Global Information Assurance Certification Paper

Implementing ISO/IEC 17799 Within a Fictitious Gaming Casino

By Larry Sobers

GIAC Certified ISO-17799 Specialist (G7799) Practical
Version 1.0 – February 2005

table of contents

1. Mission statement and business objectives

Mission Statement

It is the sole mission of Viva Casinos to provide its customers with an entertaining gaming experience. By delivering world-class entertainment, accommodations and gaming, Viva Casinos plans to increase profitability through its customer base (new and returning), establish new revenue via emerging technologies and establish its name brand as the foremost gaming and hospitality company in the industry.

Organization Objectives

- Provide world class accommodations, entertainment and gaming by delivering quality products and first rate customer service
- Increase profitability via customer loyalty and emerging technologies
- Increase existing revenue streams by offering quality products

.

2. high level security principles

Security Principles

Viva Casinos provides a secure environment for its customers and employees by adhering to all applicable state and federal regulations:

- Regulatory Compliance
  - Nevada Gaming Board
  - Sarbanes-Oxley, GLBA, HIPAA, etc

It is Viva Casinos' goal to protect the confidentiality, integrity and availability of all the information assets utilized to provide the entertainment experience.

- Demonstrate due diligence by implementing necessary controls (physical, administrative and technical)
- Protect the privacy of our customer's and employee's PII and PHI

In addition, all Viva Casinos' employees are required to submit to an exhaustive background investigation prior to employment to ensure the integrity of our customer's gaming experience.

3. maturity model for an issue

SECURITY PRINCIPLE #2

Viva Casinos provides a secure environment for its customers and employees by adhering to all applicable state and federal regulation.

Level 1 (Year 1)

- Perform gap analysis on existing controls and their ability to meet regulatory compliance of applicable state and federal regulations

- Based on gap analysis findings, initiate project with CEO-level commitment to provide

guidance on necessary remediation work for all information technologies and assets used to enable the business processes of Viva Casinos.

Level 2 (Year 2)

- Develop regulatory compliance forum comprised of applicable departments (Security, Legal, HR, etc) and CEO.
- Regulatory compliance forum should provide guidance and interpretation of all existing and new laws at the local, state and federal level.

Level 3 (Year 3)

- Improve regulatory compliance forum by adopting an internationally accepted Information Security Standard (ISO17799 or SANS 4S).
- Information Security Standard will provide a holistic lifecycle of continuous improvement that will maintain regulatory compliance and reduce audit findings, thus enhancing the security posture of the business.

4. Addressing objections in awareness

Issue #1

- In year 1, the gap analysis may indicate certain issues that may have been overlooked or swept under the rug.
    - These issues may be in direct non-adherence to industry-specific statutes and regulations of the Nevada Gaming Commission.
    - The issues may also run up against the "we've always done it this way" mentality.

Security Awareness

- As part of the gap analysis, Security Awareness is targeted as a vehicle for the improvement of the immediate problems of regulatory compliance.
    - Of immediate concern to the business is full compliance with all statutes and regulation of the Nevada Gaming Commission.
        - All employees are required to attend annual job-specific training on the statutes and regulations of the Nevada Gaming Commission
            - This requirement is a requirement of each employee's annual performance assessment
        - A representative from the Nevada Gaming Commission and/or in-house Legal specialist attends and passes out small handbooks covering the statutes and regulations and contact information for questions.
        - *The representative tells a story regarding another casino that did not train the employees on the statutes and regulations. Several of the employees unknowingly broke many of the regulations. The Nevada Gaming Commission was forced to temporarily shut down the casino and fine the owners hundreds of thousands of dollars in fines. The casino never recovered and was forced to file bankruptcy.*
    - The business couples the employee training with the appropriate security controls to meet regulatory compliance of the Nevada Gaming Commission's statutes and

regulations. Any notifications are sent for re-training on the first abuse. Repeat offenders are terminated.

- *How will it solve the issue? Why will it work?*
  - The training will help to keep honest people honest and the security controls will show due care and due diligence and make it more difficult for malicious intent to be carried out.

Issue #2

- In year 2, the creation of the Regulatory Compliance Forum may not be met with open arms.
  - The creation of the forum may not be communicated effectively to the business and its intent and importance may be overlooked
  - Participation from certain business units may be met with resistance, due to the forum being viewed as an additional layer of bureaucracy.

Security Awareness

- To continue the success of the Security Awareness program, the formation of the Regulatory Compliance Forum is communicated to the business via email, intraweb and internal newsletter.
  - The communication of the forum is sent out from the CEO via the channels described above with the guidance that all matters of regulatory compliance are to be funneled through the forum.
  - In the communication, parties acting independently of the forum on matters of regulatory compliance will be held accountable and could result in immediate dismissal.
  - The annual regulatory compliance training and handbooks are updated to reference the forum on matters of regulatory compliance.
  - *A story is told referring to another company that did not have a formal forum for discussing and interpreting regulatory compliance. The company misinterpreted the legal issues surrounding SB1386 and did not comply in the correct manner. The company did business with several California residents and was later hacked. Because they did not interpret SB1386 correctly, they thought that it only applied to companies in the state of California and did not contact any of the California residents regarding the unauthorized disclosure of the PII. The company was later investigated due to the lack of due care in regards to their compliance.*
  - *How will it solve the issue? Why will it work?*
    - The effective communication of the intent and importance of the forum will notify the business of the forum's existence and purpose.
    - The annual training will keep it fresh in the minds of the employees.
    - The signoff by the CEO will keep all business units in check in regards to attempting to circumvent the process.

Issue #3

- In year 3, the continuous improvement process being introduced by the ISMS brings a consistent method to measure overall risk in the business. It is overwhelming and introduces more work to each business unit.

Security Awareness

- In addition to annual Regulatory Compliance training, the CEO gives commitment to have the business attend Security training.
    - In the training, security is sold as everyone's job and its importance is explained to everyone.
    - The training is given to all employees and to new employees during Orientation.
        - The training is complemented by 30 minute refresher CBTs on specific topics as necessary.
    - *A story is told regarding a company that did not invest in security or security training. The company's employees unknowingly divulged confidential acquisition information, which was leaked out to the Internet driving up the price of the potential purchase company's stock. Due to the new cost, the acquisition fell through costing several new jobs. During this time, an audit was being performed and several key findings regarding the irresponsible disposal of company sensitive information to the theft of company property. The findings coupled with the acquisition failure resulted in poor stock performance for a few years for the company, which cost millions in profitability*
    - *How will it solve the issue? Why will it work?*
        - If the concept of "security being everyone's job" can successfully be taught to the business, a heightened sense of awareness in regards to security will permeate through the enterprise.
        - Security-related work will be met with less resistance
        - The concept of "security being everybody's job" is now linked to the success and profitability of the company.

5. business continuity planning

Non-compliance

The Regulatory Compliance Forum has been meeting for several months and has discussed different topics ranging from criminal/civil law to contractual language. They have provided guidance to the business regarding issues of regulatory compliance.

During this period, Viva Casinos experiences a surge in profitability and acquires Big Hot Casinos. As a part of the acquisition, several functions are eliminated due to position redundancy. One of the last systems administrators at Big Hot Casinos becomes disgruntled when he realizes that he will be laid off in a week. During the acquisition, he was given root privileges on Viva Casinos' systems to assist with the merging of systems. The system administrator sabotages several key systems and posts business-sensitive information (customer and employee PII, future potential merger and acquisition information, salary information, etc) to the Internet. In addition, he defaces the website with pornographic pictures and expletives.

The administrator is arrested and evidence is collected via Viva Casinos' Incident Handling policy to facilitate prosecution of the system administrator. The systems and the website are restored. A formal message is issued to the public apologizing for the incident. The business-sensitive information is removed from the public repositories that it was posted to and the FBI is currently investigating any leads regarding information access, while the information was available.

The only issue left is the executing of the portion of the Business Continuity Plan regarding the potential non-compliance of any state or federal laws that might have been broken due to the unauthorized disclosure of the business-sensitive information.

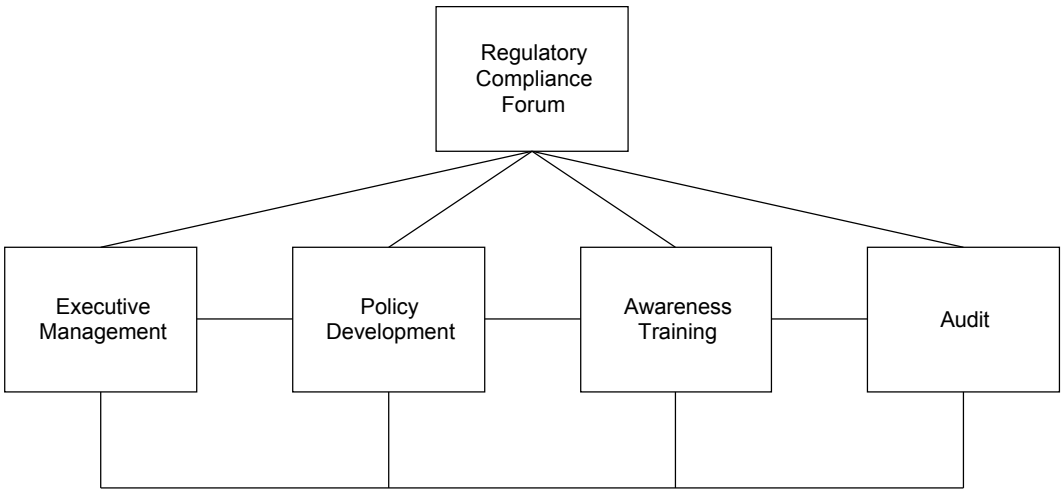
Plan

- Once core business functions have been restored, the Regulatory Compliance Forum reviews the incident.
- All instances of malicious behavior are mapped to applicable laws and regulations that may have been broken.
- The Regulatory Compliance Forum leverages the relationships that have been formed with the different regulatory bodies (i.e. Nevada Gaming Commission, Governor's Office, State Senator's Office, District Attorney, etc.) to confirm the company's liability and plan of action.
- The Regulatory Compliance Forum offers the gap analysis and remediation effort as "due care" to show that Viva Casinos has done all it could do to prohibit this type of incident.
- The Regulatory Compliance Forum present the findings to Executive Management and offer strategies to bring Viva Casinos back into compliance of any applicable laws.

6. Risk assessment and recommendations

Utilizing the FMECA (Failure, Mode, Effects, and Criticality Analysis) technique, an internal risk analysis was performed on the process used to develop the Regulatory Compliance Forum.

The Regulatory Compliance Forum's mission is to monitor and interpret any new or modified laws, statutes, and/ or regulation at the local, state and federal level. The Regulatory Compliance Forum is defined below as a system with dependencies on other business functions:



The common failure for all modules that interface with the Regulatory Compliance Forum was a breakdown in communication between any of the entities. The communication issues ranged from Minor to Catastrophic:

- Category IV – Minor
  - Audit incorrect reports audit findings
- Category III – Marginal
  - Awareness Training has no or incorrect interpretation of regulatory compliance
- Category II – Critical
  - Policy does not exist or is not updated to reflect regulatory compliance
- Category I – Catastrophic
  - Executives don't give commitment and signoff to Regulatory Compliance Forum

Each of the risks described above are easily mitigated by detective or preventative controls:

- Category II – IV
  - Preventative Control: Review documentation
  - Detective Control: Participation in Regulatory Compliance Forum
- Category I
  - Preventative Control: Executive Commitment and Signoff
  - Detective Control: Participation in Regulatory Compliance Forum

However, while these controls would mitigate the problems found in the assessment, the new controls introduce new consequences to the Regulatory Compliance Forum process. These consequences are:

- With the addition of new members, a longer time may be required to reach consensus among all of the members of the forum.
- Placing additional review around regulatory compliance documents (policy, awareness training, etc) may cause a bottleneck and delay the deliverable.