Information Technology – Audit
25 CFR 543.20 Toolkit

Version 1.0

NIGC Compliance Division

NIGC Information Technology Audit–25 CFR 543.20 Toolkit

Over twenty five years ago Congress adopted the Indian Gaming Regulatory Act (IGRA) to provide a statutory basis for gaming by Indian tribes. The National Indian Gaming Commission (NIGC) was created by IGRA to regulate gaming activities conducted by sovereign Indian tribes on Indian lands. The mission of the NIGC is to fully realize IGRA's goals of: (1) promoting tribal economic development, self-sufficiency and strong tribal governments; (2) maintaining the integrity of the Indian gaming industry; and (3) ensuring that tribes are the primary beneficiaries of their gaming activities. One of the primary ways the NIGC does this is by providing training and technical assistance to Indian tribes and their gaming regulators.

The National Indian Gaming Commission (NIGC) is pleased to present this Toolkit to all Compliance and Auditing staff. This reference guide is intended to assist IT Auditor(s), Gaming Commissioner(s) and Operations personnel in the performance of measuring compliance of their operation(s) with 25 CFR 543.20. The toolkit is designed to provide each standard as it relates to 543.20, the language of the standard, the intent of the standard, and then a recommended testing step which will ensure minimum regulatory compliance.

This Toolkit is designed to meet the minimum requirements of the NIGC MICS and does not take into account operations Tribal Internal Controls Standards (TICS) and or System of Internal Controls Standards (SICS), which may require further testing. The NIGC encourages Operations to develop standards that exceed the Minimum Internal Control Standards , because each operation is unique, therefore a robust set of controls is warranted.

If you have questions or comments about this guide, please contact the NIGC Compliance Division at **training@nigc.gov**. For more information, visit the NIGC website at **http://www.nigc.gov.**

Citation	Language	Intent and Testing
§ 543.20 (a-b)		
543.20 (a)(1)	*Supervision.* (1) Controls must identify the supervisory agent in the department or area responsible for ensuring that the department or area is operating in accordance with established policies and procedures.	**Intent:** To ensure that the TICS identify who is the supervisory agent in the department and is responsible for ensuring the IT Department is operating in accordance with established policy and procedures. **Testing: 1.** Review TICS to identify controls with respect to the supervision of the IT Department. **2.** Identify any additional controls required by the TGRA with regards to supervision. **3.** Review SICS to ensure that operations have identified and implemented controls with regards to the TGRA requirements in their TICS.
543.20(a)(2)	The supervisory agent must be independent of the operation of Class II games.	**Intent:** To ensure proper segregation of duties that the IT supervision is independent of all Class II Games. Best practices suggests that the IT department should be independent of all casino departments and should report directly to the General Manager. **Testing:** **1.** Review Information Technology Organizational Chart. **2.** Inquire with IT supervision to determine who they report to.
543.20(a)(3)	Controls must ensure that duties are adequately segregated and monitored to detect procedural errors and to prevent the concealment of fraud.	**Intent:** To ensure that IT personnel are not to be assigned conflicting roles, i.e., financial, accounting and gaming responsibilities that cannot be effectively monitored for the detection of fraud or the concealment of procedural errors. **Testing: 1.** Review Human Resources job descriptions in IT personnel files in addition to IT user groups and accounts. **2.** Flag instances of computerized IT access to financial, accounting or gaming roles.

Citation	Language	Intent and Testing
§ 543.20 (a-b)		
543.20(a)(4) (i-iii)	Information technology agents having access to Class II gaming systems may not have signatory authority over financial instruments and payout forms and must be independent of and restricted from access to: (i) Financial instruments; (ii) Accounting, audit, and ledger entries; and (iii) Payout forms.	**Intent:** IT personnel who possess access to Class II gaming shall not have access to or signatory authority over financial instruments, accounting, audit, ledger entries and payout forms. **Testing: 1.** Review system user access accounts of IT personnel for financial, accounting, ledger and payout form access. **2.** Review physical payout forms for winners. **3.** Review SICS to verify that IT personnel are not authorized to sign
543.20(b)	As used in this section only, a system is any computerized system that is integral to the gaming environment. This includes, but is not limited to, the server and peripherals for Class II gaming system, accounting, surveillance, essential phone system, and door access and warning systems.	**Intent:** Computerized 'systems' are defined as computerized systems integral to the operation of the gaming environment. Systems include electronic / electrical networked-system environments. **Testing:** Review gaming operations architectural plans and computerized network system design layout and applications system inventory.

Citation	Language	Intent and Testing
§ 543.20 (c)		
543.20 (c)	Class II gaming systems' logical and physical controls. Controls must be established and procedures implemented to ensure adequate:	**Intent:** To ensure that operational SICS have identified and implemented controls with regards to the TGRA requirements in their TICS. **Testing:** Review IT TICS, SICS and Policies and Procedures.
543.20(c)(1)	Control of physical and logical access to the information technology environment, including accounting, voucher, cashless and player tracking systems, among others used in conjunction with Class II gaming;	**Intent:** To ensure both physical and logical access to critical computerized environments, networks and application system are restricted to authorized users. **Testing:** Review IT TICS, SICS and Policies and Procedures for verification of controls in place for the control of both physical and logical access to the information technology environment used in conjunction with Class II gaming by reviewing the user access list against the current HR list.
543.20(c)(2)	Physical and logical protection of storage media and its contents, including recovery procedures;	**Intent:** To ensure that stored and archived financial, accounting and gaming data can be readily restored to the gaming operations 'live' environment during or after a critical system failure. **Testing: 1.** Review IT TICS, SICS and Policies and Procedures for data recovery controls and processes. **2.** Review data backup and recovery scheduling, testing and physical assessment of the data storage facility.

Citation	Language	Intent and Testing
§ 543.20 (c)		
543.20(c)(3)	Access credential control methods;	**Intent:** To ensure that only properly vetted and authorized personnel have access to the gaming operations secured logical and physical environments. **Testing:** Review IT TICS, SICS and Policies and Procedures for effective logical and physical access control methods and reviewing the user access list against the current HR list.
543.20(c)(4)	Record keeping and audit processes; and	**Intent:** To ensure that administrative bookkeeping and accurate and timely documentation supporting audit processes is maintained. **Testing:** Review SICS and audit results with findings from previous internal and external audits and also any records kept by the IT operation.
543.20(c)(5)	Departmental independence, including, but not limited to, means to restrict agents that have access to information technology from having access to financial instruments.	**Intent:** To ensure that technical departments and technical personnel are restricted from access to financial instruments. **Testing:** Review SICS and organizational chart structure. Perform review of financial logical access permissions and authorizations of technical personnel. Flag access accounts authorizing IT personnel to financial instruments.

Citation	Language	Intent and Testing
§ 543.20 (d-e)		
543.20(d)	*Physical security.* (1) The information technology environment and infrastructure must be maintained in a secured physical location such that access is restricted to authorized agents only.	**Intent:** To ensure that the information technology environment and supporting environments are maintained in a secured physical location. Access is to be restricted to authorized personnel in a secured physical location that is accessible only to authorized personnel. **Testing:** Conduct physical walkthrough inspection noting the access / denial methods to restrict physical access to critical locations, i.e., HID card, hard-key, biometrics, pin code, password, etc.
543.20(d)(2)	Access devices to the systems' secured physical location, such as keys, cards, or fobs, must be controlled by an independent agent.	**Intent:** To ensure that those who are recipients of the security access tools, are not the same as those who authorize, manage and assign the security access tools. **Testing: 1.** Verify roles, responsibilities and organizational positions of the personnel responsible for physical access management. **2.** Note any potential independent conflicts and effectiveness of managerial oversight.
543.20(d)(3)	Access to the systems' secured physical location must be restricted to agents in accordance with established policies and procedures, which must include maintaining and updating a record of agents granted access privileges.	**Intent:** To ensure only authorized agents gain access to secured physical locations, in accordance with established Policies and Procedures to include maintaining and updating a ledger or listing of those agents granted access privileges. **Testing:** Review SICS, TICS, Policies and Procedures also spot check any access logs and review of management's approved Authorized User Access Listing(s).

Citation	Language	Intent and Testing
§ 543.20 (d-e)		
543.20(d)(4)	Network Communication Equipment must be physically secured from unauthorized access.	**Intent:** To ensure the network infrastructure and equipment, organizational intranet and all incoming and outgoing network communications are secured from unauthorized access. **Testing: 1.** Verify the software application affected has the proper physical security measures in place that can be tested over the Network Communication Equipment environment. **2.** Obtain network communications diagrams to include flow of internal and external data flows, hardware topology and system application flows. **3.** Perform physical walkthrough of network communications architecture and facilities to include surveillance and security measures.
543.20(e)(i-iii)	*Logical security.* (1) Controls must be established and procedures implemented to protect all systems and to ensure that access to the following is restricted and secured: (i) Systems' software and application programs; (ii) Data associated with Class II gaming; and (iii) Communications facilities, systems, and information transmissions associated with Class II gaming systems.	**Intent:** To ensure that all organizational software systems and data and communication systems are restricted from unauthorized access. **Testing:** Verify the effectiveness of security and operational controls supporting the physical and logical segregation of the organizational intranet and external internet. This can be accomplished by reviewing diagrams and technical documents along with any logs
543.20(e)(2)	Unused services and non-essential ports must be disabled whenever possible.	**Intent:** To ensure the deactivation or isolation of unused services and non-essential communication and computer ports. Non-essential ports are to be disabled whenever possible. **Testing:** Review IT Policies and Procedures and perform walkthrough of open ports in vacated offices, cubicles, conference rooms, etc.

Citation	Language	Intent and Testing
§ 543.20 (e-f)		
543.20 (e)(3)	Procedures must be implemented to ensure that all activity performed on systems is restricted and secured from unauthorized access, and logged.	**Intent:** To ensure that procedures are in place that all activity performed on the computerized system is recorded and / or logged. **Testing:** Review SICS and IT Policies and Procedures. Review change management documentation, i.e., work requests, job orders, work orders and review access logs.
543.20(e)(4)	Communications to and from systems via Network Communication Equipment must be logically secured from unauthorized access.	**Intent:** To ensure that electronic communications, to include wireless, copper wire, satellite or cellular, is logically secured from unauthorized access. **Testing: 1.** Review TICS and SICS and Policies and Procedures. **2.** Verify that network security measures are in place to include any necessary routers, firewalls, switches and encryption. **3.** Verify that software upgrades to communications equipment is current.
543.20(f)	*User controls.* (1) Systems, including application software, must be secured with passwords or other means for authorizing access.	**Intent:** To ensure that only authorized system account holders have access to computerized systems, including application software. **Testing: 1.** Verify that all critical accounting, financial and gaming systems are secured with passwords or other means to limit logical system access. **2.** Review user access listings.

Citation	Language	Intent and Testing
§ 543.20 (e-f)		
543.20(f)(2)	Management personnel or agents independent of the department being controlled must assign and control access to system functions.	**Intent:** To ensure that procedures are in place that all activity performed on the computerized system is recorded and / or logged. **Testing:** Review SICS and IT Policies and Procedures. Review change management documentation, i.e., work requests, job orders, work orders and review access logs.
543.20(f) 3) (i-iii)(A-C)	Access credentials such as passwords, PINs, or cards must be controlled as follows: (i) Each user must have his or her own individual access credential; (ii) Access credentials must be changed at an established interval approved by the TGRA; and (iii) Access credential records must be maintained either manually or by systems that automatically record access changes and force access credential changes, including the following information for each user: (A) User's name; (B) Date the user was given access and/or password change; and (C) Description of the access rights assigned to user.	**Intent:** To ensure that all authorized access holders meet minimum credential requirements to retain their access permissions. **Testing: 1.** Review TICS, SICS and group user account holders. **2.** Review administrator account parameter settings for group and individual user access settings.

Citation	Language	Intent and Testing
§ 543.20 (f-g)		
543.20 (f)(4)	Lost or compromised access credentials must be deactivated, secured or destroyed within an established time period approved by the TGRA.	**Intent:** To ensure that lost or stolen user access credentials are deactivated in the minimum time period stated by the TGRA. **Testing:** Review TICS, SICS, Policies and Procedures and Employee Manuals for employee and IT Management action when compromised credentials are reported.
543.20(f)(5)	Access credentials of terminated users must be deactivated within an established time period approved by the TGRA.	**Intent:** To ensure that access credentials of terminated users are deactivated in the minimum time period stated by the TGRA. **Testing: 1.** Review TICS, SICS, Policies and Procedures and Employee Manuals for employee, IT Management and Human Resources action when compromised credentials are reported. **2.** Review user access lists for former employees
543.20(f)(6)	Only authorized agents may have access to inactive or closed accounts of other users, such as player tracking accounts and terminated user accounts.	**Intent:** To ensure that terminated, transferred or resigned personnel accounts are only accessible by, or approved by, TGRA authorized agents. **Testing: 1.** Review TICS, SICS and IT Policies and Procedures regarding User Network Security and Access activity. **2.** Verify appropriate access by comparing access logs/permissions to TICS/SICS/Policies & Procedures.

Citation	Language	Intent and Testing
§ 543.20 (f-g)		
543.20(g)	*Installations and/or modifications*. (1) Only TGRA authorized or approved systems and modifications may be installed.	**Intent:** To ensure that organizational personnel must first seek approvals of TGRA and IT Management prior to the introduction of outside software or modifications to the network or computerized systems. **Testing:** Review TICS, SICS and IT Policies and Procedures. Review a sampling of previous change management request forms for proper approvals and signatures.
543.20(g)(2) (i-iv)	Records must be kept of all new installations and/or modifications to Class II gaming systems. These records must include, at a minimum: (i) The date of the installation or modification; (ii) The nature of the installation or change such as new software, server repair, significant configuration modifications; (iii) Evidence of verification that the installation or the modifications are approved; and (iv) The identity of the agent(s) performing the installation/modification.	**Intent:** To ensure that evidential and supporting documentation is retained for all new installations and modifications to Class II gaming systems. **Testing: 1.** Review TICS, SICS and IT Policies and Procedures regarding change management and asset management. **2.** Review sampling of records retained of records of installations and / or modifications.

Citation	Language	Intent and Testing
§ 543.20 (g-i)		
543.20 (g)(3)	Documentation must be maintained, such as manuals and user guides, describing the systems in use and the operation, including hardware.	**Intent:** To ensure that documentation accompanying new or used hardware is retained describing said system in use and it's proper operation, to include hardware systems. **Testing: 1.** Review sampling of supporting system user manuals, specification sheets, build sheets, etc., and a walkthrough or the secured location(s) where maintained. **2.** Documentation may be stored or archived in an approved documentation storage file onsite, or on the vendor / manufacturers website.
543.20(h)(1) (i–vii)	*Remote access.* (1) Agents may be granted remote access for system support, provided that each access session is documented and maintained at the place of authorization. The documentation must include: (i) Name of agent authorizing the access; (ii) Name of agent accessing the system; (iii) Verification of the agent's authorization; (iv) Reason for remote access; (v) Description of work to be performed; (vi) Date and time of start of end-user remote access session; and (vii) Date and time of conclusion of end-user remote access session.	**Intent:** To ensure remote access connections are secure, approved and accurately recorded / logged. **Testing:** Review SICS, TICS and IT Policies and Procedures and sampling of remote access session logs. Remote access logs at a minimum must provide bullet points (i) through (vii).

Citation	Language	Intent and Testing
§ 543.20 (g-i)		
543.20(h)(2)	All remote access must be performed via a secured method.	**Intent:** To ensure that lost or stolen user access credentials are deactivated in the minimum time period stated by the TGRA. **Testing:** Review TICS, SICS, Policies and Procedures and Employee Manuals for employee and IT Management action when compromised credentials are reported.
543.20(i)	*Incident monitoring and reporting.* (1) Procedures must be implemented for responding to, monitoring, investigating, resolving, documenting, and reporting security incidents associated with information technology systems.	**Intent:** To ensure expedient and appropriate response to computerized incidents, faults, errors or cyber attacks. **Testing: 1.** Review TICS, SICS, IT Policies and Procedures and review sampling of Incident Responses and the courses of action taken. **2.** Review relevant work orders, job orders or work requests completed to address the incident(s).
543.20(i)(2)	All security incidents must be responded to within an established time period approved by the TGRA and formally documented.	**Intent:** To ensure all security incidents are responded to and addressed within a practical time period to mitigate the associated incident risk. **Testing:** Review TICS, SICS, or P&P for a time period established by security incidents should be responded to as soon as possible from the moment of notification.

Citation	Language	Intent and Testing
§ 543.20 (j-l)		
543.20 (j)(1) (i-v)	*Data backups.* (1) Controls must include adequate backup, including, but not limited to, the following: (i) Daily data backup of critical information technology systems; (ii) Data backup of critical programs or the ability to reinstall the exact programs as needed; (iii) Secured storage of all backup data files and programs, or other adequate protection; (iv) Mirrored or redundant data source; and (v) Redundant and/or backup hardware.	**Intent:** To ensure that adequate data and software backup controls are in place to support expedient organizational data restoration. **Testing: 1.** Review TICS, SICS and data backup scheduling processes for all application systems hosted by the gaming operation. **2.** Verify the secured storage of all backup data files and backup media.
543.20(j) (2)(i-iii)	Controls must include recovery procedures, including, but not limited to, the following: (i) Data backup restoration; (ii) Program restoration; and (iii) Redundant or backup hardware restoration.	**Intent:** To ensure that organizational controls include data, program, hardware and network restoration and recovery procedures. **Testing: 1.** Review SICS, TICS and Information Technology Policies and Procedures regarding management of system recovery processes. **2.** Review recovery and restoration documentation to include data, programs and redundant hardware.
543.20(j)(3)	Recovery procedures must be tested on a sample basis at specified intervals at least annually. Results must be documented.	**Intent:** To ensure that organizational recovery procedures are tested annually by Information Technology personnel and IT Management. **Testing: 1.** Review TICS, SICS and IT Policies and Procedures to routine recovery procedures. **2.** Review annual recovery testing documentation for performance and results of recovery test.

Citation	Language	Intent and Testing
§ 543.20 (j-l)		
543.20(j)(4)	Backup data files and recovery components must be managed with at least the same level of security and access controls as the system for which they are designed to support.	**Intent:** To ensure that backup data files and recovery components are managed to at least the same stringent level of security as the systems for which they are supporting. **Testing:** Perform walkthrough of the backup data files physical location for security access restrictions, surveillance monitoring, fire suppression systems and HVAC equipment function.
543.20(k)	Software downloads. Downloads, either automatic or manual, must be performed in accordance with 25 CFR 547.12.	**Intent:** To ensure that software downloaded to the gaming operation from outside sources, either automatic or manual, is in strict compliance with 25 CFR 547.12. **Testing: 1.** Review TICS, SICS and Policies and Procedures. Verify that software downloads are delivered through secure methods. **2.** Review Class II system records to verify that the Class II system has recorded the (a) date and time of the initiation and (b) completion of any download, (c) the components that received it, (d) the version of the download package and any software downloaded, (e) status of the download attempt (i.e., success or failure), (f), unique identifier of individual conducting or scheduling the download.
543.20(l)	*Verifying downloads.* Following download of any Class II gaming system software, the Class II gaming system must verify the downloaded software using a software signature verification method. Using any method it deems appropriate, the TGRA must confirm the verification.	**Intent:** To ensure that following the download of Class II gaming system software, the gaming system must verify the download with a software signature verification method, approved by the TGRA. **Testing: 1.** Review TICS, SICS and Policies and Procedures and verify that software downloads meet requirements. **2.** Review records to confirm TGRA verification of software

THIS PAGE INTENTIONALLY LEFT BLANK

25 CFR 543.20 Toolkit

Version 1.0

NIGC Compliance Division