |
| 7.7 | Select Ask user to change password during next sign in |  |
| 7.7 | Click Add New User |  |
| 7.8 | Click Email User Sign-in info |  |
| 7.9 | Welcome email sent to user. User must reset their password within 48 hours |  |
| 8 | Does the user require admin privileges? |  |
| 8.1 | If Yes: Follow Admin Access procedure  If No: Proceed to Validate User can Login |  |
| 9 | Admin Access Procedure |  |
| 9.2 | Get NOC Manager approval |  |
| 9.3 | Sign into Google Admin console |  |
| 9.4 | Go to Users from the Admin console Home Page |  |
| 9.5 | Find user from the Users List |  |
| 9.6 | Click User’s name to open their account |  |
| 9.7 | Click Admin Roles and Privileges |  |
| 9.8 | Click Super Admin Role |  |
| 9.9 | Mark slider as Assigned |  |
| 9.10 | Click Save |  |
| 10 | Validate User can Login |  |
| 11 | Close the Change |  |

**Termination** requests are submitted when accounts need to be terminated or disabled. This occurs when users are noncompliant with security policies or have either left or been transferred.

**Description:** The User Termination Request process will detail the steps involved in order to terminate users who have left the program our have been inactive for a certain period of time.

**Prerequisites:**

1. User termination
2. User has transferred
3. User has been inactive

**Targets:** System

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | Change request submitted |  |
| 2. | Classified as a User Termination change |  |
| 3. | Determine if this is regarding noncompliance with security policies |  |
| 3.1 | If Yes: Disable account and confirm Security Team is aware of noncompliance  If No: Proceed to account inactivity |  |
| 4 | Account Inactivity |  |
| 4.1 | Has the account been inactive for 60 days? |  |
| 4.2 | If Yes: Disable account  If No: Proceed to contractor step |  |
| 5 | Is the user a contractor? |  |
| 5.1 | If Yes: Disable account within 24 hours and notify vendor.  If No: Disable account for 30 days. After 30 days, terminate account | Capture contractor company, contractor name and user ID in preexisting accounts list. |
| 6 | Close the change |  |

**Updates and Patches** may be requested in order to implement a new software release, or apply a fix to repair any issues within the system

**Description:** The Patching/Updates procedure will allow us to conduct approved software updates and necessary patches to our systems

**Prerequisites:**

1. Software release/patch/update available

**Targets:** Servers/services

|  |  |  |
| --- | --- | --- |
| **Steps** | **Process** | **Notes** |
| 1. | NOC Schedules Change Request for discussion for next CAB Meeting |  |
| 2. | CAB discusses patch |  |
| 3. | Patch Approved? |  |
| 3.1 | **If Yes:** Schedule deployment in DEV environment  **If No:** Cancel Patch/Update change request |  |
| 4. | Schedule deployment in DEV |  |
| 5. | Patch installed in DEV |  |
| 6. | Patch tested in DEC |  |
| 7. | Patch/update testing results submitted to CA |  |
| 8. | CAB discussed test results |  |
| 9. | Approved for production? |  |
| 9.1 | **If Yes:** Patch/Update scheduled for PROD deployment  **If No:** Go back to DEC for further install and testing |  |
| 10. | Patch/Update scheduled for PROD deployment |  |
| 11. | Patch installed in PROD during next change window |  |
| 12. | NOC monitors first day after patch |  |
| 13. | Patch/Update issues? |  |
| 14. | **If Yes**: Rollback Patch/Update and send back to CAB for discussion  **If No:** Update CMDB |  |
| 15. | Update CMDB |  |

## 5.4 Step 3: Submit Change Request Form

The completed CR form is submitted to the CAB for approval. Upon receipt, a tracking number is assigned to and documented on the CR form. All emergency CR forms are submitted to the CAB for approval in a less critical timeframe and an emergency request number is assigned to and documented on the emergency CR form. In addition, the CAB updates the CR status log to include all new CRs, including emergency requests, so the change can be tracked.

Not all system configuration changes need to be approved by the CAB. For example, changes to a Microsoft Access database field may not have to be approved by the CAB. However, the system owner or designated individual must review technical and business analyses to determine how the change will impact the system and render a decision based on the information provided. All changes are tracked in either a CR status log or in an equivalent log that maintains all configuration changes.

See Section 6, Figure 3, for a sample change request status log.

## 5.5 Step 4: Perform Configuration Change Process

In Step 4, the CAB carefully evaluates the information provided on the completed CR form to determine whether or not to approve the change. Missing or inadequate information could preclude the CR from being expedited immediately. This section provides details on how the evaluation is performed and establishes a time frame for decisions to be made regarding regular CRs as well as emergency CRs.

The CAB reviews the technical and business effects of implementing the change to the system.

The Technical analysis determines the following:

* Whether the change is technically correct
* Whether the change is technically necessary and feasible within the system constraints
* How system security will be affected
* All associated costs for implementing the change
* All security components affected

The business analysis should determine the following:

* Milestones, and whether the requested time frames are feasible
* Whether the change affects an existing contractual agreement regarding the system
* Overall impact to the PO, the Division, associated costs with purchasing the hardware, software, and labor as well as the impact on personnel schedules

As proposed changes to D2C2 are brought before the Configuration Control Board (CCB), the D2C2 ISSO and the D2C2 O&M Team Security Analyst review the respective proposed change and complete an appropriate security impact assessment (SIA). Each SIA will determine whether the proposed change has a material impact on the current security posture. The CAB must consider the results of the impact analysis review before making a decision about the change. The D2C2 O&M Security Engineer will work closely with the change requestor and other developers/engineers to understand the timing and nature of the change, determine the NIST Special Publications 800-53 security controls impacted by the change (if any), and conclude on the overall impact to the current implementation of each security control. An SIA report will be developed to be used in CCB decision-making processes, and then stored securely on the D2C2 ServiceNow site.

| **Inputs** | **Frequency** | **Outputs** | **Recipients** |
| --- | --- | --- | --- |
| Change request documentation | As needed | SIA Report | * CCB stakeholders |

See Section 6, Figure 2, for a sample Security Impact Assessment Form.

The CAB reviews the CR and Impact Analysis and makes a decision based on the information provided and the Chief Architecture makes sure any changes pass the Quality Assurance test. The CR status log is used to track all CRs and corresponding decisions. The CAB has the option to choose one of the following decisions:

* Approve - Immediate implementation is authorized and may occur at any time after an authorized signature has been documented on the CR.
* Disapprove - Immediate denial of the request regardless of circumstances and information provided.
* Defer - Immediate decision is postponed until further notice. This decision could be due to lack of documentation or results of the technical and business impact analyses.

If approved, the change is implemented in the Development environment. There, it will be tested to ensure it works properly. A request to deploy in Production is then made. If the request is denied, it will go back to Development. If approved, we need to check if this is a major change that needs to be communicated to the client. From there, we will go ahead and schedule and implement the change.

## 5.6 Step 7: Perform Configuration Status Accounting

This step consists of maintaining records of all changes and ensuring the traceability of each CR from initiation through resolution and disposition. Status accounting enables the implementation of approved changes to be tracked and managed and accomplishes the following:

* Provides historical databases and records
* Updates the Configuration Management Database (CMDB)
* Provides the status of approved baseline, proposed changes, and implementation of approved status
* Determines the status of all systems in the CM process
* Tracks changes and action items

## 5.7 Step 8: Conduct Configuration Verification and Audit

The final step of the Configuration Control Process is to conduct configuration verification and audits to ensure compliance with the current configuration control requirements. Verification provides the means to examine the characteristics of each system and the supporting documents to verify that the configuration in place meets the user's needs and the current configuration is the approved System Configuration Baseline.

Audits include functional and physical configuration audits. Functional configuration audits verify that the system's actual performance conforms to the stated requirements, and that physical configuration audits ensure that the baseline documentation is a true representation of the "as-built" version of the software and hardware. In addition, as part of the audit process, CM documentation is verified for accuracy with respect to content and timelines.

* Verification and audit ensure the following:
* Changes are properly implemented
* Regulations and standards are followed
* Documentation is accurate (test results, vendor documentation, system environment, and configuration identification information, etc.)
* The system performs its functions
* Security status is constant

# 6.0 Protection of Configuration Management Plan

Deloitte protects the configuration management plan for unauthorized disclosure and modification by storing the plan in ServiceNow (SNO) and only authorized personnel that are granted access will have access to the Configuration Management plan.

# 7.0 CONFIGURATION MANAGEMENT RESOURCES

The CM resources section of the CMP describes facilities and tools used for CM activities. This information serves as guidance for planning the resources required to support the functions of each organization throughout the CM process. Because the number of staff, equipment, and space required varies according to each organization's needs, the CM manager periodically reviews the resources involved in CM and verifies that the facilities and tools are up-to-date. The CM manager also works with the system owner and CAB to determine what type of software package is best for the Organization and its systems.

## 7.1 Facilities

There are no physical and environmental controls in place for D2C2 since it is hosted in the cloud on Google’s platform.

## 7.2 Tools

Deliotte is using Teraform as the automated tool to manage CM activities and maintaining change control. Teraform is a service that is provided by google. Deliotte implements the configuration files into Teraform and google runs the scripts.

## 7.3 Configuration Management Database (CMDB)

The Configuration Management Database will be used to store configuration records throughout their lifecycle. CMDB will store attributes of configuration items, and relationship with other configuration items. Any changes resulted from the Change Management process will be tracked in the CMDB. The CMDB will be housed in ServiceNow and include the following items:

* App Configuration Files
* Terraform Built Files
* The Solution Design Document

# 8.0 REFERENCE DOCUMENTS

CHANGE REQUEST FORM

|  |  |  |
| --- | --- | --- |
| CHANGE REQUEST FORM | | |
| **Requirement #** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **CRF #** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Originator: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_ Release # \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Originator email: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Originator Phone: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Type:  [ ] New Requirement [ ] System Problem [ ] Suggestion for Improvement  [ ] Requirement Change [ ] User Interface Problem [ ] Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  [ ] Design Change [ ] Documentation Correction  Priority:  [ ] Emergency [ ] Major [ ] Minor [ ] Optional  Description:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_    Please attach supporting documentation of the requested change (screen/report printouts, document pages affected, etc.). | | |
| Status | Date | Signature/Comments |
| Reviewed & Estimated |  |  |
| On Hold |  |  |
| Canceled |  |  |
| Approved for Change |  |  |
| Code Updated |  |  |
| Documentation Updated |  |  |
| Completed |  |  |
| CFR #\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  **New Release #** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Please attach supporting documentation for review & estimates (analysis, resource estimates, layouts, document pages affected, etc.) | | |

Figure 1. Sample Change Request Form Template

SECURITY IMPACT ASSESSMENT FORM

|  |
| --- |
| SECURITY IMPACT ASSESSMENT FORM |
| Priority:  [ ] High [ ] Medium [ ] Low  CR Originator  (System Owner)  Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Title of Change: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ CR Tracking Number: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Description of Change (From CR Form):    Impact of the Change on System Security:    Sites Affected:  Will any security measures need to be suspended during the actual implementation time?  [ ] Yes [ ] No  If yes, please explain below. |

Figure 2. Sample Security Impact Assessment Form Template

CHANGE REQUEST LOG

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| CHANGE REQUEST LOG | | | | | | | | | | | |
|  | | | | Approval | | Status | | | | | |
| Request # | Reqmnt # | Date Submitted | Priority (E, MA, MI, OPT)\* | Change Approved | Change Not Approved | Hold (Future Enhancement) | Technical Evaluation Phase | Change In Progress | Canceled | Target Date | Date Complete |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |

\* E = Emergency, MA = Major, MI = Minor, OPT = Optional (as defined by the Change Request Form)

Figure 3. Sample Change Request Log Template