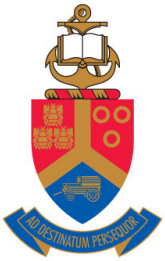


UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

# COS301
# Mini Project
# Architectural Requirements Specification

**Group 1B**


| | |
|---|---|
| David Breetzke | *u12056503* |
| Tienie Pritchard | *u12056741* |
| Ephiphania Munava | *u10624610* |
| Paul Engelke | *u13093500* |
| New Member | *uxxxxxxxx* |
| New Member | *uxxxxxxxx* |
| New Member | *uxxxxxxxx* |
| New Member | *uxxxxxxxx* |


**GitHub:**Visit

Version 1
March 7, 2015

# Contents

# 1 Access and Integration Requirements

[insert text]

# 2 Access Channels

[insert text]

# 3 Integration Channels

[insert text]

# 4 Architectural Responsibilities

[insert text]

# 5 Quality Requirements

## 5.1 Scalability

[insert text]

## 5.2 Performance Requirements

[insert text]

## 5.3 Maintainability

[insert text]

## 5.4 Reliability and Availability

[insert text]

## 5.5 Security

[insert text]

## 5.6 Monitorability and Auditability

[insert text]

## 5.7 Scalability

[insert text]

## 5.8 Testability

### 5.8.1 Type of Quality:

System Quality

### 5.8.2 Priority:

Critical

### 5.8.3 Description:

Testability measures how easy it is to create testing standards for a system and its individual components, theses standards are tested to evaluate if a criteria has been met. Thus software testability is the point to which the software system supports testing in some context. Hence if the software testability is high finding faults in the system is easier.

### 5.8.4 Stake Holder:

- Persons who operates the system : Administrator, Maintenance Operator and Tech-team.
- Persons who benefits from the system : Lectures, Teaching Assistance, Tutors, Students and Guest.

### 5.8.5 Context:

- Stimulus : The testing is performed by tester (these might be system testers, integration testers and even the end user).
- Artifact : The target of the attack can be the system or the data in the system.
- Environment  This attack can come from the user of the system or an outsider like a hacker.
- Response : The system has to authorize certain actions and responses for each of the given tasks.
- Response Measure : The measure of the system and it functionality before, during and after the attack.

### 5.8.6 Measurable Specification:

Understand-ability : The point at which the component of the system that being tested is self-explanatory.

- Separation of concerns : The point, at which the component of the system that's being tested has a well-defined responsibility.
- Observe-ability : The point, at which the component of the system thats being tested become possible to discern the test results.

**Component Under Test**
Is a test that restrictions the scope of the used software to a ration of the system that is being tested.

- Controllability : The point, at which the system thats being tested becomes possible to control the state of the component under test as required.
- Isolate-ability : The point, at which the system thats being tested becomes possible for the component under test to be tested in isolation.

## 5.9 Usability

[insert text]

## 5.10 Integrability

[insert text]

# 6 Architecture Constraints

[insert text]