Reproducibility and Audit Risk

# Executive Summary

## Objective

This report contains the findings and recommendations relating to reproducibility issues and audit risks in a specific data analytics project. The report also includes references to the code which has been partly re-written as per some of the recommendations in this report.

## Approach

An existing data analytics project was identified which covers some of the key data science tasks that a data analyst/scientist has to perform on a day to day basis. The chosen project’s objectives are to identify the top factors that are related to a driver’s alertness or lack of based on the dataset provided and choosing an optimal classifier from a bag of models that can predict whether the driver is alert or not alert using the top factors/predictors with highest accuracy.

The key themes on which the reproducibility issues and risks were identified are as follows:

* Version controlling of source
* Collaboration/Portability/Reproducibility
* Code Readability and Layout
* Coding & Naming Standards
* Literate Programming

## Highlights

The R code in which the project was written, was put together without any version control system and did not have any dedicated repository which presented the first challenge of reprodroducing the correct version of the code. The nature of the code structure and building process resulted in multiple occurrences of redundant codes, confusing variable naming conventions, multiple coding styles, missing/misleading code comments and insufficient code documentation.

Instances of coding errors were also discovered as part of the process of reproducing the projects. The technical review was limited to finding reproducibility issues and risks and excludes any recommendation on the appropriate methodology of model selection or model validation techniques.

This report contains the various reproducibility/audit issues and risks that were found in the review process, along with a number of recommendations for improvements that includes using source control tool, following one coding style and using appropriate coding standards/naming conventions, implementing defensive programming and advantage of using software containers. An excerpt of the original code is also included in the report along with the recommended changes to code to make it reproducible and more auditable.

# Introduction

## Project Introduction

The project, under review, was undertaken as part of practical work-related project experience in one of the MDSI (Master Data Science & Innovation) subject named Advanced Data Analytics Algorithms.

The dataset is a simulated observations consisting of tests taken by 100 vehicle drivers of both genders, of different ages and ethnic backgrounds, who have been sampled a total of 500 times against 3 key sets of variables (driver’s physiological attributes combined with vehicular and environmental attributes acquired from the simulated environment). There are 33 attributes in the dataset in total.

* Physiological (8 features) defined simply as P1 to P8.
* Environmental (11 features) defined simply as E1 to E11.
* Vehicular (11 features) defined simply as V1 to V11.

Each driver trail has been recorded in a simulated driving environment for a period of 2 minutes and an observation recorded every 100 milliseconds. Each driver’s trail has been defined uniquely and labelled at TrialID and every observation within each trail is defined uniquely and labelled as ObsNum.

The key objectives of the project are:

* Identify the key factors that explains most of the driver’s alertness or lack of
* Fit an optimal classifier from a bag of models that can predict whether the driver is alert or not alert, with highest accuracy.

The nature of the project is purely exploratory and the deliverables includes an analysis of the importance of features and a recommendation of an appropriate model that can be used to make predictions about the alertness of the driver.

The original deliverable included a detailed technical and recommendation report in the form of a word document and the R code, which was used in the analysis, supplied as an attached single R file.

## Review Approach & Scope

The idea of this review exercise is to identify the reproducibility issues and risks that could potentially become issues for reproducing the analysis.

Imagine a situation, where a Data Science team came across the project report and found it useful enough to invest time and resources to implement the project as a deployable model, all they have with them is an analysis that was done 3 years ago and a version of R code which probably ran fine 3 years ago but is not guaranteed to run the same, given there is no information on the environment it was run and the dependencies it had at that time.

The approach of this review is to simulate the analysis using the piece of given R code and identify the imminent issues with reproducibility of the analysis and also, in the process, to identify any key risks that can become reproducibility issues in the near future. That would involve simulating the analysis in more than one environment and different conditions/dependencies. The key idea behind this review is not only to reproduce the analysis but also be able to make it more maintainable and auditable.

The scope of the review is identified the issues and risks from the perspective of:

* Version Control
* Code Readability and Layout
* Coding Standards
* Literate Programming
* Code Portability

The review does not make any recommendations on the appropriateness of the modelling methodology or the model training or validation approach.

## Findings

Each of the findings will talk about the potential issue or risk and a separate section on recommendations on how to mitigate these issues and risks.

**No Source Control Tool**

The source code, documents and data, all together were zipped up and stored on google drive. Although, this is one form of source control but it is not an ideal way to version controlling the source. The project artifacts lacked a proper structure and different versions of code were found, stored as copies of the same file. There is no way of identifying which artifact is the latest version, which raises a concern whether the R code that was finally submitted was even a true copy of the latest version of the code. This is nothing stopping to carry on the analysis if there is no source control, but it is a key risk which in future could cause inconsistencies in the code and leaves you without the ability to undo and redo changes. Also, one loses the ability to track changes over time in case one needs to retrospectively look at the changes to review what worked and what didn’t.

**Inappropriate Central/Remote Repository**

Google Drive is not an ideal remote repository tool for hosting code repositories. The key thing missing in that setting is the ability to collaborate. Remote repositories specifically designed for controlling versions of code not only helps in sharing code among other developer/team members but also are ideal provides features of looking back in time for changes by all users and merging changes from two different users. Some of the code repository providers even have more advanced functionality of continuous integration and continuous deployment of the source. Again, having a central remote repository is not an issue but a key audit risk. Also, if several developers intend to work at the same time, then it will become an issue to consolidate everyone’s changes without investing significant time and effort and the resulting code still might be error prone.

**Missing info on package versions/ R version/ OS**

The project R code was built using the latest version of dependent packages at the time of writing the original code. It has been 3 years since then and today I was not able to re-install one of the packages mentioned in the source code. The dependent packages follow their own development cycle and might have seen various revisions since the original code was written. Fortunately, the package that I was not able to re-install is actually no longer needed in the code. Recording the version of the dependencies is a must and poses an imminent issue in the near future. Moreover, the machine/operating system it was built on has also changed, from a Window 10 OS to a macOS, the code did not travel well. Even though the code ran fine, I was not able to reconcile the results as documented previously to the current results that I am getting. Also, the version of R itself has progressed over the course of 3 years. Versions are important and requires attention of a proper version management tool that can snapshot the current state/version of OS/ dependent packages/ R version.

**Inconsistent Coding Practices**

Inconsistent style made it hard to understand what the different variables are used for and the naming convention had been arbitrary which breaks the flow of the reader/auditor who is trying to understand what the code is supposed to do. A neatly formatted code, consistent naming conventions makes it easier to read and understand the code. Also, as pointed out earlier, there are instances of code where some of the redundant code exists and could have been reviewed and removed from the final version of the code. Even though the code might run, but it presents a huge audit risk and costlier maintenance operations as the reader would have to spend a lot of time understanding the code.

**No particular programming paradigm**

Even though the project was exploratory in nature, there are instances where a functional programming approach could have been used. While it might work fine for sharing ad hoc analysis but it is essential to follow either an object oriented approach or a functional programming approach to build an industry standard solution. Hence, from reproducibility perspective I was able to reproduce the code but it poses a significant risk if the same code is adopted to build an industry standard model.

**Insufficient documentation**

As mentioned earlier, the code lacked functional programming and even where there was a function written, it lacked proper documentation. It was really hard to understand what the function does until you actually execute it. A function is meant to be a reusable piece of code and without proper documentation, a reader will be left with no choice but to write their own version of function, making the existing code redundant. Again, this is not an immediate issue but over time it might pose as an audit risk and the code becoming redundant. Even though the supporting report has some form of documentation, code itself is not self explanatory.

**Key Person Risk**

Only one person knew about the code and other artifacts, the developer. No other person can takeover and run the code independently. It simply cannot be reproduced without considerable effort.

## Recommendations

* Use source control tools like git for maintaining local repositories and Github or BitBucket for maintaining remote repositories. It is really easy to reproduce not only the latest code but also have the ability to go back in time and restore an older version of the code. These tools help in collaborating and working in a large team. These tools provide reviewers/auditor with capability to compare two versions and make informed decisions based on the differences. The re-written code has been maintained at github: <https://github.com/anuj-kapil/driveralertness>
* Adopt one style for coding and consistently use it across the code. Following one set of naming conventions and avoid giving useless and random names. Sample names in old code:

Sample names in new code:

Styler can be used to style the R code

Old Style:

New Style:

* Defensive Programming
* Assert statement was introduced to interrupt the execution early in case of input inconsistencies. This helps in building a fail-fast system and catches errors earlier than later and saves time and computation Assertions can be built into the code to fail fast in case of errors. This will save time and computation.

The following sample assertion was added in code:

* Functional Programming The problem can be broken down into smaller chunks of problems and repetitive code can be converted into a function to reduce the chances of introducing errors and make the program more readable
* Documentation While creating a function, it is essential to document what that function does and what input it takes and what to expect as an output from function and if possible include some examples of function usage. The roxygen2 package in R converts such documentation into user manual which is available as function help.

A sample documentation is shown below:

* Automate test for your functions While writing functions, a developer often tests the functions with some sample inputs. Record those sample tests into a function and run them everytime some makes a change to the function. This ensures no one breaks the existing functionality of the function.

Sample test:

* Record the version of the packages used in the R code Dependent Packages are continuously developed and newer versions are often susceptible of breaking the existing functionality in how you have implemented that package. Packrat in R is used to maintain a snapshot of the dependent packages loaded

Packrat

packrat is a package for managing R packages. The basic idea is that instead of using the default location to install packages that are shared across all R code, each project gets its own private library of packages. That way, package versions are independent from project to project. When you want to share a project with other collaborators, you may want to ensure everyone is working with the same environment – otherwise, code in the project may unexpectedly fail to run because of changes in behavior between different versions of the packages in use. You can use renv to help make this possible. When using renv, the packages used in your project will be recorded into a lockfile, renv.lock. Because renv.lock records the exact versions of R packages used within a project, if you share that file with your collaborators, they will be able to use renv::restore() to install exactly those packages into their own library. This implies the following workflow for collaboration:

Sample snapshot and restore

* Reproducibility

Containers can be used to create a reproducible version of your code/package.

Docker image with the snapshot was created first using the base image of rocker/studio which has all the necessary libraries run R and rStudio ide and on top of that we have installed all the dependent packages required for our project. This image is then configured in GitHub continuous integration workflow to regularly update with our project package on each push to the repository.

This could be configured differently to manage any updates to dependent packages in our project. Let assume someone adds a dependent package in our project, then this solution won’t work as our base Docker image is a static snapshot of all the dependent packages that our project needs today. This defeats the purpose of using packrat as on each build of package the packrat takes a new snapshot of the dependent packages which isn’t getting updated in the project base Docker image. But it can be configured to do the snapshot restore on each push to the repository.

Also, the GitHub actions could be configured to run the testthat tests on the project repository to find an issues with package.

Docker

The rocker set of docker images has made it much easier to do reproducible data analysis with R. By using one of the rocker images, we can ensure that the computing software environment, R version, and package versions are always the same, no matter where the code is being run.