Global Information Assurance Certification Paper

Viva Casinos

Mission Statement and Objectives

Objectives

- Make money
- Increase profits
- Provide safe and secure gaming experience
- Maintain high levels of customer satisfaction
- Entertain, Entertain, Entertain
- Comply with industry regulations
- Innovate business

Mission Statement

Provide an exciting and secure gaming experience for our customers, continuously increasing profit and expanding the business through innovation and superior customer service, while exhibiting compliance with the law and industry regulations.

ISMS Mission Statement

Effectively protect the business' ability to provide services to our customers and contribute profoundly to the assurance of the continuity and integrity of business operations through industry best-practices controls that allow for the effective management of IT security risks.

Guiding high level principles

1. Information is an important asset and it needs to be protected according to its sensitivity and criticality
2. Access to systems and information within Viva Casinos must be restricted to authorized personnel with a legitimate business need for such access.
3. Adequate security controls must be implemented and maintained to ensure that only authorized individuals and processes have access to Viva Casinos' information assets.
4. Authority for the enforcement of company wide information security policies remains within the Information Security department.
5. Issue specific policies, procedures, standards and guidelines must be created and maintained to support these high-level security principles.
6. Information Security, in conjunction with Internal Audit department, must also periodically verify compliance with information security policies and any laws and regulations regarding the protection of information resources. Appropriate measures must be taken to ensure risk is identified, measured and mitigated appropriately.

Maturity Model

Principle 1

Information is an important asset and it needs to be protected according to its sensitivity and criticality

Level 1

- An inventory of information assets is built
- Assets are assigned owners or "Trustees", who are responsible for ensuring asset is protected, which includes classifying and authorizing access to the information asset.
- Assets are classified according to their sensitivity (Impact to the organization should they be improperly disclosed), using four sensitivity labels: Public, Proprietary, Restricted and Highly Restricted.
- Assets are classified according to their criticality (Impact to the organization should they be made unavailable), using three criticality labels: Non-critical, Critical, Highly Critical
- Specific handling criteria is developed for each sensitivity and criticality level, for each of the following activities:

    1. Labeling/Marking
    2. Storage
    3. Communication
    4. Transmission
    5. Elimination/Deletion

- Assets are marked with their corresponding labels of confidentiality and criticality

- Policy and handling criteria is published and personnel is made aware of their responsibilities regarding the protection of classified information

Level 2

- Employees required to sign confidentiality agreements

- Third party access contracts updated to reflect information handling requirements

- Safe disposal mechanisms are provided (paper shredders, disk wipe utilities, Etc.)

- Cryptographic controls are implemented to safeguard information in storage or transit.

Level 3

- Regular audits performed to check for policy compliance
- Intrusion detection tools are used to verify compliance with policy
- Third parties audited by independent organization on compliance with the policy

Principle 2

Access to systems and information within Viva Casinos must be restricted to authorized personnel with a legitimate business need for such access.

Level 1

- Access administration for all "Critical", "Highly Critical", "Restricted" and "Highly Restricted" information assets is centralized within Information Security department.
- Segregation of duties is performed so that only security personnel can handle security related functions.
- Authentication is required prior to granting access to critical and sensitive information assets.

Level 2

- Access profiles are built based on "need-to-know" of job description. Access is granted based on these authorizations.
- Notifications are sent to Information Security upon employees leaving the company (from HR system)
- User tables are periodically audited to verify that there are no unnecessary user accounts

Level 3

- Strong authentication is required to access "Highly Critical" and "Highly Restricted" information assets
- Any employee movement (Entry, change of position or exit) is automatically notified to Information Security and access is revoked or modified accordingly in a timely manner.

- Intrusion detection tools monitor for unauthorized access attempts in real-time.
- User tables are audited periodically for unnecessary accounts or excessive privileges.
- Security standards for new systems developed to ensure proper access controls are included prior to running in production environment.

Issues likely to be misunderstood

1. Sysadmins or DBAs being revoked access to security related functions

What	Why and how solution will work
Awareness sessions to IT operations group Key items: 1. Explain segregation of duties principle and its benefits. Not only how it helps to protect the business but also the user from unnecessary liability. 2. Present real life examples of the risks of not having segregation of duties, from the business perspective (process compromised by one individual), and the employee perspective (employee being held fully accountable for any incident involving his/her access rights) 3. Present regulatory requirements that must be met by the organization and explain how the control helps meet those requirements. 4. Disassociate trust with control. Make emphasis on the fact that trust has nothing to do with it. "If it were for lack of trust, you wouldn't be working here"	This approach helps the employee appreciate the value of applying this principle and how it pertains to them. Real-life examples help to understand this rather abstract concept. When employees understand that trust (or lack there of) is not the motive of control, they become more willing to cooperate with the enforcement of control.

2. User activity being monitored

What	Why and how solution will work
Include the following items in all awareness material used to train users about information security: 1. Detail the benefits of detective controls. Present real life examples of how detective controls help identify unauthorized access attempts and system compromise. 2. Present regulatory and legal requirements for handling evidence in the corporation. 3. Explain possible consequences of failing to register user activity (Incidents not properly handled, impaired investigations) 4. Present regulatory and legal requirements that must be met by the organization and explain how the control helps meet those requirements 5. Disassociate trust with control.	By making users aware of the reasons why control needs to exist and seeking to make them agree to it, we have a better chance they support it. When users understand that trust (or lack there of) is not the motive of control, they become more willing to cooperate with the enforcement of control.

3. Users being required to sign confidentiality agreements

What	Why and how solution will work

Include the following items in all awareness material used to train users about information security. Also, include this material in an "induction" briefing (when employees enter the organization): 1. Reasons why company needs to protect its information resources. Importance of information and how it relates to the mission of the organization. 2. Present regulatory and legal requirements and how they relate to this control 3. Disassociate trust with control.	By making users aware of the reasons why control needs to exist and seeking to make them agree to it, we have a better chance they support it. When users understand that trust (or lack there of) is not the motive of control, they become more willing to cooperate with the enforcement of control.

Business Continuity Planning

What could go wrong?	Impact	BCP

Malware attack - Servers and workstations infected with virus/worm	Network availability affected System downtime Data corruption Lost business Affected customer service Affected company image and customer confidence Loss of productivity Recovery costs	Plan phase - Assemble team (CIRT team) - Establish scope of plan - Assign roles and responsibilities - Define thresholds and incident classification criteria: Example: Low severity Detection of a reduced number of systems (ie. <1% of network devices) scanning the network or exhibiting virus/worm like behavior Medium Severity Detection of a slightly significant number of systems (ie. <5% of network devices) scanning the network or exhibiting virus/worm like behavior High Severity Detection of a significant number of systems (ie. 5% or more) scanning the network or exhibiting virus/worm like behavior Do phase - Build incident handling procedures: 1. Classification of incident according to pre-defined criteria 2. Declaration of incident (Communication to management) 3. Communicate incident to all users within the organization and instruct on first level response (turn off computer, disconnect network cable, report to help desk, CIRT) 4. Mitigate/respond to incident: a) Isolate and contain threat using router ACLs, firewall rules or IPS. b) Eradicate threat using appropriate tools and techniques

Risk Assessment

Malware Attack

Controls:

Preventative

1. Virus screening firewall on network perimeter
2. Anti-virus software on PCs and Servers
3. User awareness on how to prevent virus infections

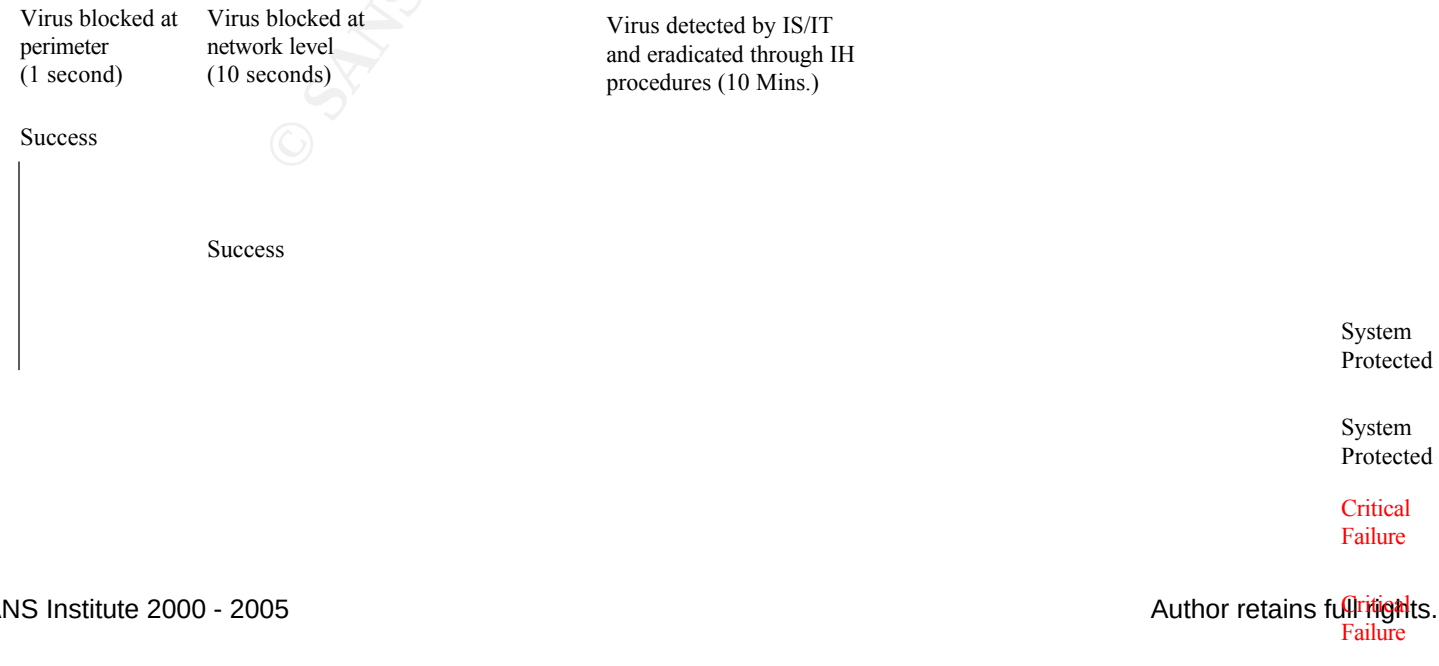
Detective

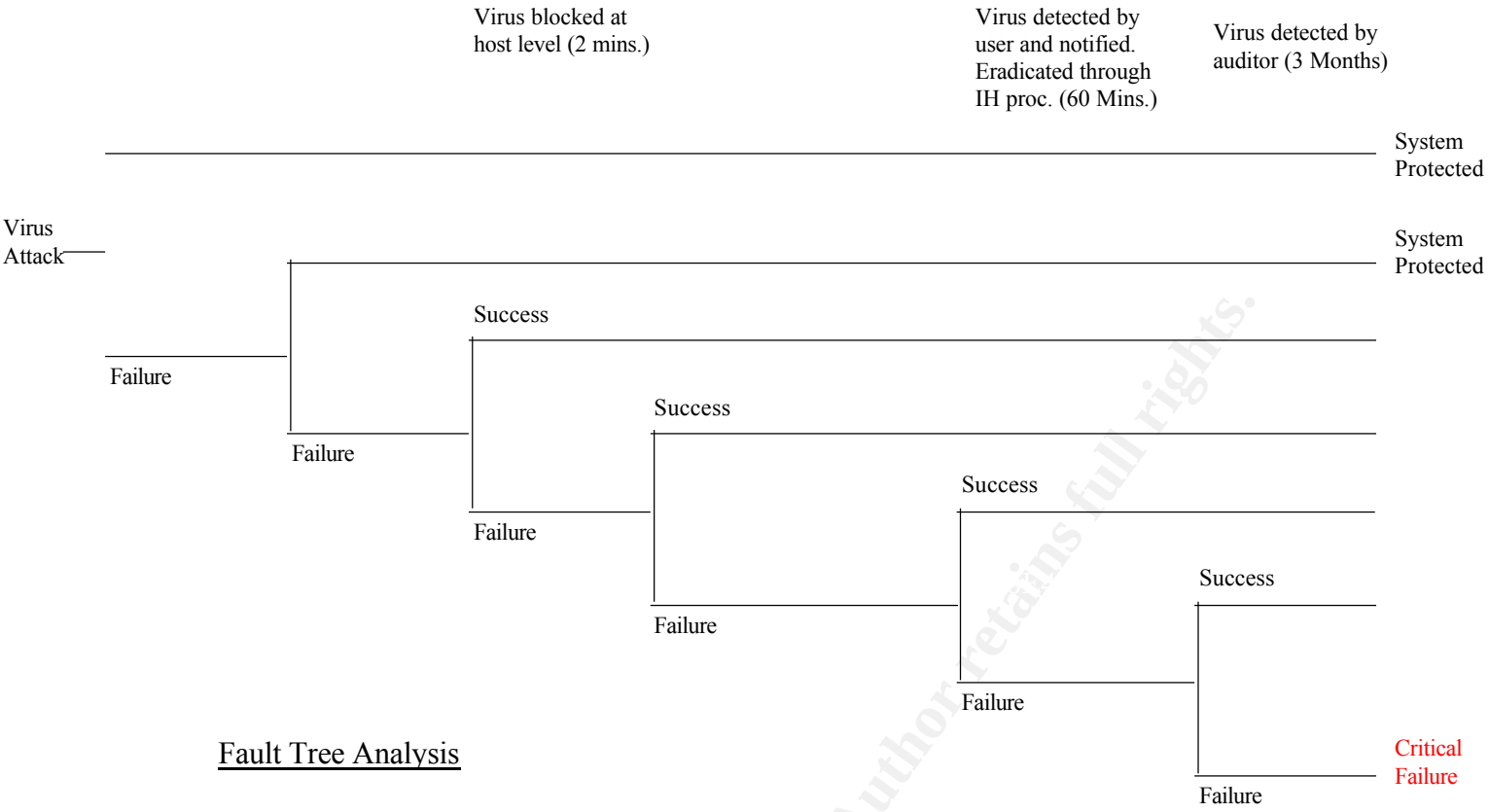
1. Virus detection on network perimeter
2. Anti-virus software alerts PCs and Servers
3. Firewall logs
4. End users diagnosis
5. Auditors

Reactive/Response

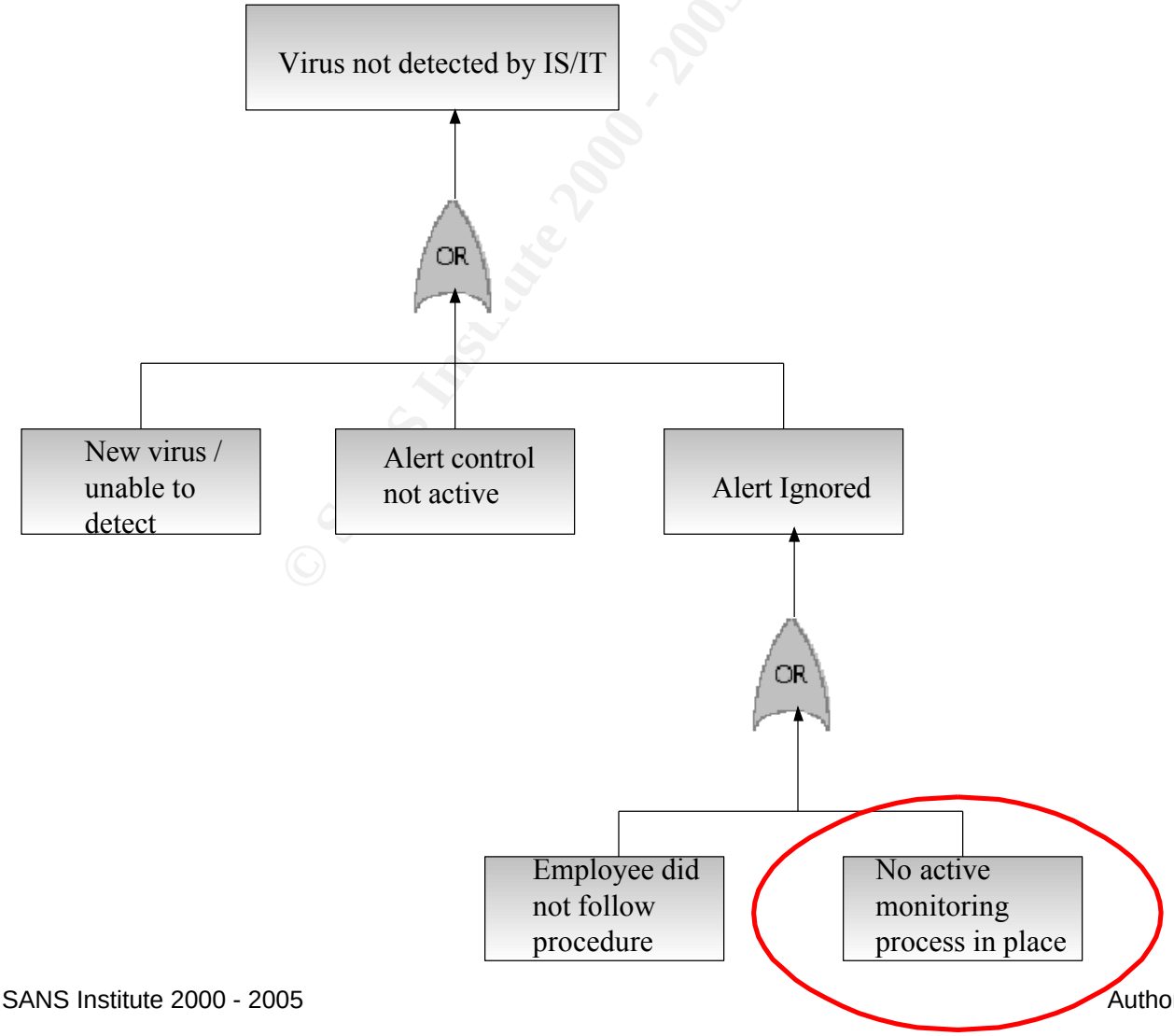
1. Business continuity plan
2. Incident handling procedure
3. CIRT team

Event tree analysis





Fault Tree Analysis



Root Cause

Countermeasures

Control	Level 1 (Fair)	Level 2 (Desirable)	Level 3 (Best)
Preventive	-Router ACLs -Mail gateway rules -System Patches -AV Updates	Level 1 Controls + -Automated patch management	Level 1 and 2 Controls + -Intrusion Prevention Systems -Heuristics
Detective	-Aggregate alert information in central server -Periodically review AV system events -Periodically review firewall logs for patterns of attack	Level 1 Controls + -Establish real time AV system alert monitoring process -Deploy network and host based intrusion detection systems	Level 1 and 2 Controls + -Active Monitoring of Intrusion Detection Systems -Honeypots

Reactive	- Incident handling procedures triggered by administrator reviewing AV events -Help Desk support -Tech support response - Build Computer Incident Response Team (CIRT)	Level 1 Controls + - Update incident response procedures to trigger upon real time alert - Update incident response target/SLA -CIRT team response	Level 1 and 2 Controls + - Dynamic ACLs and firewall rules