The Association of Racing Commissioners International
Totalisator Technical Standards

PARI-MUTUEL WAGERING
TOTALISATOR REQUIREMENTS AND OPERATING ENVIRONMENT

Sections – Index

Version 1.2a
Originally Adopted July 2011
Last Amended Dec. 2020

(a) A pari-mutuel wagering system can be relied upon only if it has an adequate system of internal controls. The Commission adopts these rules for totalisator companies and their operations on behalf of racing associations to increase the Commission's level of reliance on the totalisator facilities, equipment, and operations in the respective jurisdiction and to ensure all totalisator operations maintain the integrity of pari-mutuel wagering.

(b) Rules are descriptive, not prescriptive, and establish the concept of 'baselines' for software and equipment involved in critical operational activities and use the concept of 'defined interfaces' for operations/devices not directly connected to the central server of the totalisator vendor's wagering system.

(c) In adopting these Rules, the Commission is aware of the use of contemporary technology and telecommunications facilities in providing the totalisator wagering operation and that these facilities are not all necessarily present at the racing association's location and therefore, may be physically located outside the geographic jurisdiction of the Commission.

(d) A totalisator company retained under commercial agreement by an association is deemed for the purpose of these Rules to be the 'totalisator vendor' of the wagering system.

(e) An Independent Testing Laboratory (ITL) may be utilized for:

(1) verification of system;

(2) assessment of documented control procedures; and

(3) assessment of monitoring system (if any).

(f) Wagering Monitoring Systems (WMS) can be considered for real-time operational monitoring.

(g) Internal Control Systems (ICS) are defined to cover auditable operational procedures, i.e. operations and procedural manuals.

(h) Definitions**.** The following definitions are to be used in reading and following The Association of Racing Commissioners International Totalisator Technical Standards.

(1) Baseline envelope – the production operations environment that includes all software, hardware, and network components that are approved by the Commission.

(2) Baseline hardware – the minimum specification for hardware approved by the Commission for use in the production operations infrastructure.

(3) Baseline network – the network infrastructure and logical control software approved by the Commission and currently used in production operations.

(4) Baseline software – the version of software approved by the Commission and currently operating in production computers.

(5) Change Control Process – the Commission's process by which changes to a totalisator vendor's baseline is to be executed, evaluated, and approved.

(6) Direct Control Device – a device in a wagering network that is operated and controlled directly by the totalisator vendor for generating/displaying data, i.e. teller/cash terminals; self-serve kiosks; display devices; control/admin devices.

(7) Independent Testing Laboratory (ITL) – an entity recognized, or deemed acceptable, by the Commission to provide an independent evaluation of a totalisator vendor's baseline system and certify its compliance with these Rules.

(8) Intelligent Terminal – a direct control or peripheral device which contains code extending beyond that which is necessary to allow the device to communicate with the central controlling device to which it is directly attached or to control the presentation of data on the display unit of the device.

(9) Network security document – the document that describes in topographical format the network infrastructure, minimum engineering specifications, and security used for local and remote Device-to-Tote, Tote-to-Tote, and Data Center connection operations.

(10) Totalisator vendor – the company responsible for conducting wagering operations on behalf of an association; may be a system vendor/developer.

(11) Remote Device – a device under the control of a third party or individual not directly related to the totalisator vendor, but connecting into the totalisator vendor's operations, i.e., Internet devices, file transfer devices, wireless connection devices; "Odds" generating device not directly connected to the central server of the totalisator wagering system.

(12) System baseline document – the document that records and tabulates the elements of the baseline envelope, hardware, network, and software.

(13) Telecommunications Services – data communications facilities and carrier services provided via either wide or local area network facilities, including those operated by public carriers.

(14) Local Area Network (LAN) – a network (wireless or cable) that is finite in its reach and restricted to local wagering operations and typically deployed by, and under control of, a wagering totalisator vendor.

(15) Wide Area Network (WAN) – a network that traverses a public telecommunications carrier service - terrestrial, satellite, or wireless.

(16) Wagering Monitoring System (WMS) – a reporting process or software package that captures wagering operational activity in a format consistent with the Commission's audit, testing, and inspection requirements.

(17) Demilitarized Zone (DMZ) – a network configuration for securing an association's local area internal (totalisator) network. DMZ is a firewall configuration for securing local area networks (LANs) whereby a DMZ computer outside the firewall intercepts all incoming traffic and brokers a request for all computers on the LAN before being routed through the firewall, providing extra protection for computers behind the firewall.

(a) The following requirements relate to all wagering systems and shall be considered generic to the Commission's requirements for any totalisator vendor's computer system.

(b) System Requirements. The Commission requires that the totalisator vendor implement a computerized wagering system capable of meeting the following broad functions:

(1) efficiently perform all tasks associated with providing the specific wagering operation;

(2) ability to support the technical and operational requirements of these Rules;

(3) ability to support the Rules in force at the time for each offered product;

(4) ability to support the predicted system load requirements;

(5) ability to provide adequate system audit and security requirements;

(6) ability to provide adequate financial verification and audit capabilities; and

(7) ability to provide monitoring and reports as required by the Commission.

(c) A wagering system is deemed to extend from the central system to the point at which:

(1) a customer's transaction is presented; or

(2) system generated information is delivered to/from the central system interface, in an approved format.

(d) General Requirements.

(1) The wagering system shall be able to:

(A) sell, calculate, and cash according to the pool profile, current Rules, and number of races;

(B) produce the required reports and logs described in Section 3, Sec. 3.1 through Sec. 3.7 Reporting, Monitoring & Data Retention;

(C) accept advanced wagers;

(D) network with the remote wagering sites;

(E) offer simultaneous wagering cards;

(F) allow access to operational functions and identification of each user of those functions based on the totalisator vendor's access security policy;

(G) automatically maintain all carry-over data required for the next performance on a rotating basis, including system date and time, without operator/user intervention;

(H) be subject to modification only by authorized individuals who have secure access to the operating system;

(I) be subject to a change control process consistent with Sec. 1.5 Change Control Process of these Rules;

(J) detect abnormal system operation and the cause, such as a validation problem, communication difficulty, and computer downtime, and immediately notify the operator/user;

(K) generate data usable across two major revisions, and within all minor revisions or retrieve archived data reports requested by the Commission within twenty-four hours;

(L) include a utility program that backs up the wagering system and schedules these backups at regular intervals; and

(M) operate on a standard time (e.g. atomic clock) .

(2) The operating system must be:

(A) separated from the application software;

(B) based on identified individual users; and

(C) able to maintain auditable records of those users.

(e) Hardware Requirements

(1) A totalisator vendor must define a central system configuration that will meet the minimum specification required to ensure the wagering system:

(A) will support approved system functionality;

(B) is secure from unauthorized access;

(C) can scale to meet peak load expectations;

(D) demonstrates resilience to unplanned interruptions without loss of data and integrity; and

(E) delivers minimal risk for single point of failure scenarios.

(2) This configuration will be deemed the baseline configuration for pari-mutuel wagering system operations.

(3) A wagering system shall be consistent with multi-processor architecture with inherent degrees of:

(A) independence in the transaction processing and system control functions; and

(B) redundancy and resilience in the event of processor failure.

(f) Software Requirements

(1) Cash/Sell System.

(A) A totalisator vendor shall provide a cash/sell totalisator wagering system.

(B) The system must comply with these Rules regardless of the location of the central server for the wagering system.

(2) The Commission will approve the software configuration (baseline) of the wagering system host.

(3) All software for all components of the totalisator vendor's wagering system must be maintained under an appropriate software version control system. See Sec.1.5 Change Control Process of these Rules.

(4) The totalisator vendor shall have in place procedures for virus protection and detection, where a material risk of virus infection exists.

(5) The operational control of the wagering system must be administered in accordance with the relevant internal control system. See Sec. 2.2 Internal Control System of these Rules.

(6) Only approved application files may reside on storage media or be loaded into the memory of the wagering system host computers.

(g) Security Requirements

(1) The central system shall be located in a data center that is a secure area where only authorized personnel may enter. This facility shall have an electronic locking system that provides monitoring information relating to the entry/exit of personnel.

(2) Procedures shall be maintained to ensure that only authorized personnel are given access and there shall be a detection system that provides a log entry as well as an alert when unauthorized entry is attempted.

(3) The data center shall have an environmental monitoring system with stand-by power facilities including an uninterrupted power supply.

(4) At a central server site, all network devices, network control devices, and hosts associated with a production network must be located inside an area that only persons with a valid authorization clearance can enter.

(5) All network access to the data center shall be the subject of appropriate firewall and other logical network access security features.

(6) The Commission requires adequate security over the approved wagering system to ensure continued system integrity and audit ability.

(7) The operating system of the computer's wagering application files and database, if applicable, must provide comprehensive access security. The Commission requires that the totalisator vendor's published access security policy be complied with, including password security policies.

(8) The Commission requires that storage of passwords/PINs be in compliance with the totalisator vendor's security policy, e.g. in an encrypted, non-reversible form. This implies that, if a person, authorized or not, reads the file that stores the password/PIN data, he/she must not be able to reconstruct the password/PIN from that data even if the creation algorithm is known.

(9) The Commission requires that the totalisator vendor have formal internal reporting and that follow-up procedures exist for security breaches. For example:

(A) unauthorized attempts to access a system (sign-on);

(B) unauthorized attempts to access system resources; and

(C) unauthorized attempts to view or change system security definitions or rules.

(10) The Commission requires that there be adequate security policies and configuration management procedures in place relating to any media library administration and any off-site storage of data. It is required that all software and critical data are only to be accessed by authorized personnel.

(11) A facility/report must be available that will list all registered users on the system including their privilege level and this list must be kept current.

(h) Physical Requirements.

(1) Power to devices inside and on the boundary of the baseline envelope shall be provided from a filtered, dedicated power circuit.

(2) Cabling used in production networks shall be protected against unauthorized physical access and malicious damage.

(i) Network Requirements

(1) The Commission requires that a totalisator vendor have a documented policy on network topography, minimum engineering specification, and security – the '*Network Security Document*'.

(2) The Network Security Document:

(A) will be evaluated, assessed, and approved by the Commission;

(B) is essentially a matrix that describes the network topology of the system, details the interconnection of modules within the network, and the type of connection between the modules that is permitted;

(C) will describe the totalisator vendor's network policies for system firewalls, network connections that are inside a baseline envelope (the core area defined by the Commission as to being under baseline control), and network connections from the baseline envelope to external devices/systems;

(D) will describe the network control devices located at the boundary or inside the baseline envelope;

(E) will describe how all cabling and devices are to be clearly labeled by function;

(F) must be kept in a form that can be viewed in the event of total network destruction. Documentation must include patch records, device configuration, device location, cable location, and fault procedures. See Sec.2.7 System Resilience & Integrity of these Rules.

(j) Computer Monitoring and Network Management Systems

(1) The Commission requires that the totalisator vendor will have in place adequate monitoring tools and management functions to alert the operator/user and the Commission (if a real-time wagering monitoring system is operational) were any abnormal activity to occur.

(2) The monitoring and management systems may include:

(A help desk/technical/operational support facility;

(B) computer hardware and systems software monitoring systems that monitor hosts inside or on the boundary of a wagering system baseline envelope;

(C) network monitoring systems that monitor network devices and network control devices inside or on the boundary of a wagering system baseline envelope; or

(D) totalisator operations real-time monitoring system to allow the operator/user and/or the Commission to monitor, evaluate and report on betting, pools and revenue data held in the wagering system.

(3) These monitoring systems must be demonstrated to and evaluated as to their integrity by the Commission.

(k) Verification tools. Upon request, the Commission must be provided a means by which to verify the configuration of all devices inside and on the boundary of the wagering system baseline envelope.

(l) Totalisator Rooms.

(1) Association Facilities. An association shall provide a totalisator room to house the main computing and communications equipment or the operator/user's terminal at the association's facility, whichever is applicable. The room must include:

(A) air conditioning with humidity control to maintain a stable environment that meets the specifications of the computer equipment manufacturer;

(B) a master power switch that allows all or part of the equipment housed in the room to be turned off in an emergency;

(C) a smoke/fire alarm system that sounds locally and is tied into the association's master alarm system;

(D) fire extinguishers to deal with minor electrical fires; and

(E) an internal communication system connecting the totalisator operator/user with:

(i) the stewards or racing judges;
(ii) the mutuel manager;
(iii) each betting line;
(iv) the pari-mutuel auditor's office, if applicable; and
(v) a private outside line for communication with supervisors, programmers, or totalisator personnel at other sites.

(2) Totalisator Room Security. The totalisator room housing the CPU or operator/user's terminal that processes wagers made at an association's facility must be secured at all times. The association shall submit to the authorizing jurisdiction for approval a security plan, and any changes to the security plan, for the totalisator room housing the CPU or operator/user's terminal that processes wagers made at the association's facility. The security plan must include:

(A) a security system covering the totalisator room and any other related service, electrical, or equipment room that consists of locking closed doors and detecting unauthorized entry; and

(B) a system of controlled entry to the totalisator room and other related rooms, using:

(i) locking devices on all doors or entry points;
(ii) controlling the distribution of keys or codes necessary to unlock the doors; and
(iii) a sign-in log for visitors to include signature of person authorizing access.

(3) Tote Room Access. If the totalisator room housing the CPU or operator/user's terminal processing wagers made at the association's facility is located on property owned or controlled by the association, the association shall limit entry into the totalisator room to totalisator, association, and Commission personnel approved by the authorizing jurisdiction.

(A) The association shall submit a list of the individuals to be approved for totalisator room access at least two weeks before the first day of each live race meeting and each time a personnel change necessitates a change to the list.

(B) Personnel entering the tote room that are not on the authorized list must sign in on a visitor log maintained in the tote room.

(4) Central Processing Location. An association may contract with a totalisator vendor that uses a central processing location off the association's grounds. The central processing location shall ensure that:

(A) its on-site totalisator room meets the facility, security and access requirements in paragraph (l) Totalisator Rooms section above;

(B) the totalisator vendor’s central processing location satisfies the requirements of these Rules; and

(C) the totalisator vendor’s central processing location has a communications system connecting the central processing location with:

(i) the totalisator vendor’s representatives at the association's facility; and
(ii) a private outside line for the communication with supervisors and operations support personnel at other sites.

(a) System Baseline

(1) A wagering system baseline envelope is defined in co-operation with the totalisator vendor and the Commission and will include hardware, software, and network components that interoperate to deliver the critical operational functions of the wagering system entitled the *System Baseline Document*.

(2) The system baseline envelope is to consist of system software, hardware components, and network components that enable the system to operate in a secure environment and be consistent with these Rules.

(3) For the purposes of these Rules, all software and equipment, including central servers, communications devices, peripherals, and direct control devices, which are being utilized in a licensed operation for a racing association at the effective date of these Rules, will be considered to be:

(A) included in the initial System Baseline; and,

(B) approved for operation by the Commission.

(4) The following shall be included in the *System Baseline Document*:

(A) all system components which represent the core components of the wagering system ;

(B) application files such as those associated with transactions, account access, event control, and revenue reporting;

(C) operating systems which provide a secure environment;

(D) interface modules with databases used by the system application;

(E) interface software that interacts with any remote outlet or third party services;

(F) central systems communication devices that interface with any remote operation or third party equipment;

(G) the facility/method used to verify that the system is operating in an approved state;

(H) a system network document – the *Network Security Document* - that clearly identifies the core areas of the wagering system network. This document shall describe the network topology of the system, detailing the interconnection of modules within the network, and the type of connection between the modules that is permitted; and

(I) any other operations or procedures that are relevant to securing control of the system, i.e. the Internal Control System Document (see Sec.2.2 Internal Control Systems).

(5) Any changes to those components, including the emergency changes, are subject to approval by the Commission with regard to the Change Control Process (See Sec.1.5);

(6) Any WAN and Internet communication links will be generally deemed to be outside the wagering system baseline envelope approved by the Commission.

(7) An ITL recommendation may be required for all changes to the System Baseline Document; See Sec.1.6 Certification & Submission of these Rules.

(b) Software Baseline

(1) The Commission shall approve the software configuration (baseline) of the central system host.

(2) Any changes to the baseline software for the wagering system must be submitted to the Commission and be subject to the Commission's Change Control Process in Sec.1.5 Change Control Process of these Rules.

(c) Hardware Baseline

(1) The Commission shall approve the hardware configuration which will be deemed the baseline configuration for wagering system operations.

(2) Any changes to the baseline hardware configuration must be submitted to the Commission and be consistent with the Change Control Process outlined at Sec 1.5 Change Control Process of these Rules.

(d) Network Baseline. During the approval stage of a system network, the Commission will confirm the core areas of the system network over which verification control must be maintained and this will be defined and approved in the *Network Security Document*. See 1.2 General System Requirements (Network Requirements).

(e) Inspection tools

(1) All security logs must be reviewed and relevant entries that put the integrity of the operation or outcome of an event at risk should be followed- up by the operator/user in a timely manner.

(2) All accounting and any security event data must be held and be able to be accessed or retrieved (from back-up) for:

(A) Significant events - at least two [2] years

(B) Financial data - at least seven [7] years.

(3) There must be a procedure provided by the totalisator vendor whereby significant events will be reported to the Commission in a format to be determined by the Commission.

(4) Typical significant events to be reported on are as follows:

(A) situations where the system is incapable of supporting the Rules;

(B) significant software, hardware or network system failures;

(C) instances where there has been unauthorized access to the system;

(D) instances where internal control system procedures were unable to be followed;

(E) situations where system hardware or software version roll-backs were carried out;

(F) instances where significant work-arounds were carried out by the operator/user;

(G) instances where a system verification test result came out incorrect;

(H) instances where late event/draw closures were identified;

(I) instances where incorrect payout calculations were identified; and

(J) any other events as required by the Commission.

(f) System Baseline Auditing Requirements

(1) The totalisator vendor, with assistance from an ITL when applicable, must document all system components and identify those that are core to the system operations (*the system baseline*) to be submitted as part of the request for system approval.

(2) The approved wagering system will be subject to a condition that the totalisator vendor must not undertake any changes to the system baseline without approval by the Commission as outlined in Section 1.5 Change Control Process.

(3) The totalisator vendor must ensure there is a method in place to verify the software on which the evaluation was performed is the same as the software submitted for approval and live operation. To this end the following goals are to be met:

(A) the testing entity must be able to verify and confirm that all the system software being submitted for approval is the same as that which was evaluated. Only the system baseline files are required to be included with the submission approval;

(B) a procedure is available which outlines the method for verifying that the executable software on the production system is operating in an approved state. Where redundant production systems are used, the redundant systems shall operate the same version of software with the same configurations; and

(C) a procedure is available which outlines the method for detecting unapproved programs, command files, fixed data files, etc. that reside on any modules in the wagering system.

(4) There is a requirement for an agreement to be reached between the totalisator vendor, the testing entity, and Commission, relating to the directories in which application files will be located on the central system computers in order to establish a baseline document. Files that cannot be verified because they change frequently are not expected to include functionality that would be in the baseline, nor be stored in system application directories.

(5) There shall be adequate procedures in place to ensure that portions of the system outside the wagering system baseline envelope, as approved by the Commission, are checked regularly to ensure that unauthorized activities are not taking place on the overall wagering system.

(6) It is expected that the totalisator vendor will implement and maintain the following matters in regards to system audit:

(A) ensure that adequate system security procedures and policies are in place and that critical issues are actioned upon by management in a timely and accurate manner;

(B) all significant audit logs must be monitored and non-conformance with policy acted upon, with a record kept of the noncompliance and any resulting action;

(C) there shall be satisfactory security and control over database applications and critical configurable parameters to ensure the integrity of the system;

(D) there is to be a method to verify the integrity of the software on the host and any associated peripheral equipment operating in the production environment;

(E) all applicable user accesses shall be restricted via menu options;

(F) all remote or dial-in access shall be strictly monitored and any relevant security related logs are to be followed-up in a timely manner;

(G) network and communications security procedures are to be established, enforced and maintained;

(H) all interfaces to any subsystems are to be managed securely, and security reviews are to be performed at intervals defined by totalisator vendor policy;

(I) preventive and detective control measures shall be established with respect to the security of the production central system environment;

(J) the totalisator vendor shall ensure that adequate internal software change control procedures exist in line with its change management processes; and

(K) the Commission requires that adequate emergency change control procedures are in place.

(a) The purpose of this Section is to describe the technical and operational requirements for peripheral devices and systems which may be connected to the central wagering system in either a local or remote manner and under the direct control of the totalisator vendor or under the control of individuals or other operator/users.

(b) General Requirements

(1) Wagering devices that are managed by the totalisator vendor shall be secure in both physical and software perspectives.

(2) Internal access to totalisator vendor managed device hardware shall be gained through secure measures.

(3) Connecting ports, switches, and other interfaces shall be tamper resistant to ensure the security of the totalisator vendor managed device.

(4) Functionally, a wagering device, regardless of whether it is a totalisator vendor managed or personal device, shall:

(A) be restricted to providing a user interface with the patron(s); and

(B) not include intelligence to validate or secure a transaction.

(5) Control measures shall be in place for device software updates and documentation. See Sec.1.5 Change Control Process of these Rules.

(6) Methods and procedures shall be included in an internal control system to describe how device settings and configurations can only be amended through a secure process. See Sec.2.2 Internal Control System of these Rules.

(7) Functionality and recoverability of a device during operational conditions such as loss of power or system connectivity shall be assessed, e.g. the device shall demonstrate the capability to resume operation and complete any transaction in progress at the time of a power failure to the device. See Sec.2.7 System Resilience & Integrity of these Rules.

(c) Scope of Peripheral Devices & Telecommunications Services, for example, but not limited to:

(1) Direct Control Devices (under full control of the totalisator vendor):

(A) Teller/cash terminals;

(B) Self-service kiosks;

(C) Display devices (Tote Boards, Display Boards, Video displays);

(D) Control/admin devices; and

(E) Call center terminals.

(2) Remote Devices (not under control of totalisator vendor):

(A) Internet connected devices;

(B) File transfer devices (PCs);

(C) Wireless connection devices/Personal devices; and

(D) Systems used to calculate "Odds" that are not otherwise directly connected to the central server of the totalisator vendor's wagering system.

(3) Telecommunications Services

(A) Technology

(i) leased data line (wide area network-WAN); and

(ii) local area networks (data cable or wireless).

(B) Operation

(i) between terminal and hub;

(ii) between hubs;

(iii) between hub and central server;

(iv) between central server and hub;

(v) between central servers, e.g. ITSP; and

(vi) between central server and display boards/devices.

(d) Security for Peripheral Devices

(1) Software Security

(A) The Commission requires adequate security over the approved software to ensure continued system integrity and audit ability, including, but not limited to:

(i) The programming of intelligent direct control devices must be limited to communication with the main computer, maintenance routines, and dynamic device configuration routines.

(ii) A direct control device, whether intelligent in its configuration, or "smart" or "dumb" in its functionality, shall include programming consistent with the technical requirements for the main computer communication, maintenance routines, and dynamic device configuration routines.

(iii) Software related to the production or verification of the wager identification number, e.g. ticket number, printed on a pari-mutuel ticket or assigned by the main computer shall not reside in any peripheral device.

(iv) A direct control device may not access, alter, change, or manipulate the wagering database except to conduct the wagering or cashing functions necessary to serve the public.

(B) The Commission requires that formal internal reporting and follow-up procedures exist within the totalisator operation for security breaches to these Rules.

(2) Hardware Security

(A) The Commission requires that, at a minimum, adequate security is incorporated into the design/build of the device/peripheral hardware to ensure overall system integrity is maintained.

(B) This scope of such security would typically include:

(i) microprocessor boards;

(ii) USB/serial or other communication ports for peripheral devices;

(iii) power supplies and power on/off switches;

(iv) communications hubs;

(v) hardware storage racks; and

(vi) device intrusion sensors.

(3) Access Control Security

(A) The Commission requires that, in the design/build of peripheral devices, adequate access controls are integrated into each type of device to ensure that the integrity of the overall system is maintained.

(B) The scope of these access controls shall cover:

(i) access to money stackers/bill acceptors;

(ii) access to operating systems (e.g. Windows);

(iii) access through USB/serial or other communication ports; and
(iv) malicious intent prevention.

(C) Access to critical software files or software configuration options on the peripheral device without authorized access codes/keys must be restricted.

(e) Functionality

(1) The Commission requires that direct control devices:

(A) operate with read/print/display accuracy and integrity, for example:

(i) bill acceptors shall be capable of properly accepting and crediting applicable currency;

(ii) ticket printers shall print valid mutuel tickets. Each valid mutuel ticket must have printed on its face:

I. the name of the racetrack facility where the wager was placed;
II. the name of the racetrack where the race was conducted;
III. the number of the race;
IV. the unique computer-generated ticket number;
V. the date the ticket was issued;
VI. the date of the race for which the ticket was issued;
VII. the number of the ticket-issuing machine;
VIII. the type of pool;
IX. the number of each entry on which the wager was placed;
X. the dollar amount of the wager; and
XI. the expiration date of the ticket.

(iii) ticket printers shall print valid vouchers. Each valid mutuel voucher must have printed on its face:

I. the name of the racetrack facility where the voucher was issued.
II. the unique computer-generated voucher number;
III. the date the voucher was issued;
IV. the number of the ticket-issuing machine;
V. the dollar amount of the voucher; and
VI. the expiration date of the voucher.

(iv) ticket readers shall be able to read, validate, and properly credit vouchers and tickets;

(v) devices shall be evaluated as to their methods for validating tickets, including capture of valid tickets by the device and branding marks;

(vi) not allow nil, partial, or duplicate print of a ticket; and

(vii) access correct functions as labeled on a keypad;

(B) will detect and inform as to:

(i) paper jams/paper out; and

(ii) other consumable exhaustion/defect situations;

(C) can be uniquely identified under software/firmware control in the wagering system network;

(D) utilize a secure software download process (if any);

(E) display with reliability any information disseminated by the wagering system;

(F) allow an authorized official to post the order of finish, the official sign, inquiry sign, objection sign, or dead heat sign;

(G) are located in or near the authorized officials in a location approved by the executive secretary in order to issue the stop wagering command during normal operations and activate the "off bell";

(H) any "back up" device shall be installed in the totalisator room to allow the tote system operator/user to issue the stop wagering command if a system malfunction or human error prevents the wagering system from activating the stop wagering function at the appropriate time; and

(I) have resilience to, and maintain integrity throughout, external service faults, for example:

(i) loss of telecommunications;

(ii) loss of power;

(iii) generation of error messages;

(iv) devices shall be evaluated for handling of failed ticket printing and accounting for credits or bets made on tickets;

(v) printers shall be able to properly handle paper outages and paper jams; and

(vi) devices shall have the ability to recover from a loss of power or network disconnection while idle, while a transaction is in progress, and/or when money is owed to the patron or teller.

(2) The Commission requires that remote devices:

(A) comply with the totalisator vendor's published and approved wagering system interface;

(B) cannot access critical software files on the wagering system; and

(C) cannot initiate malicious intent activity beyond the baseline interface (firewall).

(3) The Commission requires that every transaction generated by or displayed upon a peripheral device includes a unique transaction serial number derived by the wagering system.

(f) Regulatory Compliance

(1) The Commission requires that all peripherals and direct control devices included in the wagering operations, whether at the associations' premises or at a central server location or other approved site:

(A) are defined in the system baseline as being 'smart' or 'dumb' devices.

(i) A device is defined as 'smart' if it has software functionality that decides/influences outcomes of the wager; such software, if in existence, must be adequately secured within the relevant device's hardware configuration, e.g. a secured, tamper proof cabinet/cage.

(ii) A device is defined as 'dumb' if its functionality is restricted to:

(I) interpreting data input activity to develop a data packet that is consistent with a specified interface to be received and processed as a transaction, administrative or wagering, by the central server; and

(II) receiving a transmission data packet from the central server and using that data packet to print/display a wagering transaction; display a wagering pool and odds; display other wagering operational information.

(B) include verifiable software versions:

(i) with critical system files locked in software; and

(ii) under version control;

(C) include verifiable identification in the network:

(i) with a unique serial number;

(ii) accurate in system registration;

(iii) able to be tracked in accounting of terminal transactions; and

(iv) with controlled configuration changes;

(D) be approved by the Commission for any amendments to configuration of devices in the network or to the device itself in advance by the totalisator vendor; See Sec. 1.5 Change Control Process.

(2) The Commission requires that the following direct control devices to be physically and functionally evident in the operation and will have been assessed and approved for deployment:

(A) Control Workstations/Printers

(i) a *log printer* for each computer if the system is unable to reproduce the logs upon request;

(ii) a *master control terminal* that allows the tote system operator/user to execute routine maintenance and operational functions based on individual operator/user identification/authentication;

(iii) *user terminals* that allow restricted system access to the mutuel manager, money room personnel, and the stewards or racing judges;

(iv) wagering information screen *displays;*

(v) *data storage devices* to record necessary system data; and

(vi) *backup devices* capable of recording complete system information on removable media for storage and restoration.

(B) Stop Wagering Devices. The totalisator vendor shall install two separate devices that activate the stop wagering function of the totalisator system. The stop wagering devices shall be the judge's console and a tote system backup located at the racing association. Said tote system backup may be operated by local racing association personnel and/or racing stewards, and also remotely operated by tote personnel not physically located at the racing association. If the tote system backup is operated remotely, a protocol for the remote operation shall be submitted to the racing commission for approval.

(C) Multi-purpose Displays (Tote Board). The multi-purpose displays, including the tote board, must update the odds on each betting interest in the relevant betting pools at intervals of not more than sixty [60] seconds.

(D) Cash/sell terminal/kiosk. A local area cash/sell teller terminal or a self-service kiosk is not required to be intelligent, but must have an individual identity within the network.

(E) Ticketless Electronic Wagering (E-wagering). A totalisator vendor may not use E-wagering devices unless approved by the Commission as required by Subchapter E of this Chapter.

(a) The purpose of this Section is to describe a risk based change control process the Commission requires to be used for scheduled critical, essential and desirable changes, as well as emergency changes, to the system baseline.

(b) The Commission requires that totalisator vendors utilize the Commission's change control process related to the wagering products and systems to ensure compliance of the totalisator vendor's wagering system with these Rules.

(c) The Commission requires a totalisator vendor to comply with these processes:

(1) regardless of the source of the system software used by the totalisator vendor for its pari-mutuel wagering system; and,

(2) in conjunction with the totalisator vendor's internal change management process.

(d) The Commission has determined a risk-based change control process is consistent with the Commission's requirements and may include the involvement of an independent testing laboratory (ITL) or other testing entity approved by the Commission.

(e) The objective of the risk-based change control process is to:

(1) put in place an agreed process and mechanism to gain approval from the Commission for changes to wagering software and equipment that is under change control;

(2) define the responsibilities of totalisator vendors in the change control process, to deliver appropriate documentation to enable assessment of the risks and impacts of the changes, to test the changes in an approved manner, and to submit test results to the Commission;

(3) define the responsibilities of an ITL in the change control process to assess the risks and impacts of the changes, to evaluate and test the changes, to update the baseline documentation, and to submit a certification report to the Commission for approval;

(4) assess changes to wagering software and equipment under change control based on agreed criteria to determine impact and potential risk to the operation and integrity of totalisator vendor's systems; and

(5) be complementary to the totalisator vendor's business product development process and not be evident as a roadblock to innovation and enhancement of wagering operations.

(f) The change control process is based on a risk classification system of red, amber, and green. Each systems' components under change control will be classified by a consultative group made up of the Commission, totalisator vendor, and testing entity representatives, and documented in a wagering software and equipment spreadsheet maintained by the totalisator system provider.

(1) System components shall be put into the respective classifications based on the component's impact on the fairness, audit ability, and security of wagering, wagering rules, cancellation rules, and financial reporting. See Diagram A: Baselines and Interfaces Classification Guide.

(A) Red – Major potential impact on the above classifying criteria;

(B) Amber – Significant but not major potential impact on the above classifying criteria; and

(C) Green – Minor potential impact on the above classification criteria.

(2) Based on the classification of the component, testing and deployment of the change shall be done as follows:

(A) Red changes shall be independently tested starting immediately after the totalisator vendor has submitted the change request. The change shall not be deployed until after the testing is complete and the Commission approves the change.

(B) Amber changes shall be independently tested as designated by the Commission. The change may be deployed either before or after testing.

(C) Green changes shall be randomly tested at the direction of the Commission. The change is deployed prior to testing. Amber/Green testing will be designated by the Commission.

(g) The outline of the change control process is:

(1) The Commission will obtain a list of the totalisator vendor's systems and applications that will be classified as wagering software and equipment and may, therefore, require change approval from the Commission.

(2) Changes to wagering software and equipment under change control are to comply with this change control process, which is based on the technical risk classification of the change which is to occur.

(3) Amber and Red changes to wagering software and equipment deemed to be under change control will need pre-approval from the Commission before implementation.

(4) Under the change control process, the testing entity recommends changes for approval to the Commission depending on the risk classification of the change.

(5) A change to a system component under change control will assume the same classification as assigned to the system component itself.

(6) A different classification for some changes will be considered by the Commission in consultation with the testing entity, provided the totalisator vendor submits a satisfactory justification for the variation from the default risk classification.

(7) Associations and totalisator vendors shall present new products/major updates for any change that is seen as potentially contentious to the Commission for an approval in principle before any project is initiated.

(10) This pre-compliance assessment is to ensure projects are deemed "compliant in principle" by the time work commences on the project.

(11) The testing entity will raise any direct non-compliance with the Commission and the relevant totalisator vendor as early as possible while reviewing the documentation and change requests.

(12) Having visibility of this compliance depends on the nature of the change and the level of information provided.

(13) Shall the non-compliance not be obvious, the testing entity may only be able to accurately assess this during the later stages of the change control process and this will immediately be flagged with both the Commission and the relevant totalisator vendor.

(h) Emergency Changes

(1) Any wagering system update that meets the Commission's definition of an emergency release may be released into production in accordance with the Commission's emergency release process.

(2) An emergency release may be initiated without Commission review.

(3) The Commission's definition of an emergency release is when a totalisator vendor's system would be at serious risk, left vulnerable to attack, or where an urgent and important repair is required for an unexpected failure.

(4) The Commission's emergency release process is:

(A) Totalisator vendor identifies that an emergency system change is required.

(B) At all times, prior to implementing the change, totalisator vendors will send an e-mail to the Commission to advise that the change is to be deployed.

(C) An ITL may also be copied on this email.

(D) Totalisator vendors shall also phone an authorized officer of the Commission to inform them about the emergency release, if available.

(E) The change can be deployed to production once this notification email and follow-up phone call has been sent.

(5) Totalisator vendors will list all affected applications immediately following the deployment of the emergency release and will submit the list to the Commission at the same time as the relevant change request.

(6) Totalisator vendors will submit a change request including risk classification to the Commission within 24 hours, or, the next working day.

(7) Totalisator vendors will advise the Commission within three working days if the system change was successfully implemented and the problem resolved.

(8) The emergency change is then integrated into the agreed change control process, and the risk classification is verified by the testing entity.

(i) Wagering Baseline Spreadsheet

(1) A testing entity will assist in the definition of a wagering system baseline. See Sec. 1.3 System Baseline of these Rules.

(2) The testing entity's recommendation is required for all changes to the system baseline document; any changes, including the emergency changes, are subject to approval by the Commission.

(3) The spreadsheet will list the totalisator vendor's current wagering software and equipment lists, with all components identified and details of the status of each component as wagering software and equipment or not.

(4) Any item categorized as wagering software and equipment is further characterized as falling under change control or not.

(5) Wagering software and equipment under change control is subject to the change control process outlined in this Section.

(6) Testing entities are responsible for notifying the Commission in regard to:

(A) any new components that are added to the wagering software and equipment spreadsheet; and

(B) any modifications that are made to the wagering software and equipment spreadsheet, such as:

(i) re-categorization of wagering software and equipment;

(ii) adding or removing components from change control; and/or;

(iii) classifying items under change control as red, amber or green.

(7) A change to a system component under change control will assume the same classification as assigned to the system component itself in the wagering software and equipment spreadsheet.

(8) A different classification for some changes can be considered by a testing entity and the Commission provided totalisator vendors submit a satisfactory justification for the variation from the default risk classification.

(9) The testing entity will notify the Commission and totalisator vendors about any additions or modifications to the wagering software and equipment spreadsheet as soon as they become apparent during the change control process for each release.

(10) A final version of the revised wagering software and equipment spreadsheet will be submitted by the testing entity to the Commission for approval along with the testing entity's certification report.

(11) Although a totalisator vendor is responsible for maintaining its wagering software and equipment spreadsheet, the Commission has the final say in the classification of any system component under change control.

(j) Methodology

(1) Traffic light system ("red"; "amber"; "green").

(2) "Red", "amber", and "green" system components (software & equipment) are agreed at initial point (baseline).

(3) If a system change involves a "red" component, then the system must be evaluated by the testing entity before being put into production.

(4) If a system change involves an "amber" component, then the system update can go into production but must be evaluated by the testing entity within six months.

(5) If a system change involves a "green" component, then the system update can go into production without a recommendation from the testing entity or Commission approval.

(6) The Commission can do random audits of "green" and "amber" changes for consistency with process definitions/parameters.

(7) Emergency fixes are allowed on the spot subject to a formal notification being sent to the Commission at the time and then the emergency fix, as categorized under traffic light system, is picked up in the next round of testing.

(8) The Commission acknowledges that this methodology should not be used as a roadblock to the totalisator vendor's business product development or day-to-day operations.

(k) Data Changes:

(1) A data update in any wagering system database or data file related to baseline systems that is required may be applied in accordance with the following release process:

(A) at all times, totalisator vendors will notify the Commission about the data change by e-mail prior to implementation of the change; and

(B) the data change can be made once this notification e-mail has been sent.

(2) Review of the data change is not required by a testing entity.

(3) Identified issues that subsequently require a software change to a component under change control must have that change submitted for assessment by the Commission in accordance with the change control process.

(4) For each data change, totalisator vendors will provide a detailed analysis report describing the reason for modification, an analysis of the modification, and the proposed resolution.

(5) This report will be emailed to the Commission and a copy may be sent to the testing entity.

(l) Random Sampling

(1) The Commission requires a testing entity to independently test randomly selected green changes to confirm that the changes are compliant, the risk classification is accurate, and to validate correct operation.

(2) This random sampling ensures that the testing entity and the Commission are both comfortable with the risk classification that a totalisator vendor is establishing for green changes.

(3) This random sampling of green changes should occur every six months.

(4) The Commission will select the green changes that will be independently sampled.

(5) The number of changes to be sampled is not a definitive number and it may be that the number of changes put through by totalisator vendors warrants a greater (or lesser) number of changes being selected for sampling.

(6) The selection also depends on the number of changes that are classified as green.

(7) As part of the sampling process, the testing entity will review the change to confirm that the change is correctly classified as green.

(8) The testing entity will also conduct independent testing of the changes selected by the Commission for sampling.

(9) If any sampled green changes are found to be non-compliant, the risk classification is inaccurate, and/or the testing entity has been unable to validate the correct operation of the change, the testing entity must inform the Commission that the changes have failed independent testing within two working days after identifying the issue.

(10) The testing entity will copy the relevant totalisator vendor on the report about the non-compliant changes.

(11) The Commission will determine the course of action following the report of a non-compliant change.

(m) System Changes

(1) Red Process

(A) Totalisator vendor submits a change request to the testing entity.

(i) This change request will:

(I) provide details about each proposed change that will be made to wagering software and equipment under change control to support the functionality defined within the requirements specifications;

(II) include details about additional and/or modified software that will be introduced to the baseline systems since the last approved version;

(III) include details about baseline files that have been removed since the last approved version; and

(IV) include totalisator vendor's risk classification and a justification of the risk classification for each change.

(ii) Submission of change requests to the testing entity will be performed on an as-needed basis within a timeframe agreed to by both parties.

(iii) The Commission will be copied on all change requests submitted to the testing entity.

(B) Totalisator vendor will provide any further information and documentation that the testing entity requires to make a comprehensive assessment of the change request.

(i) The testing entity:

(I) will review the change request and confirm that the change request encompasses the scope of the project for wagering software and equipment under change control;

(II) will assess the risk classifications submitted for each change for technical accuracy;

(III) will raise with the totalisator vendor any items requiring re-classification and seek agreement on the change;

(IV) will submit to the Commission for a ruling any risk classifications that cannot be agreed upon; and

(V) will review the change request for adherence to the Commission's compliance requirements.

(ii) Any items that are considered to be non-compliant are raised for discussion between the testing entity and totalisator vendor.

(iii) Any items that cannot be agreed upon are submitted to the Commission for a ruling.

(iv) The Commission will be copied on all correspondence between totalisator vendor and the testing entity.

(v) The certification report that the testing entity submits to the Commission for approval will reference the final version of the request that is submitted.

(C) Totalisator vendor will submit a copy of the test plan to the testing entity for the whole project.

(i) The test plan is to include:

(I) formal identification of requirements and applications affected by the changes;

(II) a list of testing areas that are/are not in scope for the project;

(III) pass/fail criteria;

(IV) exit criteria;

(V) the definition of suspension and resumption criteria;

(VI) testing resources including roles and responsibilities and environmental requirements;

(VII) testing risks;

(VIII) the testing schedule;

(IX) faults and issue reporting process;

(X) the process for scope changes that need to be made after the start of the testing cycle; and

(XI) a list of test cases that will be executed for the project.

(ii) The testing entity will review the test plan for changes classified as red to ensure that it sufficiently addresses the scope of the changes.

(iii) Any areas identified as insufficient or missing based on rules compliance criteria will be raised with totalisator vendor for consideration.

(iv) The testing entity will send the final version of the test plan to the Commission.

(D) Totalisator vendor will submit the testing exit report to the testing entity.

(i) The testing exit report is to include:

(I) all final test results for each of the test scripts executed for red changes;

(II) a list of testing areas that were not tested as identified in the 'out of scope' section of the test plan;

(III) a list of defects that were raised and resolved as part of the project (for the purpose of ensuring no oversight of critical defects);

(IV) a list of defects that were raised and not resolved as part of the project, e.g. acceptable failures and expected behavior; and

(V) where a defect is marked as an acceptable failure and a manual procedure or workaround exists, details about the procedure or workaround are detailed in the testing exit report.

(ii) The testing entity:

(I) audits the test results to ensure all relevant test cases are executed and have a satisfactory outcome;

(II) assesses any manual workarounds for completeness and correct operation to confirm that the solution addresses the issue and to ensure that the workaround is feasible; and

(III) sends the final version of the testing exit report to the Commission.

(iii) Any manual workarounds occurring as a result of an acceptable failure will be documented in the totalisator vendor's operations manual and these are to be reviewed by both the testing entity and the Commission for compliance.

(iv) Approval of the manual workarounds will be required from the Commission before these may be used in production.

(v) The testing entity will raise any procedural deficiencies or potential issues with the totalisator vendor and the Commission for review.

(vi) Once a solution is agreed upon between the testing entity, totalisator vendor, and the Commission, the totalisator vendor will resubmit the updated operational manuals to the testing entity and the Commission for final review.

(E) Changes classified as red should also be subjected to independent testing by a testing entity to validate the implementation of the red change prior to deployment of the change into production.

(i) This independent testing is not an exhaustive test of all operational conditions, but rather a test to verify correct implementation of the red changes for compliance and usability.

(ii) The testing entity will have visibility of totalisator vendor's test scripts and results for reference purposes (from Sec.1.5 (m)(1)(D)(ii) above).

(F) The testing entity will develop a complete baseline for any new wagering software and equipment under change control (baseline systems).

(i) For existing wagering software and equipment under change control that has been modified, the testing entity will update the relevant baseline document and highlight any changes made since the last approved version.

(ii) In conjunction with the totalisator vendor, the testing entity will devise a method of verifying that the tested version of software is the version to be put into production by the totalisator vendor.

(iii) The final version of all baseline documents will be provided to the Commission and the totalisator vendor.

(G) Upon successful completion of the assessment, the testing entity will generate a Commission report reflecting the scope of evaluation for red changes and the test results.

(i) The report will highlight any changes since the last approved baseline.

(ii) The testing entity will submit the report to the Commission and the totalisator vendor is to be copied on the report.

(iii) The compliance report is prepared against the final version of the change request that is submitted by the totalisator vendor and reviewed by the testing entity.

(iv) The Commission provides a notice following the submission of the testing entity compliance report and this notice indicates whether the change is approved or refused.

(H) Totalisator vendor can implement changes once approval from the Commission has been granted.

(2) Amber Process

(A) Changes classified as amber require independent testing by a testing entity to validate the implementation of the amber change.

(B) This independent testing is not an exhaustive test of all operational conditions, but rather a test to verify correct implementation of the amber changes for compliance and usability.

(C) The testing entity will have visibility of the totalisator vendor's test scripts and results for reference purposes.

(D) Although flexibility exists in the amber process for the testing entity to test amber changes in arrears within six months of the change being deployed to production, it may be the totalisator vendor's preference for independent testing to take place prior to deployment of the amber changes into production in order to maintain player experience and ensure that players are protected from risk.

(E) The steps in the change control process for amber changes are consistent with Sec. 1.5(m) (1) Change Control Process above.

(3) Green Process

(A) The steps in the change control process for green changes are consistent with Sec. 1.5(m) (1): (A), (B), (F) and (G) Change Control Process above.

(B) Upon successful completion of a totalisator vendor's internal testing and quality assurance process, the totalisator vendor may deploy the green changes into production.

(C) At a later date and based on a random selection of changes by the Commission, the testing entity will generate a Commission report reflecting the scope of evaluation for green changes.

(D) The testing entity will submit the report to the Commission and the totalisator vendor will be copied on the report.

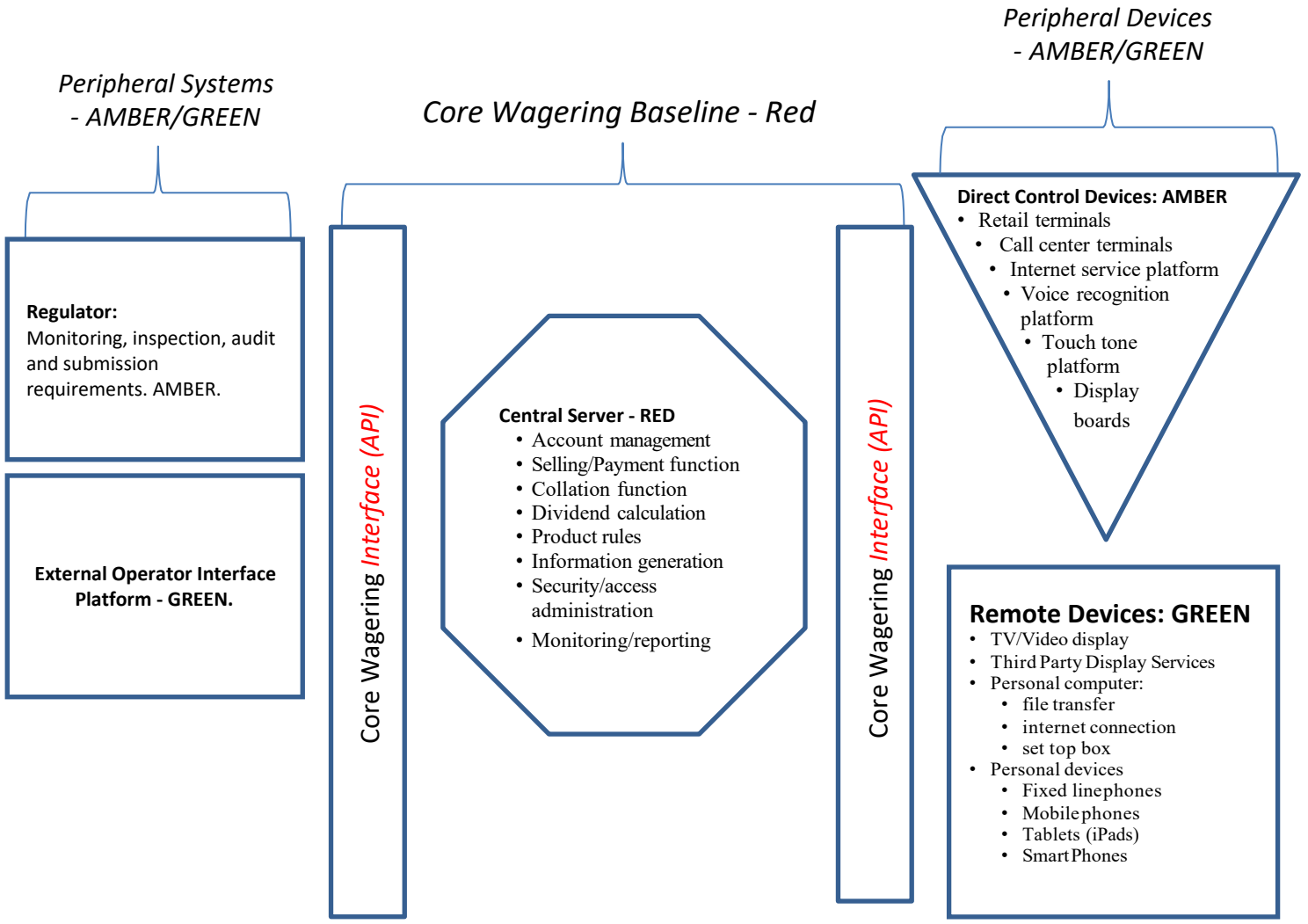
(n) Configuration Changes

(1) Configuration changes to all direct control devices inside and on the boundary of the wagering system baseline envelope must only be permitted in line with the totalisator vendor's access security policy.

(2) An audit log must be maintained for all changes to the configuration of any network devices inside and on the boundary of the wagering system baseline envelope.

(3) The audit trail must not be modifiable by persons authorized to make the configuration changes.

Diagram A: Baselines and Interfaces Classification Guide



(a) Certification & Submission

(1) Purpose

(A) This section outlines the requirements for the evaluation and assessment for compliance and approval of a totalisator vendor's wagering system and internal control system.

(B) The process includes the use of an independent testing entity for evaluation against these Rules prior to a submission to the Commission for approval to permit a wagering system version to be introduced into a racing association's production operation.

(2) The process takes into account the following documents:

(A) System Baseline Document;

(B) Network Security Document; and

(C) ITL Certification Recommendation.

(b) System Testing Requirements

(1) Testing Requirements and testing entity recommendation

(A) The security and controls, functional and operational requirements of the system are to be evaluated and recommended by an independent testing entity.

(B) The testing entity's recommendation is required on:

(i) the system integrity and reliability;

(ii) whether the system is consistent with these Rules;

(iii) whether the controls and procedures required exist and are effective; and

(iv) the System Baseline, Network Security, and Internal Control System Documents.

(c) Associated Systems Requirements

(1) All software and equipment for devices/peripherals associated with the wagering system are required to be tested for reliability in processing and delivering all transactions for the wagering system.

(2) There shall be adequate security arrangements and controls between the approved wagering system and the associated equipment.

(3) These security arrangements must form part of the independent assessment and the testing entity recommendation.

(d) Submissions Requirements

(1) The submission to the Commission for approval, at the minimum, should include the following:

(A) background of the wagering system;

(B) purpose of this submission – system/operational changes description;

(C) testing entity recommendation of the wagering system in accordance with above requirements;

(D) totalisator vendor's comments on any conditions included in the testing entity's recommendation;

(E) list of all software versions and associated software check algorithms, if any;

(F) list of all relevant hardware and operating systems – product names, models and versions;

(G) associated systems that are connected to the wagering system;

(H) a *System Baseline Document;*

(I) a *Network Security Document;* and

(J) an *Internal Control Systems Document.*

(a) The Commission requires the totalisator vendor to maintain and follow appropriate and adequate operational documentation covering:

(1) Software Selection

(A) Software functionality specification;

(B) Software change control process;

(C) System testing process; and

(D) System commissioning;

(2) Totalisator Operations Personnel

(A) Delegated Authorities;

(B) Duties;

(C) Responsibilities;

(D) Lines of communication; and

(E) System operations manual.

(3) Information to Commission

(A) A totalisator vendor's wagering system must have the capability of providing to the Commission, pari-mutuel wagering data on electronic media acceptable to the Commission.

(B) The totalisator vendor shall also provide documentation about the structure of the data.

(4) Business Contingency Plan. A totalisator vendor must submit and obtain approval for a business contingency plan (see Sec. 2.7 System Resilience & Integrity).

(b) Compliance. A totalisator vendor is subject to licensing, inspection, and regulation by the Commission to ensure the integrity of:

(1) the information obtained by use of the totalisator vendors wagering system;

(2) its employees;

(3) its Internal Control System (see Sec. 2.2 Internal Control System);

(4) its adherence to the Commission's Change Control Process (see Sec. 1.5 Change Control Process); and

(5) its engagement of an independent testing entity for evaluation of systems and changes to systems (see Sec. 1.3 System Baseline).

(a) The Commission requires that the totalisator vendor of a wagering system maintain an Internal Control System which documents a system of internal controls for wagering operations conducted on behalf of an association, as well as administrative and accounting procedures.

(b) The Commission, in its assessment or inspection of a totalisator vendor's activities and functions, may require a totalisator vendor's company to provide documented output from an accredited audit process where that process has included a review of internal control systems, for example a Statement of Audit Standards 70 (SAS 70) or Statement on Standards for Attestation Engagements 16 (SSAE 16) or equivalent audit conducted by an accredited party under the American Institute of Certified Public Accounts (AICPA) standards.

(c) An Internal Control System shall include:

(1) Software documentation.

(2) A system operations manual describing the authority, duties, responsibilities, and lines of communication for operations and support personnel. The manual shall include:

(A) sufficient detail to ensure operations personnel perform their job duties effectively;

(B) complete documentation for operation of the totalisator system and its software, including:

(i) the duties described in Sec. 2.3, Personnel Requirements, of these Rules;

(ii) clearly defined restrictions for totalisator room access;

(iii) general block diagrams of function options (menu tree) available to operations personnel;

(iv) a glossary of terms used in reports, including formulas for calculating the displayed results;

(v) the relationship, if any, between information contained in reports;

(vi) start-up and shutdown procedures;

(vii) general operating procedures;

(viii) restart and recovery procedures; and

(ix) emergency procedures, including a list of individuals to notify if a system requires an emergency revision.

(3) A systems development lifecycle manual. This manual shall include an outline of:

(A) system functionality specification;

(B) software vendor selection process, if any;

(C) internal change request management;

(D) change assessment process;

(E) internal testing and quality assurance process;

(F) system acceptance by the totalisator vendor; and

(G) commission to production process.

(4) A totalisator vendor shall develop and follow internal procedures that manage all system changes. The procedures shall:

(A) establish controls to prevent unauthorized and potentially inaccurate software changes from being incorporated into the production environment;

(B) regulate both scheduled and emergency changes to ensure the integrity of the wagering system;

(C) require software changes to be developed and tested only in a test environment that is not connected to a production environment; and

(D) require all system changes to be evaluated and certified as being consistent with the Commission's Change Control Process. (See Sec.1.5 Change Control Process).

(a) General Requirements.

(1) A totalisator vendor must provide necessary personnel to perform the duties described in the Rules.

(2) The totalisator vendor shall employ a sufficient number of personnel to ensure an adequate segregation of duties between the personnel performing the respective critical duties.

(3) The totalisator vendor may use job titles different from those in these Rules.

(4) The totalisator vendor must have job descriptions containing the experience, education, and organization training requirements for each of the following critical duties:

(A) network manager;

(B) software specialist;

(C) systems analyst;

(D) totalisator operator; and

(E) technician.

(5) The totalisator vendor must certify in writing to the Commission that its personnel are properly trained to carry out their respective duties.

(6) The totalisator vendor is responsible for the actions of its personnel relating to the operations and use of the wagering system.

(7) The totalisator vendor shall designate an individual to act as a point of contact for communications between the Commission and the totalisator vendor.

(8) The Commission may determine which totalisator vendor's personnel must be licensed.

(9) The totalisator vendor must provide the Commission:

(A) a list of all totalisator personnel assigned to work in pari-mutuel operations;

(B) the list must indicate the position for which each person is qualified; and

(C) if a new employee is assigned to work in pari-mutuel operations, the totalisator vendor must update the list of personnel and provide it to the Commission.

(10) A totalisator vendor's employee may not hold a position of software specialist and totalisator operator simultaneously unless approved by the Commission.

(11) A totalisator vendor's employee is prohibited from wagering while on duty.

(12) Network Manager. A network manager shall:

(A) coordinate the totalisator vendor's wagering systems operations;

(B) ensure that each operations personnel follow proper procedures when operating the wagering system;

(C) determine the on-site and off-site storage locations for the back-up media;

(D) provide information and prepare any report requested by the mutuel manager or pari-mutuel auditor; and

(E) ensure:

(i) a current list of operations personnel is maintained;

(ii) all operations personnel are qualified; and

(iii) the appropriate pari-mutuel accounts are maintained within the wagering system.

(13) Totalisator operator. A totalisator operator shall:

(A) maintain the communication links to the locations to and from which the racetrack facility is simulcasting and ensure data is transmitted accurately;

(B) consult with the mutuel manager and/or pari-mutuel auditor when a problem occurs in determining a pool or calculation and suggests alternatives for continued operation, including possible temporary restrictions on or suspension of the communication links;

(C) perform necessary daily performance testing, system initialization, monitoring of wagering operations, and system shutdown;

(D) execute established procedures to shutdown system software and hardware in emergency situations including:

(i) loss of communication between computers or peripheral devices;

(ii) power surges or failures;

(iii) operating with a partial system; and

(iv) restarting the system during a performance.

(E) perform necessary system maintenance;

(F) perform daily back-ups as outlined in Sec. 2.7 of these Rules;

(G) ensure information is entered in the tote maintenance log detailing all repairs or modifications to the totalisator system;

(H) immediately notify the mutuel manager and pari-mutuel auditor, via e-mail, of an incident and follow up with a written report no later than 24 hours after the time of the incident, addressing each unusual occurrence during totalisator system operations including a description of the probable cause of the occurrence and the corrective action taken;

(I) maintain a copy of the incident report or enter information about the occurrence in the system incident log for each unusual occurrence during totalisator system operations; and

(J) consult with the mutuel manager and/or pari-mutuel auditor regarding any other operational issues encountered.

(b) Technician. The totalisator vendor may provide technicians to service and maintain the wagering systems equipment.

TOTALISATOR REQUIREMENTS AND OPERATING ENVIRONMENT
DIVISION 2 OPERATIONAL REQUIREMENTS
RULE §2.4 WAIVERS FOR TECHNOLOGICAL ADVANCEMENT OR OFF-SITE PROCESSING

(a) The Commission recognizes that technology and the locations for processing wagers will change due to technology advancement. Therefore, an association or totalisator vendor may petition the Commission for a waiver of the Rules under this Chapter.
(b) To petition for a waiver under this section, the association or totalisator vendor must submit to the Commission a written application describing in detail the purpose, nature, duration, and extent of the requested waiver. The application must also include the process by which existing requirements of the system will be properly maintained.
(c) The Commission shall not grant the waiver unless the Commission determines the requested waiver will not decrease the efficiency, speed, or accuracy of either the existing pari-mutuel wagering system or the Commission's audit function.

(a) Purpose

(1) This section outlines the Commission's requirements for the entire totalisator network, including central server, local hubs, and remote operations.

(2) There are two types of sub-networks within a Totalisator Network:

(A) Device-to-Tote Network – a network restricted to local totalisator operations, conducted by a totalisator vendor on behalf of an association, to include selling and administrative terminals/devices as well as 'stop betting' and display devices.

(B) Tote-to-Tote Network – a network, whereby a central server acts as the common pooling computer for co-mingling of pari-mutuel wagers, connected to server hubs controlling other Device-to-Tote networks located at other wagering outlets.

(b) Inter-systems Communications

(1) A totalisator vendor may use a totalisator system that operates in Tote-to-Tote network and/or Device-to-Tote mode.

(2) The wagering system network must, without regard to the location of the central server:

(A) meet the requirements of this chapter;

(B) comply with the Rules;

(C) use the current version of a Tote-to-Tote message communications protocol, e.g. Inter-Tote Systems Protocol; and

(D) use the current version of Standardized Track codes recognized by the Commission.

(3) Data exchanged with computer systems and devices outside the wagering system baseline envelope must pass through at least one network control device (firewall).

(4) The network control devices must implement the controls as defined in the *Network Security Document*.

(c) Common Pooling

(1) An association's use of the totalisator vendor's wagering system to common pool is subject to the systems and equipment requirements of these Rules and that the wagering systems are in an approved location.

(2) Common pools must be merged and calculated at the site the totalisator vendor designates as the central server.

(3) The host racetrack for which a common pool is created must also provide a wagering system that:

(A) directs each wagering system involved with the common pool regarding:

(i) the pools offered;

(ii) live and scratched race animals;

(iii) common pool totals;

(iv) network odds and probable payout;

(v) start and stop wagering commands;

(vi) official orders of finish; and

(vii) deduction and payout calculations.

(B) produces reports showing the amount wagered on each race animal and pool from each site, in accordance with the approved Inter-Tote Systems Communications Protocol.

(d) Help Desk

(1) If the central server wagering system network consists of one or more remote sites, a "Help Desk" facility shall be provided to assist participating operations with problems, disputes, and maintenance calls.

(2) The Help Desk system shall enable direct access to multiple operators via a call to a dedicated number.

(3) There shall be sufficient capacity on this dedicated number for normal operation.

(4) The "Help Desk" shall maintain an e-mail contact address.

(5) All calls or e-mails to the "Help Desk" shall be answered or acknowledged within 24 hours.

(a) A totalisator vendor's wagering system using a direct connection Device-to-Tote network may use whatever communications protocol is adequate to serve the purpose of these Rules.

(b) Approval for information exchange with computer systems and devices outside the wagering system baseline envelope will be considered on a case-by-case basis by the Commission taking into account, at a minimum, the following:

(1) the requirements of Sec.2.5, Totalisator Network;

(2) the message authentication scheme utilized;

(3) physical security of the network (including interve ning hubs, bridges and routers);

(4) connections to the external devices;

(5) the sensitivity of the information being transferred;

(6) whether the computer system inside the baseline envelope or outside the baseline envelope initiates information transfer;

(7) audit information recorded on the central server pertaining to the transfer of files and information; and

(8) intrusion detection utilized and immunity from unauthorized computer access or system software attacks.

(c) A remote site is considered part of a Tote-to-Tote network and is subject to the requirements of Sec. 1.2 General System Requirements of these Rules.

(d) If the failure to compile pools or payout winning prices is isolated to a remote site:

(1) the stopping of wagering or the manual cashing and accounting of tickets need only occur at the affected site; and

(2) the relevant information must be transmitted between the central server and the remote site through the normal communication link or facsimile machine and must be verified by the voice link.

(a) System Backup

(1) The wagering system must be backed-up to removable electronic media. Before conducting pari-mutuel wagering, the totalisator vendor shall submit a backup procedure plan to the Commission for approval.

(2) There must be periodic back-ups (at least daily) of each variable database file on the wagering system's storage media.

(3) Copies of all daily database backups shall be retained at a location other than the central server site. The method used to backup and retrieve the infor mation must ensure that the information is secure and cannot be used or obtained in an unauthorized manner.

(b) Disaster Recovery

(1) A totalisator vendor must have a disaster recovery plan to allow an association to continue to conduct pari-mutuel wagering in the event of a disaster at the central server location.

(2) In the event of a disaster, e.g. a flood/fire, there must be a method of ensuring that data related to customer entitlements and government revenue, since the last backup and the transaction log, can be rebuilt up to the point of the disaster.

(3) Network documentation must:

(A) be kept in a form that can be viewed in the event of total network destruction; and

(B) include patch records, device configuration, device location, cable location, and fault procedures.

(c) Business Continuity

(1) All wagering system equipment must be able to adequately recover to the point of failure following an interruption. For example, some typical tests that shall, at a minimum, be conducted to assess compliance with these Rules are:

(A) failure of central system local area network (LAN) interfaces;

(B) failure of central LAN;

(C) failure of central data communication interface devices;

(D) failure of single data communication interface;

(E) high data communications error rates on line;

(F) a foreign or additional device placed on a LAN;

(G) a foreign or additional device placed between LAN bridges, communications controllers, or on data communication lines between sites;

(H) single data communication port failure on Remote Controller (if any); and

(I) LAN failure on Regional or Local Controller (if any).

(2) The Commission requires that, in the event of a failure whereby the system cannot be restarted in any other way, it must be possible to reload the database from the last backup point (the previous night) and fully recover vital transactions via the transaction log up to the point of the failure.

(3) Certain database update information of a non-critical nature may not be required to be automatically recovered. Exceptions of this nature would need first to be agreed with the Commission.

(d) Emergency Procedures

(1) The wagering system must be supported by an uninterruptible power supply (UPS).

(2) A totalisator vendor must have emergency procedures to address a wagering system failure.

(3) The procedures will apply whether the system is operating as a stand-alone wagering site for separate pool wagering or as a satellite in a common pool network.

(4) In a Tote-to-Tote network, if system failure occurs at either the remote site or the host:

(A) the Commission and the network's mutuel and system managers shall establish the pools for the unaffected sites;

(B) the failure site shall cease wagering; and

(C) the Commission shall then determine when the failed pari-mutuel system may resume operation.

(e) Communications within a Wagering System Baseline Envelope

(1) The Commission requires that all communications services within, and external to, the system baseline envelope:

(A) are of sufficient bandwidth capacity to manage sustained load;

(B) are secure in their technology configuration; and

(C) are resilient to unplanned interruption.

(2) There is to be no loss of information due to a failure of a redundant communications network within a wagering system baseline envelope.

(3) In this sense all information traversing the network between remote equipment and the host shall be recoverable once communications is restored.

(f) Connection of External Devices to Networks inside a Wagering System Baseline Envelope

(1) Unused ports on network devices and network control devices inside and on the boundary of the wagering system baseline envelope shall be disabled.

(2) Host computer systems, network devices, and network control devices inside and on the boundary of the wagering system baseline envelope must be immune from high loads (broadcast storms) or faults on any part of the network outside the baseline envelope.

(g) Communications between Separate Wagering System Baseline Envelopes

(1) Information flowing between different baseline envelopes in a Tote-to-Tote network should be subject to authentication and encryption, unless the intervening network is physically secure and under the complete control of the totalisator vendor. Note that wide area network communication links will be generally deemed to be outside a baseline envelope.

(2) There is to be no loss of information due to a failure of a redundant communications network between wagering systems in a Tote-to-Tote network.

(3) Communication between devices in a Tote-to-Tote network should be immune from computer/network attacks.

(h) Communication to Devices outside a Wagering System Baseline Envelope (Firewall)

(1) Network control devices shall be configured to discard all traffic other than that which is specifically permitted by the *Network Security Document*.

(2) Configurations that discard specific traffic types and allow everything else are not acceptable as a security approach.

(3) Computer systems within the wagering system baseline envelope must not be affected by computer/network attacks emanating from outside the baseline envelope.

(4) Operational procedures for network control devices must include the capturing and regular review and follow-up of all significant access violations.

(5) Approval for information exchange with computer systems and devices outside the wagering system baseline envelope will be considered on a case-by-case basis by the Commission taking into account, at a minimum, the following:

(A) the message authentication scheme utilized;

(B) physical security of the network including intervening hubs, bridges, and routers;

(C) connections to the external devices;

(D) the sensitivity of the information being transferred;

(E) whether the computer system inside the baseline envelope or outside the baseline envelope initiates information transfer;

(F) audit information recorded on the central system pertaining to the transfer of files and information; and

(G) intrusion detection utilized and immunity from computer attacks.

(i) Internet Connections

(1) Internet connections, if any, must demonstrate adequate network based and host based intrusion detection capabilities. This includes the automatic alerts in the event that a security breach occurs.

(2) The wagering system at the point where it is connected to the Internet service provider must incorporate a Demilitarized Zone (DMZ) like architecture.

(3) The internal and external firewalls must be of a type to ensure that any weakness in one firewall structure is not duplicated in the other firewall.

(4) The operator/user must have the ability to terminate a remote customer's session.

(a) Monitoring

(1) Computer hardware and systems software monitoring packages supplied by third party manufacturers/software vendors which are used to monitor hosts inside or on the boundary of a wagering system baseline envelope must be demonstrated to and approved by the Commission.

(2) Network monitoring systems supplied by third party manufacturers/software vendors and which monitor network devices and network control devices inside or on the boundary of a wagering system baseline envelope must be demonstrated to and approved by the Commission.

(3) The configuration of central system monitoring tools and network management systems must not be changed without formal authorization consistent with the totalisator vendor's access and security procedures.

(4) A device outside a wagering system baseline envelope must not be able to affect the configuration of network devices or network control devices through use of malicious practices such as:

(A) imitating the IP address of a host monitoring system or a network management system;

(B) imitating the hardware address (Ethernet address) of a host monitoring system or a network management system; or

(C) replaying previously captured communications.

(5) A device outside a wagering system baseline envelope must not be able to:

(A) affect the operation of the central system; and

(B) read or modify critical data.

(b) Reporting

(1) A wagering system must be able to produce hard copy reports and logs necessary to audit pari-mutuel activity and to recreate any given day of wagering in its entirety.

(2) A totalisator vendor shall retain the information needed to produce these reports and logs on storage devices for at least 365 days after the date the wagering occurred.

(3) A totalisator vendor shall provide information requested by the Commission no later than 48 hours after the totalisator vendor receives the request.

(4) A printed report for the Commission must have consecutively numbered pages and each page of the report must be headed with:

(A) the name of the race track;

(B) the date and time in hours, minutes, and seconds the report was produced;

(C) the performance number, if applicable;

(D) the wagering site to which the report refers;

(E) the version of software in use; and

(F) the parameters of the data provided.

RULE §3.2 PRE-WAGERING REPORTS

(a) On request by an authorized officer, before starting wagering each day, the operations personnel shall print any of the following reports:

(1) a System Initialization Report showing:

(A) the date and time the system was initialized;

(B) the identity of the operations personnel initializing the system; and

(C) the software version in use;

(2) a Configuration Parameter Report showing:

(A) the pools that may be offered and that are currently operational in the wagering system;

(B) the display cycle frequency, pools, any minimum pool required, minimum wagers, and means of display of any approximate odds or will-pays produced;

(C) the minimum and maximum value of wagers for every pool that a direct control device may accept;

(D) which direct control devices are activated;

(E) which remote sites may input into the wagering system;

(F) the split percentages and payout parameters for each multi- leg pool offered;

(G) verification of all operational locking devices;

(H) the amount of delay between locking switch activation and actual stop betting or cancelling;

(I) the canceling parameters for regular and supervisory direct control devices;

(J) configurations placed on each direct control device;

(K) the method of breakage and rounding used in calculating the payout;

(L) takeout percentages for each host site and for the live races; and

(M) federal tax withholding rates and parameters;

(3) a Race Information Report showing for each live race and simulcast performance to be offered:

(A) the pools to be opened, indicating totals starting at zero and totals starting with money from advance wagering;

(B) pool summaries of all advance wagering;

(C) money added due to overages;

(D) underpayments or money added due to carry-overs; and

(E) the race animals for each race, showing entries and scratched animals;

(4) an Odds Report showing the opening line of odds for the Win pool; and

(5) a teller/cash terminal report listing the teller's name and location.

For each race offered, the wagering system must be capable of printing the following reports and have them available for review by authorized officers :

(1) a Scratch Report showing the time each late scratch was entered into the wagering system and the amount of money to be refunded in each pool;

(2) a Betting Report, produced immediately on activation of the stop betting command and final merge of wagering information from all sites showing:

(A) the amount wagered and to be refunded for each betting interest or combination in each pool offered, and the net amount for each pool to be used for calculating the payout;

(B) the final dollar odds for the Win pool; and

(C) time of stop betting and time of each pool transmission;

(3) a Calculating Price Report, produced before each race is declared official, showing for each pool:

(A) the winning betting interests or combinations;

(B) the winning wagers;

(C) the minimum payout prices;

(D) the breakage;

(E) the amount paid to the public;

(F) the total amount wagered;

(G) the total amount refunded;

(H) the amount added to the pool, when applicable;

(I) the actual pool total; and

(J) the takeout in total dollars;

(4) a Probable Payout Report showing the payouts for multiple and exotic pools, subject to scratches, cancellations, and dead heats;

(5) a Scan Report for multi- leg pools of four or more legs, showing:

(A) the total wagered in the pool;

(B) the amounts of any carryover;

(C) the winners of completed legs;

(D) the amount of possible winning wagers, based on paying the winner of completed legs combined with every betting interest entered in subsequent legs; and

(E) late scratches in each leg;

(6) a Race Summary Report, produced before and after the race results are official, showing as the sum for all pools paid out in that race:

(A) the amount wagered;

(B) the amount refunded;

(C) the net amount to be used for calculating the payout;

(D) any money added to the pool;

(E) the actual pool total;

(F) the total commissions;

(G) the breakage;
(H) the amount paid to the public;
(I) the carryover balances; and
(J) the liabilities (due to/due from);

(7) a Daily Summary Report, produced with the Race Summary Report, showing the cumulative totals, for each pool and for all pools combined, of the items listed under the Race Summary Report.

RULE §3.4 END-OF-DAY REPORTS

After wagering has ceased each day, the totalisator system must be capable of producing and printing the following reports and have them available for review by the mutuel manager and/or the pari-mutuel auditor, as requested;

(a) a Wagering Device Balance Report showing for every direct control device terminal operated on that day including:

(1) the teller's name or identification number, or a patron activated designation;

(2) the total value and number of tickets sold, cancelled, and cashed, separating the outs from the current day's tickets;

(3) the total amount of money drawn from the money room, including the beginning draws;

(4) the total amount of money returned to the money room; and

(5) a listing of adjustments made to each wagering device balance after each teller/cash terminal has been individually balanced;

(b) a Wagering Summary Report showing:

(1) by wagering site, the amount wagered, refunded, and added for every pool and for each race;

(2) the time of day each race's pools closed;

(3) the commissions deducted, breakage calculated, and amount paid out for every pool in each race;

(4) the total value of outstanding tickets before the pools were opened for the performance, the value of tickets cashed during the performance, the value of tickets to be added to the outstanding ticket total, and the new outstanding ticket total; and

(5) the total value of outstanding vouchers before the pools were opened for the performance, the value of vouchers cashed during the performance, the value of vouchers to be added to the outstanding voucher total, and the new outstanding voucher total;

(c) a System Balance Report comparing the pool and paid-out totals obtained by processing the transaction files with the pool and paid-out totals obtained from the actual calculations;

(d) a Money Room Balance Report showing cash added and subtracted from the beginning day's balance resulting from the day's wagering and cashing transactions; and

(e) a IRS Report showing the winner's social security number, the ticket number, amount won, and taxes withheld for each transaction requiring a Form W2-G.

RULE §3.5 AD HOC REPORTS

When requested by an authorized officer, the totalisator operations personnel shall produce the following reports:

(a) an Odds Progression Report showing each successive line of odds for the Win pool and the time it was displayed to the public;

(b) a Ticket and Transaction History Report showing the appropriate portion of the ticket history log for the requested ticket identification numbers;

(c) a Wagering Device History Report showing the portion of the wagering device log requested;

(d) an Outstanding Ticket Report showing the following information for uncashed winning tickets retained in the totalisator system:

(1) the ticket identification number;
(2) the wagers on the ticket;
(3) the date and performance for which the ticket is outstanding;
(4) the value of the winning wagers; and
(5) the direct control device location and number;

(e) an Outstanding Tickets Cashed Report, for a performance, race, or pool, showing each outstanding ticket cashed that day, in the form of the Outstanding Ticket Report, including the identity of the direct control device that cashed the ticket and an indication as to whether the ticket was cashed using a manual keyboard entry or an automatic machine read;

(f) a Manually Cashed Tickets Report, for a performance, race, or pool, showing every ticket cashed that day in the form of the Ticket History Report, the identity of the direct control device that cashed the ticket, and an indication as to whether the ticket was cashed using a manual keyboard entry or an automatic machine read;

(g) a Cancelled Tickets Report, for a performance or race, showing each ticket canceled that day in the form of the Ticket History Report, the identity of the direct control device that cashed the ticket, and an indication as to whether the ticket was cashed using a manual keyboard entry or an automatic machine read;

(h) a Network Balance Report summarizing the activity and liabilities for each site within a Tote-to-Tote network;

(i) a Scan Report for each multi-leg pool over four legs, showing the amount bet on every combination of the pool and the total amount bet; and

(j) an Account Activity Report showing the following information for each E-wagering account:

(1) the unique account number;
(2) the date and time of each transaction;
(3) the unique identification number of each transaction;
(4) the location of each wager;
(5) the amount of each transaction;
(6) the type of pool, animal number, and amount of each wager;
(7) the account balance; and

(8) the account holders name;

(k) a Stop Payment Report showing the identity of the wager that has been stopped and when that wager is released for payment; and

(l) an Exchange Rate report that identifies the currency of sites participating in a network.

RULE §3.6 SPECIAL REPORTS

(a) A totalisator vendor shall produce any special report requested by the Commission no later than 72 hours after receiving the request. The wagering system must be able to produce a special report that filters data by:

(1) performance;
(2) race;
(3) pool;
(4) betting interest;
(5) direct control devices;
(6) date;
(7) sites; or
(8) any combination of the indicia in this section.

(b) Report heading must contain the criteria outline in Section 3.1(b) (4), General Requirements, for a report.

(a) On-Line Logs

(1) The wagering system must produce various daily on-line logs. The totalisator operations personnel shall provide a printed copy of a daily log to an authorized officer(s) on request.

(2) The wagering system must produce the following logs:

(A) a Teller/Wagering Machine History Log showing for every direct control device operated during a performance:

(i) the time the direct control device was opened and closed;

(ii) for each wagering transaction, the wagers made, tickets issued, and total value of the transaction;

(iii) for each cashing, cancelling, or refunding transaction, the identification numbers of the tickets processed, the wagers paid out, and the value of the wagers paid out;

(iv) for each cashing transaction, an indication as to whether the ticket was cashed using a manual keyboard entry or an automatic machine read;

(v) the amount of each cash draw and return;

(vi) any special function, including Teller Balance, accessed through the direct control device; and

(vii) the times of day each of the transactions listed in this subdivision was made;

(B) a Ticket History Log showing for every ticket issued:

(i) the identification number of each cashed/canceled ticket;

(ii) the direct control device location and number;

(iii) the wagers and their values;

(iv) the cashing/canceling machine location and number;

(v) the amount paid out;

(vi) the time of day each transaction occurred; and

(vii) an indication as to whether each transaction was manual or automatic;

(C) a User Terminal Log showing the time of day of each entry for:

(i) each terminal other than a wagering machine operating during a day:

(I) each log-on/log-off and the operator/user's ID code;

(II) each command or transaction entered;

(III) each Stop Betting, Order of Finish, Official, and Sales Open command and the device that issued it;

(IV) each occurrence of loss/restoration of communication between computers or sites; and

(V) each occurrence of discrepancy between computers or sites when comparing databases;

(ii) each direct control device operated during a performance:

(I) each log-on/log-off and the teller's ID code, if applicable; and

(II) each instance of loss/restoration of communication and the direct control device;

(D) a System Error Log showing the date and time of each error;

(E) a System Journal Log with date and time of each entry, including remote access, showing every day the system is operated for wagering, maintenance, or other purposes:

(i) System shutdown commands, the device from which they were issued, and the user ID of the individual issuing the commands;

(ii) the individual user ID and the originating device for every attempt successful or unsuccessful, to access the operating system;

(iii) the individual user ID and the originating device for every attempt, successful or unsuccessful, to access the application programs;

(iv) all commands that affect the operating environments issued from the operating system command line;

(v) all commands issued from within the application program in an attempt to access the operating system; and

(vi) a listing of every operational or operating terminal during computer operation;

(F) an Account Activity Log showing the following information for each E-wagering account:

(i) the unique account number;

(ii) the date and time of each transaction;

(iii) the location of each wager;

(iv) the amount of each transaction;

(v) the type of pool, animal number, and amount of each wager;

(vi) the account balance; and

(vii) the account holder's name.

(b) Off-line Log

(1) The totalisator operations personnel must maintain a system incident log and make it available on request for review by an authorized officer(s).

(2) The system incident log must include a description of each incident involving the wagering system, including system failures, their causes, and corrective actions taken.

RULE §3.8 WAGERING MONITORING SYSTEM

(a) Notwithstanding any other reporting and data retention requirements of this Section 3, the Commission may, at a future point in time, give consideration to the use of a real time wagering monitoring system (WMS).

(b) The Commission may use the WMS to enhance its audit and inspection capabilities through access to, and assessment of, information on totalisator activity held in the totalisator vendor's wagering systems.

(c) WMS information would, at a minimum, consist of bet and pool calculation records and betting and revenue statistics, as well as operational activity alerts.

(d) A WMS would enable the Commission to monitor the totalisator vendors' wagering operations in real-time and thereby enhance its compliance program designed to protect the interests of players by independently ensuring the integrity of the wagering system.

(1) The information from the totalisator vendor's wagering systems would ideally be sent to a tamper-proof WMS data store (the WMS Vault).

(A) The Commission would have online access to the WMS Vault and could access the data in it using standard office software tools, e.g. Microsoft Excel.

(B) A WMS Vault shall be backed up at regular intervals to enable complete restoration in a disaster recovery situation.

(C) The data monitoring and collection software will only have permissions to insert data into the WMS Vault. There shall be no module with permission to update or modify the data.

(D) The report generator modules shall only have permission to read data from the WMS Vault.

(E) The Commission shall have online access to the WMS Vault and be able to view data using standard and customized reporting tools.

(F) The Commission shall be able to view the data recorded by the WMS using standard and customized reports. This information shall be provided or made available upon request in the following format:

(i) *Monitor Entity*: name and description of the particular data recorded, e.g. Advertised Off Time, Scratching, Pool Betting Close Time, etc.

(ii) *When*: time the Monitor Event was generated.

(iii) *Systems*: indicates the system(s) that generates the Monitor Event, e.g. name of totalisator system provider.

(iv) *Event, Pool, or Bet: Monitor Entity* is generated at either an event, pool, or bet level using commission approved racing codes.

(v) *Specific Data*: data specific to this Monitor Event only, e.g. pool type, late scratching, cancellation etc.

(vi) *Common Data*: data that is common to all Monitor Events.

(G) On each event the Commission shall be able to:

(i) view all the data as it comes into the WMS Vault; or

(ii) run a report with particular specifications for further analysis on an event, a meeting, and all events on a particular day, or period.

Revision History

Version Number	Date Modified	Rule Number	Page	Change Description
1.2a	Dec. 12	Section 1.4(f)(2)(b)	17	Amended to add, "Said tote system backup may be operated by local racing association personnel and/or racing stewards, and also remotely operated by tote personnel not physically located at the racing association. If the tote system backup is operated remotely, a protocol for the remote operation shall be submitted to the racing commission for approval."
1.01	July 2012	Section 1, Rule 1.1(h)	15	(e) Functionality (1) The Commission requires that direct control devices: (A) operate with read/print/display accuracy and integrity, for example: (i) bill acceptors shall be capable of properly accepting and crediting applicable currency; (ii) ticket printers shall print valid ~~wagering~~ mutuel tickets. Each valid mutuel ticket must have printed on its face: I. the name of the racetrack facility where the wager was placed; II. the name of the racetrack where the race was conducted; III. the number of the race; IV. the unique computer-generated ticket number; V. the date the ticket was issued; VI. the date of the race for which the ticket was issued; VII. the number of the ticket-issuing machine; VIII. the type of pool; IX. the number of each entry on which the wager was placed; X. the dollar amount of the wager; and XI. the expiration date of the ticket. ~~and vouchers containing requirements in Sec. 321.29 Mutuel Tickets and Sec. 321.31 Vouchers;~~ (iii) ticket printers shall print valid

				vouchers. Each valid mutuel voucher must have printed on its face: I. the name of the racetrack facility where the voucher was issued. II. the unique computer-generated voucher number;

				III. the date the voucher was issued; IV. the number of the ticket-issuing machine; V. the dollar amount of the voucher; and VI. the expiration date of the voucher. (iv) ticket readers shall be able to read, validate, and properly credit vouchers and tickets; (iv) devices shall be evaluated as to their methods for validating tickets, including capture of valid tickets by the device and branding marks; (vi) not allow nil, partial, or duplicate print of a ticket; and (vii) access correct functions as labeled on a keypad;
1.01	July 2012	Section 1, Rule 1.1(h)	2	(h) Definitions. The following definitions are to be used in reading and following ~~the Rules in Section 321, Subchapter B~~ The Association of Racing Commissioners International Totalisator Technical Standards.
1.00	**July 2011**	**Original Document Published**		