**Document Control**

|  |  |
| --- | --- |
| Project Manager | Smaridge Laura |
| Document Author | Experian UK |
| Date | 15/11/2018 |
| Version | 0.1a |
| Classification | Experian Confidential |

**UK &I Solution Division**

**Cyber Security Upgrade Test Approach**

Document Owner

|  |  |
| --- | --- |
| Name | Role |
| Chandramouli Pasumarthy | Test Lead |

Approval

Following approval, this document will be base-lined by promoting it to a major version number (e.g. 1.0), recording the names and positions of approvers in the Approval Record and, if applicable, accepting all tracked changes. The Approval Record can be found in the Document Control Appendix at the end of this document.

A soft copy of email approvals will be maintained and stored as a permanent record of acceptance of this document.

Change Control

This document is subject to change control. All requests for change should be referred to the document owner.

The Change History can be found in the Document Control Appendix at the end of this document.

Distribution

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Role | Reason | Departments |
| Smaridge Laura | Project Manager |  |  |
| Pugh Graham | Business Analyst |  |  |
| Telford Adrian | Delivery Manager |  |  |

**Contents**

[1. Introduction 3](#_Toc532480823)

[1.1 Document Purpose 3](#_Toc532480824)

[1.2 References 4](#_Toc532480825)

[1.3 Project / Solution Overview 4](#_Toc532480826)

[1.4 Objectives 4](#_Toc532480827)

[2. Scope 4](#_Toc532480828)

[3. Test Approach 4](#_Toc532480829)

[3.1 Test Basis 4](#_Toc532480830)

[3.2 Test Design 5](#_Toc532480831)

[3.3 Test Execution 5](#_Toc532480832)

[3.3.1 In Scope 5](#_Toc532480833)

[3.3.1 Out of Scope 5](#_Toc532480834)

[3.4 User Acceptance Testing 5](#_Toc532480835)

[3.5 Non - Functional Testing 5](#_Toc532480836)

[3.6 Test Environment Requirements 6](#_Toc532480837)

[3.6.1 Security Testing 6](#_Toc532480838)

[3.6.2 Non- Functional Testing 6](#_Toc532480839)

[3.7 Test Data 6](#_Toc532480840)

[3.8 Test Tool Requirements 6](#_Toc532480841)

[3.9 Defect Management 6](#_Toc532480842)

[3.9.1 Defect Workflow 6](#_Toc532480843)

[<The defect workflow to be updated> 6](#_Toc532480844)

[3.9.2 Defect Triage Roles 6](#_Toc532480845)

[3.10 Test Reporting 6](#_Toc532480846)

[3.11 Test Suspension Criteria 6](#_Toc532480847)

[3.12 Test Resumption Criteria 6](#_Toc532480848)

[4. Roles and Responsibilities 7](#_Toc532480849)

[5. Test Closure and Approval Process 7](#_Toc532480850)

[6. Risk Management 7](#_Toc532480851)

[6.1 Responsibility 7](#_Toc532480852)

[6.2 Risk Management Activities 7](#_Toc532480853)

[6.3 Risk Governance 8](#_Toc532480854)

[7. Test Deliverables 8](#_Toc532480855)

# Introduction

## Document Purpose

The Test Approach document is intended to provide its readers with a comprehensive view of the tactical approach adopted to test Cyber Security Upgrade project by detailing the high-level features and components that will be tested. It outlines the feasibility and effort required to create testing processes to address all security requirements of Project Cyber Security Upgrade. This document details on the test approach by defining the test methodologies, test processes and test requirements specific to the project. It encapsulates the different test approaches adopted, specifications on the test environment, test data management processes and defect management process.

## References

<List out all documents that support this Test Approach in the table below.>

|  |  |  |
| --- | --- | --- |
| Document Id | Document Title | Version |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Note: - This document is owned, produced and controlled by the testing team under the governance of the Test Delivery Office.

## Project / Solution Overview

Cyber Security Upgrade proposes a standard approach to testing, based upon the methodology. The proposed approach will follow the agreed model, which identifies both the testing stages and the deliverables that must be tested at each stage of the project lifecycle.

The approach falls into four main Testing stages, listed in order:

- Regression Testing

## Objectives

<List out primary business objectives aligned to the Project>

# Scope

<List out the high-level functionalities or scenarios and Test conditions >

|  |  |
| --- | --- |
| **High Level Business Functionalities** | **High Level Test Scenarios** |
|  |  |

# Test Approach

Cyber Security Upgrades project adopted Agile methodology to test multiple applications in various sprints to cover the security tests of each application.

## Test Basis

Below list of project documentation, which should be referred as the test basis.

* + Business URLs

## Test Design

To cover end to end functionality security testing.

* + Pre-Run on application to ensure the production version of code it has.
  + Ready with all Data and screenshots.
  + Do a final run on the updated version of applications to ensure it has all latest code applied.
  + Report if any application failures.

## Test Execution

### In Scope

Types of testing that are in scope for the project should be detailed in the below format with no of cycles planned as per the estimate considerations

* Build Verification Testing
* Regression Testing
* Test Automation (as applicable)

|  |  |
| --- | --- |
| **Security Testing** | |
| **Owner** | QA Team |
| **Test Objective** | To ensure application security. |
| **Scope** | To cover security tests of the application based on the changes that are received. |
| **Technique** | Security testing. |
| **Test Levels & Test Types** | Pre- Testing, Post Testing, BVT & Regression testing & Security Testing |
| **Test Deliverables** | Test Approach, Test Plan, Test Cases, RTM, QGR |
| **Entry Criteria** | Receive the application with code changes once Unit testing completed from Development team with QGR approved. |
| **Exit Criteria** | Get QGR approved for QAT and request to promote the build to UAT. |

### Out of Scope

If the test types are out of scope for testing team who will own this and what will be input back to the testing team to be detailed

* Unit Testing
* Functional testing.
* Client System Integration Testing
* User Acceptance Testing

## User Acceptance Testing

NA

## Non - Functional Testing

NA

## Test Environment Requirements

### Security Testing

Additional Security tests are being added

### Non- Functional Testing

NA

## Test Data

BA should provide the data for the applications that are to be tested.

## Test Tool Requirements

<List out the tooling that has been identified to support overall testing. Consider tooling used for test design, test execution, test reporting for functional as well as non-functional testing.

## Defect Management

<This is expected to be directly inherited by the programme / capability Test strategy/

Test Procedure, however it is worth considering how defects will be reported with regards to tooling, metrics captured, and what process will govern the management of the defect for the planned testing to verify what is specified in the programme / project Test Strategy/ Test Procedure is sufficient for your testing. It should Details the triaging process for each test types and representatives to manage and track the defects to closure>

### Defect Workflow

### <The defect workflow to be updated>

### Defect Triage Roles

<List out the Names, Roles and responsibilities for defect triage, need to consider all types of testing applicable for the project. Functional and Non-functional>

## Test Reporting

<How the test status reporting for all the phases and metric capture planned for the project with owners assigned >

## Test Suspension Criteria

< List out the scenarios where the test suspension will happen>

## Test Resumption Criteria

< List out the conditions through which resumptions will be done>

# Roles and Responsibilities

<Listed out the Key project and testing roles and detail the responsibilities with respect to the project>

|  |  |
| --- | --- |
| **Roles** | **Responsibilities** |
| Test Lead | Reporting on testing activities. |
| Test Analyst | Design and execute tests. |

# Test Closure and Approval Process

<Entry and exit parameters for the test closure to be detailed here>

# Risk Management

Currently QA is provided with very few number of QAT URLs an access, there is a risk where QAT can be delayed until the details, functional specifications and access provided.

## Responsibility

|  |  |  |
| --- | --- | --- |
| **Sl. No.** | **Risk Management Level** | **Owner** |
| 1 | Project Delivery head | Telford Adrian |
| 2 | Project Manager | Harriet Rymell |
| 3 | BA | Pugh Graham |

## Risk Management Activities

<The objective of this section is to detail the activities that shall be performed as part of the Risk Management process at various level:

* Determine the risk event or condition
* Identify the consequence of the risk event
* Evaluate the risk to determine the impact and probability of occurrence, and determine the Risk Score. Risk Impact, Risk Probability options and Risk Score calculations are listed below
* Identify the appropriate risk response strategy. List of response options are given below
* Develop Mitigation / Contingency plan as required
* Communicate the risks to appropriate stakeholders
* Continuously monitor and reassess risks, and implement mitigation or contingency plan
* Close the risk when the risk is not valid anymore

|  |  |
| --- | --- |
| **Risk Impact Level** | Following is the Risk Impact Scale:  1 - Low  2 - Medium  3 - High  4 - Very High |
| **Probability (Likelihood of Occurring)** | Following is the Risk Probability Scale:  1 - Very Unlikely  2 - Unlikely  3 - Possible  4 - Likely  5 - Very Likely |
| **Risk Score** | Calculated as Risk Impact \* Risk Probability |
| **Risk Response Strategy** | Following are the risk response options:  Accept  Mitigate  Reduce  Transfer  Avoid  Monitor |

## Risk Governance

<The objective of this section is to detail how Risk governance activities will be performed as part of the project>

* Risks identified during the project shall be monitored by the project team and discussed with the project stakeholders during the weekly status review meetings, and shall be reported in the Daily and Weekly status reports

# Test Deliverables

| **Deliverables** | **Role/s Responsible** | **Reviewers** | **Approvers** |
| --- | --- | --- | --- |
|  |  |  |  |