bmm compliance

26 October 2015

To:	**Greyhound Breeders, Owners & Trainers Association Ltd (GOTBA)**		
Attention:	**Jim Absalom**	**Email address:**	**gotbav@gmail.com**
From:	**Anna Fernando**	**Total pages:**	9
Subject:	**Audit of Box Draw program**		

If there were any difficulties in transmission, please telephone +61 3 9895 9888

This document and any following pages are intended solely for the named addressee, are confidential and may contain legally privileged information. The copying or distribution of them or any information they contain, by anyone other than the addressees, is prohibited. If you have received this document in error, please let us know by telephone, and then return it by mail to the address below. We shall refund your costs of doing so.

Dear Jim,

Please find attached our report of the audit conducted on Greyhound Racing Victoria’s box office draw software.

Please do not hesitate to contact us if you require further information.

Fernando

Anna Fernando

VP - Operations

Executive Summary

GOTBA has engaged BMM Australia Pty Ltd (BMM) to carry out an audit of Greyhound Racing Victoria's computer Box Draw program.

BMM's findings were as follows:

- We are able to confirm that the automatic box draw program operates in accordance with the rules for Box Draw in Greyhound Racing and that the automatic box draw program generates random box draws.
- There is no evidence that the method of operation of the program has any influence on the outcome of the programs. There is no evidence that the box draw program is influenced by details of the connections of the entrants nor any previous performance or draws for the entrants.
- The automatic box draw program could not be re-run at all.
- The automated box draw program is used for each box draw, unless a manual box draw is specified in race set up. It was not possible to enter the box draws when a random box draw was scheduled.

Fernando

Anna Fernando

VP – Operations

Table of Contents

1 INTRODUCTION

GOTBA has engaged BMM Australia Pty Ltd (BMM) to perform an audit of Greyhound Racing Victoria's box draw software. This software is part of GRV's Fast Track system.

2 SCOPE OF WORK

The purpose of BMM's audit was to confirm that the box draw program is fit for purpose. In particular, BMM's independent review focused on the following areas:

- Confirm that the box draw program will generate automatic random box draws.
- Confirm that there are sufficient validation steps to ensure that the automated box draw program is used for each box draw.
- Confirm that the box draw is not influenced by factors such as the order in which greyhounds are entered in the input screen, trainer or owner.
- Confirm that the random number generator used in the random box draw is reset correctly.
- Confirm that the box draw cannot be re-run without sufficient security controls.
- Provide recommendations as appropriate where tighter controls in the process can be implemented.

3 THE REVIEW PROCESS

BMM reviewed the computer program source code for the automatic box draw program supplied by Greyhound Racing Victoria. BMM also conducted an analysis of box draw results generated by the software.

In addition, the reviewer observed the new box draw program being used for the box draw for a meeting and went through a number of test scenarios with the grader. The test scenarios included tests with the random box draw process and security around the box draw processes.

4 EVALUATION

4.1 Box Draw Criteria

The only criteria used by the “BOXDRAW” program for allocating starting boxes are those provided for in the rules of Greyhound Racing. Each dog has equal standing and is randomly allocated a box from those available. Where there is less than a full field, nominated boxes are excluded from the Draw.

The order of entry of dogs into meetings and/or races has no influence on the Draw. The box draw program does not use any information about the dogs to influence the outcome of the Draw. This includes dog name, owner, trainer, past draws and their race form.

The box draw program does not consider past performance or previous box draw information when performing the Box Draw.

It should be noted that the rules of Greyhound Racing Victoria require that the draws be random, not that they be fair. We confirm that each draw is carried out in complete isolation of all other draws and, in particular, of the draw history for a given dog, trainer or owner.

4.2 Box Draw Security and Audit Trail

The box draw program operates under sufficient security in that only graders are provided with access to set up the race in preparation for the box draw. The box draw is then automatically scheduled based on the times set by the grader for the box draw to commence. The grader has no access to a function that actually performs the box draw. Interested parties are able to login and observe the program in operation and the result of the box draw is displayed to all. Once the box draw is run, the grader has no ability to re-run the box draw.

It should be noted that there is no ability in the system to re-run a box draw. In the event an error is found with the box draw, the grader seeks written permission from senior management to have the draw re-run manually. The result of the draw is updated by the Information Technology department in the back-end of the system. A paper trail is maintained by GRV.

A change control process has been introduced that covers all changes to the Fast Track system. This ensures that all changes to the system will be controlled and authorised, with a manual record trail in place.

It is noted that a mechanism to store an audit trail of the results in the new system has not been implemented. It is recommended that this be implemented in a future release.

4.3 Box Draw Software

The source code concerning the random box draws was examined. No bias was found to be introduced in the draw mechanism.

All races for a meeting have their boxes drawn at once, one after another. If a race is handicapped, then the runners in the race are grouped by their respective grade. Each group in order is randomly drawn from, so that if the first group has 3 dogs, the first 3 boxes are randomly assigned to them. Then if the next group has 2 dogs, the next 2 boxes are randomly assigned, and so on. For non-handicap races, all boxes are randomly assigned to the runners. Besides the grouping by handicap, no dog or box is assigned any bias over the others.

If there are reserve dogs, they are assigned boxes at the end. If the race is handicapped, then the reserve dogs are assigned boxes randomly. If it is not handicapped, then the reserve dogs are assigned boxes in order of their "rank" and "placed rank".

4.4 Box Draw Random Number Generator (RNG)

The RNG used by the Box Draw Service is the Random class provided by the .NET framework, wrapped in a class designed to provide thread safety. A source code review of the RNG and statistical testing of sample output was conducted.

4.4.1 Description of RNG

The RNG is a subtractive random number generator. The RNG state consists of a table of 55 32-bit integers, along with two indexes into the table that are incremented on each call. Integers in the range of [0, 2^{31}-1) are produced by the RNG.

4.4.2 Initialisation

The RNG's state is initialised using the system's tick count, an integer that contains the number of milliseconds since the system started. This means that if the RNG is initialised around the same time after starting the system each time, the number of possible starting states will be a much limited subset of all the possible RNG states.

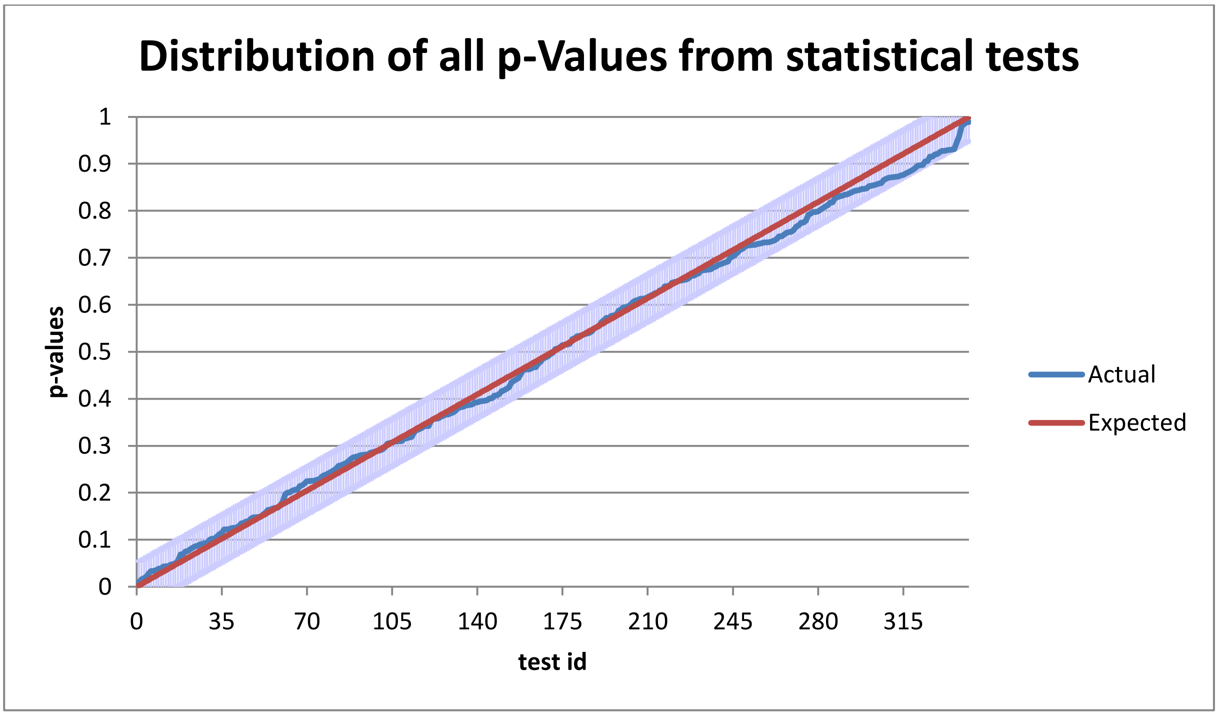
4.4.3 Scaling Algorithm

When a number is drawn in a required range (e.g. a number between 1 and 8), the RNG draws the next random number in its sequence, divides it by the range of the RNG (2^{31} – 1) and multiplies it by the required range. E.g. $scaled\ number = \frac{next\ random\ number}{2^{31}-1} * 8$, (+ 1 to make it between 1 and 8, instead of 0 and 7). This introduces a small bias as the required range will not divide evenly into the RNG's range (unless the required range is 2^{31} – 1 itself). Also, the use of division by a number that isn't a power of 2 is likely to introduce slight rounding errors. However, the size of any bias introduced by these issues will be negligible for the ranges used (up to 8), and would take billions of draws to be noticeable.

4.5 Statistical Tests

Statistical tests were performed on the output from simulations of the RNG. Sets of numbers of varying sizes from 500 to 20,000,000 in the ranges of 32, 52 and 111 were generated three times each and tested. Most tests passed, except for the Gap Test on the larger sample sizes. Given that the RNG passed the more rigorous Diehard tests, and the purpose of this RNG, the failure of the Gap Test is not considered significant. Without the Gap Test results, the remaining tests pass at the 95% and 99% confidence intervals.

The chart below shows the distribution of test result probabilities for all tests except the Gap Tests, and shows an expected linear distribution of results.



4.6 Re-draws and manual overriding of Draws

We confirm that the functionality exists to prevent races from being re-drawn by the automatic box draw program. As stated previously, there is no ability to re-run the automatic box draw program.

The new system also has the ability to enter box draw results where the box draw has been performed at the track i.e. for a final race. This functionality is only available to stewards and graders. It is only activated for a race where the race is set to 'manual' in the race calendar. The manual box draw could not be used for races set to 'random', nor could it be repeated.

5 SUGGESTIONS FOR TIGHTER CONTROL

In the previous system, the manual box-draw program sends an e-mail to senior management when it is run, asking for authority to be verified. A grader would need two e-mails giving authority before he could continue to perform a manual box draw. This functionality has not been implemented in the new Fast Track system.

The results of all box draws are stored in the database. No audit trail is created to keep track of any changes made to these records. The audit trail should also record the fact that a manual draw is performed.

BMM reviewed a manual change control policy which has been implemented to ensure that all changes to the system or database are approved and controlled with manual records.

It is our recommendation that a feature to alert senior management when manual box draws are run and an audit trail for box draw records be implemented in a future software release.

6 SUGGESTIONS FOR IMPROVEMENTS TO THE RNG

Although the RNG implemented is in BMM's opinion fit for its intended purpose, it could be replaced with a better implementation to provide more statistically random results.

There are two options that are recommended:

- Use a different non-secure RNG, such as the well-known Mersenne Twister algorithm, and manage the RNG's state between calls (see Initialisation and Cycling below); or
- Use a cryptographically secure RNG, such as the RNGCryptoServiceProvider that is provided by the .NET framework.

6.1 Initialisation

If the chosen RNG requires seeding, the initial seed should be changed to something that uses more sources of entropy, such as the RNGCryptoServiceProvider class (which in turn does not require seeding). The RNG's previous state, where applicable, should be restored on subsequent start-ups of the system in order to keep re-initialisation to a minimum. Otherwise the output of the RNG becomes too dependent on the initialisation method.

6.2 Cycling

Non-secure RNGs should be cycled randomly in the background where possible in order to keep the next output unpredictable.

6.3 Unbiased Scaling

Care should be taken when scaling a raw RNG number to a number in a given target range so that no bias is introduced. The range of the RNG's raw numbers should first be reduced to some multiple of the target range. There are many ways to do this, but they all generally require discarding and redrawing raw numbers whenever they fall outside of this reduced range.

7 CONCLUSIONS

We are able to confirm that the automatic box draw program operates in accordance with the rules for Box Draw in Greyhound Racing and that the automatic box draw program generates random box draws.

There is no evidence that the method of operation of the program has any influence on the outcome of the programs. There is no evidence that the programs are influenced by details of the connections of the entrants nor any previous performance or draws for the entrants.

The automatic box draw program and manual box draw program could not be re-run at all. There are sufficient validation steps to ensure that the automated box draw program is used for each box draw, unless a manual box draw is scheduled for the race.