IACSP
International Association of Certified Surveillance Professionals

Conducting Surveillance Audits in Gaming Environments

A Best Practice and White Paper

International Association of Certified Surveillance Professionals (IACSP)

A proven method of ensuring proper protocols and regulations are being adhered to, and for detection of theft, fraud, or other illicit activity, is by conducting an audit of a person or function on a periodic basis. The following Best Practice and White Paper is developed for Surveillance Professionals to assist in proven practices within their gaming establishment to perform and detect breaches in policies, procedures, internal controls, regulations or internal/external theft or fraud.

Definitions

Audits – An assigned surveillance observation of an individual, area, department or critical transaction, for a specified period of time, to monitor the adherence of policy, procedures and internal controls, and to detect potential or existing theft, fraud or other illicit activity.

Audit types include the following:

Minimum Level - A routine audit such as a dealer pace audit, guest service, routine transactions, and/or for minor policy/procedure reviews or service requests.

Intermediate Level – An audit of personnel, key or critical areas, departments or transactions for the purposes of detecting internal or external theft or fraud. This audit would include player ratings and points of sale (POS), etc.

Comprehensive Level – A Close Watch initiated on information developed or received involving a serious control or policy violation or of a criminal nature.

Audit Parameters - The operational guidelines for a specific audit described including; what and who is being audited, for how long, the personnel assigned to

perform the audit, chain of command and confidentiality requirements and other resources necessary, etc.

Audit Report – A detailed report of the audit conducted and its finding. Recommendations may be included to correct issues or concerns detected. Report is normally released to department heads, senior executives including the general manager and Human Resources, and others with a need to know to assist in the review and correction of the audit findings, including legal counsel.

Case Log – A log used by surveillance personnel assigned to an audit of significant or suspicious activity and exceptions observed during an audit. The Case log is reviewed by the Case Manager and is used to track the observations made, and will be used to complete the final audit report.

Case Manager – Surveillance person assigned to manage a specific audit to include development or refinement of audit parameters, scheduling and assignment of personnel, and day to day review of audit status and case developments, including retention of video. Reports to senior surveillance personnel.

Close Watch – A continuous observation of a person, place, or thing conducted based on information developed or received. A Close Watch continues until the subject is proven innocent or guilty, not involved, or is otherwise removed from suspicion or concern. Close Watches are normally reserved for issues or concerns of a serious nature.

Critical Transaction – A transaction that occurs in gaming or non-gaming areas or departments involving company revenue, funds or assets such as jackpots, table fills or credits, retail sales, etc.

Gaming Control Board (GCB) also called by various names including gambling control board, gambling board, and gaming commission) – A government agency charged with regulating casino and other types of gaming in a defined area, usually a state, and of enforcing gaming law in general.

Tribal Gaming Agency - A regulatory agency that works on behalf of various tribes of Indians. The agency is responsible for Inspecting, examining and monitoring all gaming activities and the gaming entity.

Audit Purpose

Surveillance departments perform audits for three reasons:

1. At the behest of management to monitor and report game speed, evaluate dealers, guest service, employee job performance, check player ratings for accuracy, new game analysis, etc.
2. At the direction of surveillance management to detect violation of policy or procedure, criminal activity, problem gambling, suspicious activity, or other issues affecting profitability of the property.
3. Received information or business intelligence such as statistical or transactional.

Audits are assigned and performed to allow focused attention on a specific individual, area, activity, certain critical transactions or a department. Intensive surveillance attention provides a thorough observation and review of what is actually being done by an individual, employees of a department, or an operation, as opposed to the policy/procedure presented by department personnel or financial data.

Surveillance video redefines the people, policies and procedures, and controls, including financial, put in place to provide protection and detection ability. Audits also identify where employees and supervisors create shortcuts or *workarounds* which weaken established policies and procedures. Audits can ensure that minimum internal control standards, federal and state gaming regulations are being adhered to, to avoid possible negative repercussions and/or fines.

Audits can be an effective tool for Surveillance to aid in its mission of protecting the property and assets.

Types of Audits

There are a number of audit types: dealer pace audits/evaluation, table game ratings, transactional, policy/procedure, employee performance, guest service, etc.

Audits should remain confidential and within the Surveillance Department until completed and then the results will only be distributed by the Surveillance Manager or Director who may distribute audit results to executives, and/or in a limited format to affected operational departments.

There are also escalating levels of audits:

Minimum Level Audits:

At a minimal level, Surveillance would see most, if not all of the above. These types of audits are usually conducted at the request of a department head such as Gaming Operations, Human Resources, or Senior Management. They are performed as a routine service by Surveillance e.g. pace audits and other time/motion studies. Information and results can be discussed freely at this level within the Surveillance Department, and audit assignments are broad. Participants in audits at this level are encouraged to explore the subject on a large scope and cast a wide net.

(ex. A case manager is assigned to conduct a routine audit on the Food and Beverage department. The manager chooses one agent on each shift to participate and assigns them each a number of venues to audit. Results are logged based on the case manager's requirements and passed between the agents from shift to shift within the department. This is a Minimum Level Audit.)

Intermediate Level Audits:

At the next level we conduct audits of personnel, departments, key areas and critical transactions to detect internal and external theft and fraud in both gaming and non-gaming areas. Examples of these types of audits are the observation of Table Games player ratings, Slot jackpots, Points of Sales (POS) in food and beverage venues, bartenders and cocktail servers, Players Club, and Cage/count room(s), etc. Information and results are generally more restricted at this level and may be kept to the surveillance team themselves or others based on a "need to know" basis. Audit assignments become more specific to a location or topic as the scope becomes more limited. The case manager may adjust requirements or specifications to achieve the desired results.

(Ex. cont. One of the agents notices that not all guests receive their receipts from a certain bar in the casino. The agent informs the case manager, who then instructs each shift to focus on this bar and find out why some guests aren't being given receipts. The case manager adjusts audit requirements to include the names of each bartender and server working at this bar, and when their shifts end and start. This is now an Intermediate Level Audit.)

Comprehensive Level Audits:

At the highest level is a Close Watch. This is an observation of a person, place, or thing, usually performed based on received or developed information or intelligence. This observation may continue for an extended period of time or until a final determination such as innocence or guilt can be made. Information and results are highly restricted at this level to maintain confidentiality. The audit may focus more on specific suspects or crimes and may contain sensitive topics or incriminating evidence. The audit requirements or parameters may be narrowed down to solely encompass a specific person, if necessary.

(Ex cont. The audit shows that one bartender has been charging guests full price for high end beer but ringing it up as cheaper beer and pocketing the difference. The guests are not issued receipts in an attempt to cover the bartender's tracks. The case manager now places the bartender on a close watch and all of his transactions are watched. A review is conducted of his past transactions as well in an attempt to determine how much money has been stolen. The tone of the audit shifts now into a criminal investigation. Evidence is gathered for charges against the bartender. This has now progressed to a Comprehensive Level Audit.)

Time and Resources

Because every operation is different in gaming environments, the type and scope of an audit is commensurate to the available surveillance personnel without detracting from normal day to day operations.

Audits can range in time required from six or ten minutes for a decisions per hour check to between eight to seventy-two hours or more for an audit of a department or key area. A close watch may continue for a longer period if required, depending on the severity of the concern.

In most operations, audits are performed by one agent. This agent is normally replaced with another agent for breaks and lunch periods. Very sensitive audits should be solely conducted and completed by one agent if possible, to keep the audit consistent.

The case manager, supervisor or manager should monitor for any criminal activity detected during an audit and communicate with the appropriate gaming authority or law enforcement entity. In some cases, those agencies may be allowed to participate in the audit process where criminal activity is detected. In those instances, the audit is converted to an investigation.

Audits can be managed by the agent and his/her supervisor, the surveillance manager or director, or a case manager specifically assigned to manage the operation of the audit.

Audit Parameters

All information concerning the subject of the audit should be provided to the personnel assigned. This includes, but is not limited to, operating procedures, regulations, Minimum Internal Control Standards (MICS), employee schedules, or any other relevant data. Most importantly, the objective of the audit should be clearly stated, communicated and adhered to. Nothing should ever be relayed to anyone outside of the needed management.

Reporting

When completed, a written report should be generated. An audit report should be comprehensive, and any video and/or breakdown related worksheet(s) evidence should be retained and referenced in the report. A video review log should be attached to the audit to identify cameras, locations and related information.

Creating audit forms to use where the objectives are identified and observation results can be quickly noted, and where data can be quantified for audits that are recurring on a regular or scheduled basis can be helpful. Fundamentally, the forms need to identify the who, what, where, when, how and why of the audit. Forms are helpful for quick review to determine if the desired data is being collected and can be used as backup data for the report.

Forms for MICS are helpful for the drop and count functions and any function where internal controls are part of the audit process including those forms used by a Tribal State Compact, Tribal Gaming Agency or other regulatory authority.

Forms will ensure consistency in reporting from surveillance personnel on similar audits so they can be easily understood when reviewed by management.

Final results of audits are typically reviewed by surveillance management and then communicated to appropriate senior executives for review and handling.

The case manager should read the reports for correctness, completeness, conciseness, and clarity to see that the objectives were met in the audit. The manager should make sure all photos are labeled correctly and they identify the person, object, location or activity correctly. All video should be reviewed to ensure that procedure violations or activity that are identified in the report are clearly observed on the video by the timelines indicated in the report and that employees and subjects are identified correctly. Any contributions, entries, or logs pertaining to the audit should be checked at least daily by the case manager to ensure requirements and objectives are being met. Deviations or incomplete data should be identified and rectified at the earliest point possible to prevent the waste of time and resources or false reporting.

Successful audits can result in changes in operations, discipline or termination of employees and managers, and/or arrest of those involved if the theft or fraud is detected.

When an audit results in changes to policy, procedures, or controls, a follow up audit should be conducted after they are implemented within the subject department. This will allow surveillance to determine if the department has, in fact, implemented the new requirements and whether they are working as planned. Changes can be made at this time if necessary. Additionally, surveillance may be able to determine the value they've added back to a department due to the audit performed such as increased hands per hour, reduction of loss in Food and Beverage, or game pricing. When value can be calculated this should be included in surveillance quarterly or annual report to senior executives to demonstrate the added value surveillance can bring to the operation.

Original Authors:

Derk J Boss, CFE, CPP, CSP – President of IACSP; Director of Surveillance, Angel of the Winds Casino Resort
Alan W Zajic, CPP, CSP, ICPS – IACSP Director of Programs; Casino/Hotel Security Consultant, AWZ Consulting
Jen Boss, CSP – IACSP Director of Education; Chief Operations Officer, DJ Boss Assoc

Additional IACSP Board of Directors Contributors:

Ron Buono, CSP – IACSP Board of Directors Member; Executive Director of Surveillance, MGM Grand
Randy Boynton, CSP – IACSP Director of Certification & Training; Surveillance Director (Retired)
Ron Flores, CSP - IACSP Board of Directors Member; Commissioner, Pechanga Gaming Commission

Additional Contributors:

Kevin Cheesman, CSP – Director of Surveillance, Grand Casinos
Michael Kelley, CSP – Surveillance Shift Manager, Angel of the Winds Casino Resort
Jason Boss, CSP – Tribal Gaming Agency Enforcement Surveillance Agent, Ilani Casino Resort
Jesse Silva – Director of Surveillance, Valley Forge Casino Resort
Anthony DiSalvatore, CPP, PSP, PCI, CFE, CLSD – Front Office Manager, Radisson RED; Security/Surveillance Director (Retired)

Document Revision History

Completed by original authors on July 13, 2019.

Sent out to the International Association of Certified Surveillance Professionals (IACSP) Board of Directors on July 15, 2019.

Returned from Board of Directors on August 29, 2019.

Final edits and formatting sent to IACSP membership and selected industry professionals on August 30, 2019.

Returned from IACSP membership and selected industry professionals on February 16, 2020.

Published on April 02, 2020.

IACSP
International Association of Certified Surveillance Professionals

Founded in 2001, the International Association of Certified Surveillance Professionals (IACSP) is a growing organization established by your peers and colleagues throughout the industry to develop and provide training to prepare surveillance personnel for the future. Our mission is to train existing and future surveillance agents in the core skills of their profession and also to develop the next generation of surveillance agents, supervisors, managers and directors. As you know, surveillance departments are continuously being challenged to protect our properties more effectively. The need for highly trained personnel has never been greater. The IACSP addressed this issue through training; a certification program developed by surveillance directors. For more information, to contact an IACSP member, or to become a member of the association, visit www.iacsp.org.