

Achieving Compliance for the Indian Gaming Industry through ISO 27001



Network Computing Architects, Inc.

A compliance comparison to the regulations of the Indian Gaming Industry

It is estimated by the National Indian Gaming Commission (NIGC) that there are over 360 Indian Gaming establishments in the United States. Since the inception of the Indian Gaming Regulatory Act (IGRA) in 1988, the Indian Gaming industry has seen significant growth in annual revenues from \$200 million to over \$26 billion in 2007, (higher revenues than both Las Vegas and Atlantic City combined). The industry's significant revenues, multi-jurisdictions, limited regulatory resources and the growing use of server-based gaming provides a unique and enticing environment for organized crime and large scale criminal activity increasing the need for security controls.

What Information Security Regulations Exist for the Indian Gaming Industry?

There are three levels of regulations that must be adhered to today:

Federal Regulations (NIGC MICS) The NIGC Minimum Internal Controls Standard (MICS) has been in force for more than five years. They were developed from the internal control standards that were suggested in 1995 by the National Indian Gaming Association and the Native American Casino Trade Association. Effective January 1999, the NIGC MICS became the first complete set of regulations covering all areas of native gaming including information and network security.

State "Compact" Regulations Contracts between the state and tribes for "class III operations", operating casinos with slot machines and table games are called "compacts", and each tribe negotiates its own compact with the state. Sometimes the compacts are the same for every tribe in the state, while in other states they can be different for each tribe. Compacts specify what games casinos can offer to their guests and define the rules for those games. They also may denote the hardware and software that must be used in the casino.

Tribal MICS (Minimum Internal Control Standards) Each tribe, or its designated tribal gaming regulatory authority, is required to establish and implement the minimum internal control standards set forth in the Indian Gaming Regulatory Act (IGRA). The tribal requirements must equal the controls stated in the NIGC MICS, but can often be more stringent.

The NIGC regulatory requirements are intended to address the people, processes, equipment and information involved in the gaming industry. There can be different security measures required based on the type of gaming activity and unique audit checklists and worksheets exist for each. These can include but may not be limited to video surveillance audits, physical security for casinos, Cage Audits, Bankroll Verification, Information Technology and others. In addition, disclosure requirements exist in the form of the Department of Treasury's Bank Secrecy Act as well as adherence to the Payment Card Industry (PCI) Data Security Standard (DSS).

What is ISO 27001?

Information is a critical asset to the operation and perhaps even the survival of your organization. ISO 27001 is a standards-based approach for building Information Security Management Systems (ISMS) that was developed, and is supported internationally, by members of the International Organization for Standards (ISO). ISO 27001 evolved from British Standard (BS) 7799 and is intended to provide a framework for managing information security.

Why an ISMS?

Given that the ISO 27001 standard requires ongoing management and enhancement, the P-D-C-A (Plan-Do-Check-Act) must be followed not only for what is in place today, but for future changes as well. This methodology will also ensure that you are in compliance with current NIGC regulatory requirements as well as those that may come in the future.



Achieving Compliance for the Indian Gaming Industry through ISO 27001

How Network Computing Architects Can Help!

NCA is a Pacific Northwest regional consulting firm that has been in business for over 15 years and specializes in providing information security management solutions and services. The primary objective of the NCA's professional services practice is to assist our clients with minimizing the likelihood that threats and risk will exploit vulnerabilities to critical assets. In order to be effective at this task, we have to first analyze, assess and audit the client's Information Security components to ensure that we obtain enough knowledge of their unique environment to act as a trusted advisor. As a trusted advisor, NCA works with our clients to identify their available information security budget and appropriate use of that budget.

NCA's ISO 27001

NCA achieved ISO 27001:2005 certification in December of 2007.

ISO 27001 Associate Consultancy

Since BSI is the certification body for an ISO 27001:2005 certification, they are unable to provide any form of consulting services to clients looking to develop an ISMS and achieve certification. Therefore they have set up a partnership program in which to refer clients to consulting organizations called Associate Consultants. BSI offers Associate Consultancy status to organizations that they believe have a credible and acceptable service in terms of value and performance to consult other organizations in developing an ISMS. NCA achieved ISO 27001:2005 certification in December of 2007. NCA is the first associate consultant in the United States to achieve their own ISO 27001 Certification.



ISO/IEC 27001:2005 Certified
IS 506700



ISO 27001- 012 1207



Comparison Between NIGC MICS and ISO 27001

METHODOLOGY	NIGC MICS AUDIT CHECKLIST FOR INFORMATION TECHNOLOGY	ISO 27001
Intended Use	Audit Guidance for Minimum Requirements	Management Requirements
Assurance Method	Audit Reports	International Certification
Stance	Reactive with a very limited scope	Proactive
Gaming Program Changes	A written plan of implementation for new and modified programs shall be maintained, and shall include, at a minimum, the date the program is to be placed into service, the nature of the change, a description of procedures required in order to bring the new or modified program into service (conversion or input of data, installation procedures, etc.), and an indication of who is to perform all such procedures.	Annex A controls specific to development and security requirements.
IT Personnel Independence	The information technology personnel shall be independent of the gaming areas.	Controls specific to network segmentation and segregation of duties.
General Controls For Gaming Hardware and Software	Management shall take an active role in making sure that physical and logical security measures are implemented, maintained, and adhered to by personnel to prevent unauthorized access that could cause errors or compromise data or processing integrity.	General clauses as well as Annex A controls specific to management responsibilities.
Security Logging	If computer security logs are generated by the system, they shall be reviewed by information technology supervisory personnel for evidence of multiple attempts to log-on, or alternatively, the system shall deny user access after three attempts to log-on.	Controls specific to security monitoring and logging.
Document Storage	Documents may be scanned or directly stored to an unalterable storage medium.	Controls specific to information classification, labeling, handling, storage and destruction.



Network Computing Architects, Inc.

855 106th Ave NE | Bellevue WA 98004 | 877-566-9622

Spokane WA 425-766-6706 | Portland OR 888-968-5434

Los Gatos CA 408-342-9900 | Las Vegas NV 702-457-7990

www.NCAnet.com

COMPLIANCE COMPARISON