Multi-Jurisdictional Testing Framework

Date of release / version	Version History	Participating jurisdictions
November 2015 – V 1.0	Initial release – Test lab standards v1, RNG v1	Alderney; Isle of Man; Great Britain; Denmark;
	List new standards added; Describe changes made to any existing standards.	If new jurisdictions are added, version will increase to include them.

Framework contact: iagr@iagr.org

Purpose

To establish a framework, agreed between the participating jurisdictions, for the independent testing of remote (online) gaming product.

Testing performed to the standards contained in this framework will be recognised by the participating jurisdictions.

Scope

For the first release of this framework, the scope is restricted to the testing of random number generators (RNG) for use in remote gambling, and to the reporting of RNG testing results. The framework also outlines good practise guidelines for testing laboratories to adhere to.

It is intended that the framework scope will be increased as new aspects are agreed and incorporated.

Background

It is increasingly the case that gambling regulators are utilising the services of outsourced specialist testing laboratories for the purpose of game fairness testing. To date, each jurisdiction has generally developed their own technical standards and testing requirements and appointed these external specialist testing laboratories to carry out testing against those standards. Although the individual technical standards often differ between jurisdictions, there is a core element that is common and the goal of regulators is the same – that is to ensure the fairness of gambling products offered to players.

Often in the remote industry, it is the same product (game) that is being offered into each jurisdiction without modification apart from some contextual functionality, such as the language or player account and reporting functionality. Where there are areas in technical standards that are common between regulators, it makes sense to agree on an approach for the testing of that product. Different regulators with common goals could each benefit from sharing what they consider best practise in order to develop a common agreed framework.

Process

This framework is not intended to replace existing requirements in any of the participating jurisdictions. It is intended that, where a jurisdiction has signed up to this framework, they will recognise testing performed against this standard for the purposes of their RNG testing requirements. That is to say that, once an RNG has been tested against this standard, it would not be necessary to duplicate testing in order for it to be considered for release in any one of the participating jurisdictions.

The labs performing the testing must be recognised as suitable to carry out remote product testing in each of the participating jurisdictions in order for it to be considered for release in those jurisdictions. Where a testing lab is only recognised in a subset of the participating jurisdictions for this framework, then testing performed by that lab would only be valid in those subset jurisdictions (unless stated otherwise by any other participating jurisdiction).

Once a product has been tested in accordance with this framework, gambling operators would still need to adhere to the individual requirements relating to the release of new product in each jurisdiction. For example, where a jurisdiction requires a copy of the testing report or any other supporting forms or information, then operators would need to follow those processes and include this framework's testing evidence as required.

Agreed standards

Attached as appendices are the agreed standards.

Appendix A – Testing facility operational guidelines. This attachment outlines the operational processes a regulator would expect are in place within a testing laboratory. It covers aspects such as the organisation's structure and independence; personnel and infrastructure; and general procedures and operations.

Appendix B – Random number generator (RNG) testing and reporting. This standard outlines the general characteristics of RNGs and how they should be tested. It also details what information should be included in the testing report. The aim of this is to ensure all testing laboratories are testing to an equivalent standard, and the scope and results of testing is transparently documented.

Appendix C – Game testing standards (not yet included)

Appendix A - Operational guidelines for Testing Facilities

September 2015 v1.0

Contents

BACKGROUND

For a regulator to accept the testing performed by a testing facility in another jurisdiction, they would need a level of assurance over the suitability and capability of that testing facility. This document aims to outline the areas that a regulator would expect to be present in a testing facility participating in testing exchange. It assumes any outsourced testing facility is already subject to the regulation of the host jurisdiction. This means that the testing facility has already undergone the 'on entry' probity, independence, competence and financial fitness checks required by the local regulator (i.e. the testing facility has undergone a licensing or similar approval process).

Whilst this document does not specifically cover the 'on entry' checks a regulator would perform on a testing facility[1], it will touch on similar areas as part of ongoing suitability. It will cover in more detail the independence and competence areas as these are different to what is expected of a gambling operator.

It serves as a guideline of the operational aspects that a testing facility should have in place. The regulator's requirements placed on a testing facility may differ within each jurisdiction and local legislation will always take precedent.

1. ORGANISATION

1.1. Alignment / Independence

The testing facility must be independent and not aligned to any party in the gaming industry, e.g. gambling software developers, operators and equipment service providers. The testing facility may be an adjunct to a regulatory body.

The testing facility must not:

a) enter into any conflicting commercial dealing with a gambling operator;
b) have any direct or indirect pecuniary interest in a gambling operator;
c) participate in or be involved in a gambling operator's design, manufacture, selection, purchase, supply, installation, service or operation of any gambling products or services anywhere in the world.

Clauses 1.1(a) and 1.1(b) do not apply where :-

a) the testing facility is testing, evaluating and certifying gaming equipment in accordance with its accreditation as an testing facility;

   Nb. It is acknowledged that testing facilities often provide a range of services not related to fairness testing. These are permitted providing such work does not affect the impartiality of any testing services offered.

[1] Those checks are similar to what would be conducted for a gambling operator's licence application and is outside the scope of this work (Note: a licence application form produced by IAGR is available on the website for this purpose).

1.2. Continuity of supply

The testing facility must demonstrate a sufficiently stable and continuing business, such that a regulator may rely upon it for the supply of testing services to the gaming industry over an adequate period of time.
Note: It is not uncommon for a testing facility to generate some of its business from sources outside the gaming industry.

1.3. Professional liability indemnity insurance

The testing facility must carry an appropriate level of professional liability indemnity insurance or ensure adequate arrangements are in place to manage any liability resulting from the provision of testing services.

1.4. Organisation and management structure

The testing of gaming equipment is complex and requires an understanding of the industry at management and operational level and specific technical skills.

The testing facility will be required to satisfy the regulator that its management possesses an adequate understanding of the gaming industry, the major issues involved, and that it is organised appropriately to be able to address those issues.

The testing facility must demonstrate that it is capable in the areas of:

a) understanding and knowledge of the gaming industry;
b) understanding the needs for equipment and facilities;
c) controlled and documented procedures;
d) testing rigor;
e) confidentiality; and
f) regulatory compliance.

such that the regulator is confident that the organisation fully understands its commitment and is able to provide testing services to the gaming industry.

The organisation must be capable of completing test and evaluation functions without the need to assign, delegate, subcontract or otherwise engage any person not directly employed by the organisation to carry out the testing or evaluation of gaming equipment except for :-

a) the testing of electromagnetic, electrostatic, radio frequency, magnetic or similar interference;
b) testing against electricity standards;
c) information security or other none gambling specialist areas. Where specialist functions do require outsourced assistance, notification must be given to the relevant regulator.

1.5. ISO/IEC17025 Accreditation

The testing facility must be accredited to ISO/IEC 17025[2] by an accreditation body that is a Signatory to the ILAC Mutual Recognition Arrangement in the field of Information Technology Testing for class 22.02 Gaming Software Tests.

If the testing facility is in the process of being assessed by an ILAC accreditation body for such accreditation, they may still be able to commence testing work however accreditation must be obtained prior to the issuance of testing certificates.

Note: Accreditation to ISO/IEC 17025 will mean that the organisation operates in accordance with ISO 9001 standards for quality management systems.

1.6. Compliance Committee

The testing facility must establish a Compliance Committee which is empowered and appropriately staffed to undertake probity investigations, investigate business policies and practices as they relate to the testing of gaming equipment, and to investigate instances of the improper or inadequate conduct of evaluating, testing and certifying gaming equipment.

The Compliance Committee will undertake investigations as requested by the regulator, and provide the results of those investigations in written reports to the regulator.

2. PERSONNEL

2.1. Skills and Qualifications

It is expected that the testing facility will employ appropriately qualified, competent and experienced staff having the relevant skills and qualifications, such as:

a) Computer science/programming;
b) Mathematics/statistics;
c) Electrical/electronic engineering;
d) Data communications and encryption;
e) Quality management; and
f) Information security.

2.2. Quality Manager

As required of a quality-accredited organisation, the testing facility must have a designated Quality Manager.

[2] ISO/IEC 17025 is the 'General requirements for the competence of testing and calibration laboratories', as issued by the International Organization for Standardization.

The Quality Manager will have ultimate responsibility in ensuring the consistent quality of deliverables, however, this responsibility may be delegated to other appropriate and independent members of staff.

The Quality Manager will have the right to refuse to release a deliverable if, in his or her opinion, it does not meet the organisation's requirements for quality.

2.3. Backup for key personnel

The testing facility must demonstrate that it has appropriate policies and programs to ensure that the required skills and qualifications can be provided by more than one staff member. This requires that suitably trained 'back-up' staff are available when key personnel are unavailable.

2.4. Cross Training

The testing facility must have in place procedures for transferring specialised knowledge from key personnel to other personnel in the organisation.

2.5. Probity

The testing facility will have procedures and maintain records to ensure that all principals, directors and employees involved in testing satisfy the requirements of the regulator in regard to personal probity and that employees do not have vested interests in any aspect of the gambling industry.

2.6. Personnel Induction

The testing facility will have in place procedures to ensure that:

a) all personnel have satisfied the requirements of the regulator in regard to any probity checking and the obtaining of any necessary licences or approvals before commencing work on the testing of gaming equipment;
b) all personnel are trained to comply with the organisation's quality management systems shortly after commencing employment;
c) all personnel are familiar with the organisation's code of conduct;
d) details of any change in principals, directors and testing personnel are notified to each relevant regulator including, for commencing principals, directors and staff, details of nature of and jurisdiction where probity checking was satisfied.

3. INFRASTRUCTURE

3.1. Security and Access Control

The testing facility's test environment must be controlled to allow access to authorised employees only or authorised third parties, and all equipment, samples and records of testing, whether in a physical or electronic form, must be:

a) maintained in a secure environment, and
b) controlled to allow access to authorised employees only.

3.2. Record Keeping

The testing facility must retain all records[3] associated with the testing of gaming equipment.

All such records must be:

a) retained for a period not less than five years;
b) stored in or transferred to a format which is accessible by the regulator and does not alter the content of the records; and
c) protected from unauthorised access.

3.3. Test Equipment and Tools

The testing facility must have appropriate test equipment, devices and software for the testing of gaming equipment. It is highly desirable that the testing facility provides a testing environment which is representative of the infrastructure and conditions that will be found in operation. The testing facility must test in an environment that accurately reflects the intended live environment. If it's necessary to replicate an eGambling system or to be able to supervise a build performed on an operator's equipment, then the necessary arrangements must be within the testing facility to allow for this.

Where remote connection to an operator's system is required, the testing facility must ensure:

a) Records of the system infrastructure, environment variables and versions of software are kept;
b) That there are technical means of determining remotely, beyond reasonable doubt, that the systems that are subject to compliance testing are the same as, or representative of, the systems to be put into production.

[3] Records' includes all correspondence with relevant parties and submission materials (or a way of verifying the authenticity of any copy of materials).

4. PROCEDURES AND OPERATIONS

The testing facility must follow documented procedures and methods suitable for testing gaming equipment to standards and legislation of or similar to those required by regulators.

Alternatively, the testing facility may demonstrate its capability to develop documented procedures and methods to address such requirements, using examples taken from another relevant field.

4.1. Technical Standards

The testing facility must demonstrate a knowledge of and capacity to test gaming equipment against relevant technical standards and/or incorporated documents which may apply to such equipment.

4.2. Procedures for testing

For the **fairness testing of games of chance**, the testing facility must have or be capable of developing test procedures and methods in the following areas:

a) game design and implementation;
b) random number generators;
c) statistical characteristics and probability;
d) game rules and return to player verification;
e) progressive jackpots;
f) peer-to-peer;
g) program code and software compilation; and
h) software verifiability and reproducibility.

For **eGambling platform testing**, the testing facility must have or be capable of developing test procedures and methods which cover the testing of the following areas:

a) customer registration and accounts;
b) data gathering, player tracking and bonus points systems;
c) centralised progressive jackpot controllers;
d) common wallet systems;
e) transaction logging and reporting;
f) communication protocols and encryption;
g) network traffic; and
h) software verification.

Where **information security reviews** are performed, the testing facility must have or be capable of developing test procedures and methods which cover testing of the following areas:

i) IT governance;
j) physical and logical access controls;
k) backups and system recovery;
l) audit logging and reviews; and
m) software change and release management.

The testing procedures and methods must be able to verify the correct transfer of data between the various layers of an eGambling system (operating systems, networks, applications and databases) and that each interface correctly processes data.

Note: The operation of gaming equipment will, from time to time, indicate problems with systems that are already in the field. The testing facility must be able to re-test games or equipment to determine whether the identified problems are present in these other previously tested items.

4.3. Cooperation with regulators and key event reporting

Regulators expect testing facilities to work in an open and cooperative way and to inform the regulator of any matters they would reasonably need to be aware of in exercising its regulatory functions. The testing facility must ensure they are able to discuss any aspect of gaming equipment and software testing with the relevant regulator in the jurisdiction the product is being tested for.

Matters that may have a material impact on the testing facility's business or ability to conduct testing should be notified to the relevant regulator as soon as reasonably practicable, include the following:

a) Relevant changes to the circumstances of the organisation or the individuals employed by the organisation.
b) Any investigation by a professional, statutory, regulatory or government body into the testing facility's activities, or the activities of a person occupying a key position employed by them, where such an investigation could result in the imposition of a sanction or penalty which, if imposed, could reasonably be expected to raise doubts about the continued suitability to test gambling equipment.
c) The commencement of investigations by an internationally recognised accreditation body into your conduct as a testing facility or your testing of gambling systems.
d) The suspension or revocation of the testing facility's ISO 17025 accreditation.
e) Any breach in the testing facility's information security where that adversely affects the confidentiality of client data.
f) Any other matters that have a material impact on the business or on the ability to conduct its business.

Testing facilities should have a whistle blower policy in place allowing any member of staff to report issues of concern to management or directly to the regulator. All testing facility staff members are to be made aware of the communication process they can use to report integrity concerns; for notifying the regulator, they should be issued with a contact email address of the regulator within each jurisdiction for whom they provide testing.

5. GLOSSARY

- Gaming equipment: Gambling product, software or ancillary equipment developed for gambling.
- Gambling Operator: A gambling software developer or a gambling operator that provides remote gambling facilities.

September 2015

Randomness

Regulatory strategy for testing and certification

1. Introduction

This document establishes a strategy relating to random numbers, whether determined by a pseudo-random number generator (pRNG) usually in software, or a random number generator (RNG) by a suitable physical phenomena (electrical, mechanical, radioactive, etc) – all being RNGs for the purpose of this document.

The purpose of this document is to establish generic RNG requirements and a minimum approach for their testing and certification by testing facilities. Following this framework will allow regulatory authorities to readily compare RNG certifications from other jurisdictions and different certification organisations.

2. RNG Requirements

2.1. RNG

2.1.1 General

Random number generation and game results must be 'acceptably random'. Acceptably random here means that it is possible to demonstrate to a high degree of confidence that the output of the RNG (or pRNG), game, lottery, or virtual event outcomes are sufficiently unpredictable through, for example, statistical analysis using generally accepted tests and methods of analysis. Adaptive behaviour (i.e. a compensated game) is not considered appropriate.

2.1.2 Attributes

RNG's should be capable of demonstrating the following qualities: the output from the RNG is uniformly distributed over the entire output range and game, lottery, or virtual event outcomes are distributed in accordance with the expected/theoretical probabilities.

2.1.2.1 Software

Software pseudo–random number generators must demonstrate the following qualities:

a. the output of the RNG, game, lottery, and virtual event outcomes should be unpredictable, for example, for a software RNG it should be computationally infeasible to predict what the next number will be without complete knowledge of the algorithm and seed value;

b. random number generation does not reproduce the same output stream (cycle), and that two instances of a RNG do not produce the same stream as each other (synchronise);

c. any forms of initialisation, seeding and re-seeding used do not introduce predictability;

d. cycle (produce output) in the background, unless specifically designed to work "on demand"; and

e. seeding sources should be demonstrably random sources of entropy.

2.1.2.2 Hardware

For games or virtual events that use the electrical, mechanical, or physics phenomena to generate the outcome of the game (hardware RNGs), the hardware RNG used should be capable of meeting the requirements in section **2.1.2.1** 0 where applicable and in addition:

a. mechanical components should be constructed of materials to prevent decomposition of any component over time (e.g. a ball shall not disintegrate);

b. the properties of physical items used to choose the selection should not be alterable; and

c. players should not have the ability to interact with, come into physical contact with, or manipulate the electrical, physics, or mechanical derivation of the results.

Where a hardware RNG utilises a software pseudo-RNG for failover purposes, the pRNG must meet the requirements of section **2.1.2.1**.

2.2. Mapping & scaling

Any scaling applied to the output of the random number generator maintains the qualities in section **0**.

Degrees of freedom of the output should be verified by standard methods.

2.3. Use of random numbers

When random numbers, scaled or otherwise, are received, e.g. following a game requesting a sequence of random numbers, they are to be used in the order in which they are received. For example, they may not be discarded due to adaptive behaviour.

Numbers or sequences of numbers are not to be discarded, unless they fall outside the expected range of numbers required by the virtual event – such an occurrence should result in an error being logged and investigated.

Restricting adaptive behaviour prohibits automatic or manual interventions that change the probabilities of game outcomes occurring during play. Restricting adaptive behaviour is not intended to prevent games from offering bonus or special features that implement a different set of rules, if they are based on the occurrence of random events.

2.3.1 Monitoring

The output of RNGs should be monitored with real-time statistical tools. The purpose of monitoring is early detection of abnormal statistical behaviour enabling timely appropriate remedial action. Any abnormalities should result in an error being logged and investigated.

Best practice monitoring will include independent mapping between RNG output and game symbols should verify game symbol usage. RNG output –v- game symbols logs may be maintained and verified as a non-real-time monitoring exercise.

2.3.2 Security

Security of generated numbers must be maintained through to their usage (e.g. numbers are not transmitted unencrypted between RNG server and game server). RNG output and game symbols should be used immediately and should not be unnecessarily stored in memory before use.

Unless the software is designed to operate differently, the seeding or restarting of RNGs should be minimised.

3. Reporting results of RNG testing

RNG reports should contain all pertinent information so as to enable vendor-to-vendor and tester-to-tester comparisons and to enable the regulator to clearly see the scope of testing.

The purpose of the following isn't to mandate the format of a test report; it is to outline the minimum elements that would expected to be contained within reports. How the lab selects to display the information is up to them (in table format, different order to that outlined below, etc), so long as all the minimum information is present.

3.1 Test Laboratory Details

Contact details of test laboratory, physical location(s) where testing was performed, date(s) of testing including any resubmissions required and certificate reference number – certification signed off by test supervisor.

3.2 Executive summary

3.2.1 Introduction

Introduction about the supplier, system (online casino, poker, lottery) utilising the RNG, jurisdiction and applicable compliance standards/requirements (including date and version).

3.2.2 Description of RNG

Briefly describe the RNG and its use in the gaming/lottery system.

3.2.3 Scope of testing

NOTE: Vendor generated output testing only is an unacceptable scope.

In scope/out of scope technical standards/features of RNG or RNG related features of the gaming/lottery system.

Scope should specifically state the basis of the findings:

a. *vendor supplied output testing (include industry standard hash of the sequence provided);*

b. *tester generated output from vendor supplied source (include hash of the source code provided and descriptive identifiers of build and operational environment specifications provided by vendor and hash of the documents stipulating such matters);*

c. *source code review;*

d. *theoretical basis of algorithm and supporting crypto-analysis evidence; and/or*

e. *limitations of assurance because of scope of testing (range, degrees of freedom, seeding, re-starting, etc) likely foreseen by tester.*

3.2.4 Limitations of use of RNG

Any limitations on the use of the RNG should be cited. This might include but not be limited to:

- *the acceptable degrees of freedom (DOF) permitted for the RNG,*
- *whether it is suitable for use with / without replacement, and*
- *any dependency on operating system functionality that, if modified, could impact the operation of the RNG (e.g. Java SecureRandom).*

3.2.5 Conclusion

Conclusion of evaluation – RNG complies or RNG complies under certain conditions.

3.3 Detailed test results

3.3.1 Test methodology

> It is anticipated that NIST tests and / or Diehard Tests shall be used when evaluating random sequences. The qualified tester will choose the appropriate tests on a case by case basis depending on the RNG under review.

The RNG has been evaluated by performing the following tasks:

1. *Review of RNG documentation to understand the implementation of RNG in the gaming system.*
2. *Research about RNG algorithm/hardware to ensure there is no publicly known weakness or vulnerabilities associated with the RNG under evaluation.*
3. *Review of source code to verify that the implementation of RNG is in accordance with the RNG documentation.*
4. *Statistical testing of raw output of RNG and scaled/shuffled decks data.*
5. *Any issues or non-compliance are reported to the supplier who resolve these issues. Once the issues are resolved, these are re-evaluated to confirm the non-compliance has been addressed adequately.*

Complete the table below using the following column values.

Req No. *Compliance requirement number*

Req Description. *Description of the compliance requirement*

Compliance Status *Comply/Does Not Comply/Not Applicable/Out of Scope*

Comments *Describe how RNG complies with the compliance requirement OR why the RNG does not comply OR why the compliance requirement is not applicable OR why the compliance requirement is out of scope*

Req No.	Requirement Description	Compliance Status	Comments
2.1.1	General		
2.1.2	Attributes		
2.1.2.1	Software pRNGs		
a			
b			
c			
d			

Req No.	Requirement Description	Compliance Status	Comments
e			
2.1.2.2	Hardware RNGs		
…	…		
2.3.2	Security		

3.4 Identification of RNG

Include the following information about the RNG evaluated in this section.

3.4.1 Hardware RNG

Manufacturer:

Model:

Serial number:

Interface type (USB, serial):

Number of modules and configuration: *automatic failover, manually switch to backup module, concurrent use of multiple modules*

URL of manufacturer's website for this module:

3.4.2 Software RNG

Supplier:

Version details (unique identifier, version number):

Environment particulars: *Platform supplier and version hosting the RNG (if applicable), operating system details.*

RNG Algorithm:

Language of implementation (C++, Java, etc.):

File names and industry standard hashes

List hashes of source code files and binaries (if applicable) of the RNG evaluated.

For hardware implementation of the RNG, include hashes of the code (drivers, scaling, etc.) used to implement the RNG.

For software RNG, include hashes of the code for RNG algorithm and the code related to RNG algorithm (seeding, background cycling, scaling, etc.)

NOTE: Sufficient information should be contained in the test report to verify that any live instance of the RNG accurately reflects the tested version. This would include the file names and hashes of source code and executables, all critical files as designated by the developer and tester must be listed. In addition to the core RNG any pertinent operating environment details must be listed such as the operating system, gaming platform and other environmental variables that if modified could impact on the test certificate results.

Details of who controlled and observed the build process and generated the digital signatures must be provided.

3.5 References

List of documents used for reference (compliance requirements, literature/URLs for software RNG, URLs for hardware RNG, supplier's documentation, etc.)

Ref 1

Ref 2

etc

3.6 Annex A – statistical testing results

Describe the statistical tests carried out and the results for the raw output of RNG and scaled/shuffled decks data for each type of games (degrees of freedom) being served by the RNG.

3.6.1 Testing results for raw output of RNG

An adequate selection of NIST and / or Diehard Tests shall be used when evaluating random sequences (raw output of RNG).

At least two random sequences (one tester generated and one vendor generated) shall be tested and these shall pass tests with a minimum confidence level of 95%.

For input data format and sample size, running these tests and interpreting the test results, refer to:

For NIST - http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf (Special Publication 800-22, Revision 1a)

For Diehard - http://www.stat.fsu.edu/pub/diehard/

Present test results here indicating success/failure of individual tests as well as overall assessment.

3.6.2 Testing results for scaled data or shuffled decks data

Chi Square/Frequency and Runs Up and Runs Down tests shall be applied to the scaled/shuffled decks data generated using the RNG being evaluated.

Degrees of Freedom (DOF) = Scaling range required for a game – 1

 # numbers drawn at once and whether this data is drawn with or without replacement.

At least two input data files each containing 3,000,000 scaled numbers or more shall be used for testing scaled data for every unique DOF being used by the gaming system.

At least two input data files each containing 3,000,000 shuffled cards (i.e. numbers between 0 and 51 or 1 and 52 assuming joker is not being used) or more shall be used for testing shuffled decks data

The data shall pass with a minimum confidence level of 95%.

Present test results here indicating success/failure of individual tests as well as overall assessment.