Information

Name:	Sock Shop
Description:	A socks-selling e-commerce demo application.
Version:	
Date Created:	2021-05-21T11:35:27.839
Git Commit:	
Git Tag:	
Git URL:	
OpenShift Cluster API URL:	
Created by Jenkins Job Name:	
Created by Jenkins Build Number:	

Risk Assessment for 'Sock Shop'

TABLE OF CONTENTS

1 PURPOSE

This document is an assessment of risks associated with the usage of the Sock Shop. Risks are identified based on requirements and functions of the system and classified according to predefined rules. This will serve as a basis for risk management strategies and measures during the system life cycle.

2 BASE DOCUMENTS

The risk assessment is based on the following documents:

Reference Document	Version	Prefix for Ref. No.
Combined Specification Document	null / 3-WIP	N/A All Ref. Numbers are unique
System and Software Design Specification	null / 2-WIP	

3 ASSUMPTIONS

None

4 RISK ASSESSMENT PROCESS

Section 4.1 gives a high level description of the risk assessment table (see section 5). Details and classification rules, for the values in columns that need additional explanation, are given in section 4.2.

4.1 RISK ASSESSMENT TABLE DESCRIPTION

The risk assessment table in section 5 comprises the following columns:

Column	Description
Risk No.	Identifier of the risk for reference within other documents
Reference No.	Unambiguous reference to a specific requirement, function or a group of requirements in a reference document. The prefix indicates the referenced document
Requirement / Function	Short description of requirement or function
GxP	Relevance of the requirement or function for GxP or non-GxP (e.g. business). See section 4.2.1
Description of Risks/Failures (or reason for GxP = No)	Description of possible risks or failures associated with the requirement or function. More than one risk or failure may be associated with a requirement or functionIf non-GxP risks are not evaluated, reason for classification as non-GxP is provided.
Prob. of Occurrence	Relevance of the requirement or function for GxP or non-GxP (e.g. business). See section 4.2.1
Severity of Impact	Possible impact of the failure if it is not detected. See section 4.2.2
Prob. of Detection	Most probable point in time when the failure will be detected in routine operation of the system. See section 4.2.4

Risk Priority Number (RPN)	Product of the individual factors which determine the risk based on relevance, impact, probability of detection and Prob. of Occurrence (optional). See section 4.2.5
Risk Priority	Categorized risk which is derived from the risk priority number RPN. 1 identifies highest risk priority and 3 lowest risk priority.
Proposed Measures	Proposed measures (e.g. additional test requirements, design requirements, functional limitations, and organisational or procedural measures) for risk mitigation. This entry is mandatory for priority 1 GxP risks and optional for all other risk priorities
Comments	Comments as applicable (optional)

4.2 CLASSIFICATION RULES

4.2.1 GXP RELEVANCE

The requirement or function is evaluated to determine if it is related to GxP. If there are both GxP and non-GxP risks, GxP is documented as it is the more relevant risk. However, the associated non-GxP risk should also be taken into account.

GxP Relevance	Value	GxP value in section 5	Option	Description
Yes	2	R2	n/a	The requirement is directly related to GxP regulated activities. Failures could lead to incorrect data, loss of data, deterioration of product quality, or risk exposure for safety of patients or customers.
No	0	N0	Non-GxP risks are not being evaluated	The requirement is directly related to GxP regulated activities. Failures could lead to incorrect data, loss of data, deterioration of product quality, or risk exposure for safety of patients or customers.
	1	N1	Non-GxP risks are evaluated lower than GxP risks	
	2	N2	Non-GxP risks are evaluated the same as GxP risks	

Each non-GxP risk can have a different option for evaluation since the RNP is computed automatically. Thus, no project-level evaluation option is used. The selection is done individually in each Risk Assessment task. The value contains the GxP relevance and the number used to compute the RPN.

4.2.2 PROBABILITY OF OCCURRENCE

This project does not use Probability Of Occurrence.

4.2.3 SEVERITY OF IMPACT

The severity of the impact of a possible failure is evaluated according to the following classes:

Severity of Impact	Value	GxP Impact	Non-GxP Impact (e.g. to cover business risks)
Low	1	No impact on product quality, patient safety, or data quality; no impact on data integrity is expected: no deviation from regulatory obligations or predicate rules	Low cost risk; no delay of regulatory processes
Medium	2	Product quality, patient safety, or data quality could be impacted; correctable impact on data integrity; potential; probability of a deviation from regulatory obligations or predicate rule	Medium cost risk; short delay of regulatory processes
High	3	Product quality, patient safety, or data quality will probably be impacted; uncorrectable impact on data integrity; deviation from regulatory obligations or predicate rules	High cost risk; significant delay of regulatory processes

4.2.4 PROBABILITY OF DETECTION

The most probable point in time when a possible failure is detected is classified according to the following table:

Probability of Detection	Value	Description
Inmediate	1	The failure is detected immediately when it occurs. The user is able to take immediate measures to correct the failure before any impact can occur.
Before Impact	2	The failure is not detected immediately by the user but later before it may have any impact. The effect of the failure may still be corrected or minimized by appropriate corrective actions.
After Impact	3	The failure will most probably not be detected before the expected impact occurs.

4.2.5 RISK PRIORITY NUMBER AND RISK PRIORITY

Calculate a risk priority number RPN by multiplying the values of the individual factors:

RPN = Value(GxP Relevance) * Value(Prob. of Occurrence) * Value(Severity of Impact) * Value(Prob. of Detection)

Assign the risk priority for the risk according to the following table:

RPN	**Risk Priority**
1-2	3
3-8	2
>8	1

A risk considered as non-GxP and not being evaluated will lead to a RPN = 0 and Risk Priority = 0.

4.2.6 PROPOSED MEASURE

Depending on the risk priority risk mitigating measures must be defined according to the following table. The System Owner must ensure that the defined measures are being implemented.

Risk Priority	**Requirements for mitigating measures**
1	Measures in addition to functional or requirements testing need to be defined, whenever feasible. Measures can be procedural measures (e.g. additional checks, four eyes principle, typically defined in a WI or SOP) or technical measures (e.g. additional technical checks, technical security measures).
2	Measures need only to be defined if the underlying functionality cannot be tested, or cannot be tested on an appropriate level.
3	In general no risk mitigating measures need to be defined.

5 RISK ASSESSMENT TABLE

Risk No.	Ref No.	Requirement/ Function	GxP (see 4.2.1)	Description of risks/failures (or reason for GxP = No)	Prob. Occur.	Severity Impact	Prob. Detect.	RPN	Risk Prio.	Proposed Measures	Comments
OFI1805-131	OFI1805-128	Story Continued	None	Summary:RA CONTINUED.	None	None	None	N/A	N/A	Mitigations: OFI1805-132 Tests: None	N/A
OFI1805-133	OFI1805-128 OFI1805-130	Story Continued TST CONTINUED	None	Summary:Risk Assessment - TST.	None	None	None	N/A	N/A	Mitigations: None Tests: None	N/A

The following table contains more information about the proposed mitigations:

Mit. No	Type	Mitigation description	Risk No.
OFI1805-132	mitigation	Mitigation CONTINUED	OFI1805-131

6 DEFINITIONS AND ABBREVIATIONS

6.1 DEFINITIONS

Term	Definition
Jenkins	Build engine supplied by cloudbees - part of OpenDevStack (BI-IT-DEVSTACK)
xUnit	Unit testing framework, aggregaults across multiple languages

6.2 ABBREVIATIONS

Abbreviation	Meaning
ODS	OpenDevStack
EDP	Enterprise Development Platform

7 REFERENCE DOCUMENTS

- Combined Specification Document (version null / 3-WIP)
- System and Software Design Specification including Source Code Review Plan (version null / 2-WIP)
- Functional and Requirements Testing Plan (version null / 3-WIP)

No further reference documents

8 DOCUMENT HISTORY

Version	Date	Author	Change Reference
1	See Summary of electronic document or signature page of printout.		Initial document version.

The following table provides extra history of the document.

Version	Date	Author	Reference
	See summary of electronic document or signature page of printout.		