2008-01-18 12:42:00

G007_CHANGE_AND_CONFIGURATION_MANAGEMENT

Change & configuration management

Guidelines

1. Preliminary

1.1 Authority

This document is issued by the Financial Services Regulatory Commission (the Commission) pursuant to r 105(g) of the Antigua & Barbuda Interactive Gaming and Interactive Wagering Regulations.

1.2 Confidentiality

This document, all related documents, and methodologies embodied in this document and related documents ("*the documents*") are the property of the Financial Services Regulatory Commission. Unauthorised copying and distribution of *the documents*, by any means, on any media is prohibited.

This document, its themes, and ideas are strictly confidential and may not be used in any manner other than its expressed purpose, without the written permission of the author. The documents are authorised for use by licence holders.

The documents are copyright.

1.3 Disclaimer

The guidelines provided in this document are current at the time of writing. The Commission may in its absolute discretion amend these guidelines, or any definitions or interpretations pursuant to this or related documents at anytime.

Each licence holder should ensure it has the current version of each document.

1.4 Queries

All queries relating to this document should be made, in writing, to:

Director of Gaming
Financial Services Regulatory Commission
First Caribbean Financial Centre
Old Parham Road
St John's
Antigua and Barbuda

e-mail : director@antiguagaming.gov.ag

A.1 References & related documents

The Financial Services Regulatory Commission utilised many documents and international standards when compiling the suite of guidelines.

The current list of related guidelines is available from the Commission's website at http://www.antiguagaming.gov.ag.

Licence holders and other interested parties should acquaint themselves with the contemporary documents before relying on them.

1.5 Table of contents

2. Guidelines

2.1 Preliminary

2.1.1 Introduction

The licence holder shall document and implementing change and configuration management processes. These processes shall be a component of the approved control systems.

2.1.2 Objectives

The objective of change management process is to ensure that all changes are assessed, approved, implemented, and reviewed in a controlled manner. All software and infrastructure changes should have a clearly defined and documented scope.

2.1.3 Scope

The change management system should incorporate:

a. policies;

b. procedures;

c. control systems – changes to the control systems must be approved by the Commission;

d. software systems; and

e. hardware systems

NOTE: Software and hardware are components of the control systems and may also be components of gaming equipment.

2.2 Configuration and change management

2.2.1 Asset identification and management

REGULATORY OBJECTIVE

Licence holders shall effectively manage all assets which have an affect on the business security or compliance.

2.2.1.1 Identification of assets – configuration items (CI)

1. Licence holders will identify all software, hardware, and firmware (including rules) assets which may affect the security or compliance of the information systems and gaming equipment.
2. Each asset, and its version, shall be uniquely identified. Each such identified asset is referred to as a “configuration item” (CI).

2.2.1.2 Configuration item (CI) risk management plan

1. The importance of each CI in achieving, or maintaining security and/or compliance shall be rated in accordance with the licence holder’s risk management policies and procedures. That is if the CI was

compromised and failed to meet its security and/or compliance obligations what would the likely "impact" be on the licence holder's security and/or compliance.

2. There shall be a configuration item plan which lists all software, equipment, and system configuration item. The plan shall uniquely identify the CI, its version and release date.

3. The likelihood of each CI affecting the licence holder's security and/ort compliance during modification, upgrading or bug fixing should be rated in accordance with the licence holder's information security policies and procedures.

4. Controls should be commensurate with the relevant risk of any amendments to any CI affecting the security or compliance of the licence holder's systems.

5. The configuration item risk management plan shall be reviewed with each change request and change. The configuration item risk management plan shall be included with Release Notes, and provided to the Director of Gaming.

6. All configuration items should be uniquely identifiable and recorded in a configuration management database (CMDB) to which update access should be strictly controlled. The CMDB should be actively managed and verified to ensure its reliability and accuracy. The status of configuration items, their versions, location, related changes and problems and associated documentation should be visible to those who require it.

2.2.1.3 Internal configuration item audits

1. Internal configuration audit procedures should exist and should include recording deficiencies, initiating corrective actions and reporting on the outcome.

2.2.2 Formal policies and procedures

REGULATORY OBJECTIVE

Licence holders shall maintain security and compliance of application software and information.

2.2.2.1 Change control procedures

1. The implementation of changes shall be controlled by the use of formal change control procedures.

2. Change management procedures shall ensure integration with the inventory of assets (see *G005 Administrative systems, policies, and procedures*).

3. All entries to the change control procedures design, change request, or problem reports shall be logged and the log maintained.

4. All changes shall be prioritised from design through to deployment and included in release notes.

5. Licence holders shall ensure that change and configuration of design, development, testing, and deployment of software, equipment, and systems is administered by appropriate automated techniques.

2.2.2.2 Technical review of applications after operating system changes

1. When operating systems are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on the organisation, security, or compliance.

2.2.2.3 Restrictions on changes to software packages

1. Modifications to software packages shall be discouraged, limited to necessary changes.
2. All changes shall be strictly controlled.
3. Potential changes shall be assessed for the risk of adversely affecting the system security and compliance before approval.
4. Changes shall be tested for the impact of system security and compliance before release to a production system.

2.2.2.4 Accountability and traceability

1. Each phase of the change and configuration management guidelines shall ensure that all changes are accountable and traceable.

2.2.2.5 Outsourced software development

1. Outsourced software development shall be supervised and monitored by the licence holder.
2. Where software, equipment, or systems are out-sourced to a third party provider then the licence holder shall satisfy itself that the relevant policies, controls, and procedures are equivalent to those outlined in these guidelines. This includes where operations such as "white labelled" servers are utilised.

2.2.3 Technical vulnerability management

REGULATORY OBJECTIVE

Licence holders shall reduce risks resulting from exploitation of published technical vulnerabilities.

2.2.3.1 Control of technical vulnerabilities

1. Timely information about technical vulnerabilities of information systems being used shall be obtained, the licence holder's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk(s).

2.2.3.2 Change requests

1. The licence holder shall have a formal method for personnel to make change requests.
2. Change requests shall be an entry to the change control procedures.

2.2.3.3 Problem reports

1. The licence holder shall have a means for all stakeholders (staff, contracts, management, customers, and Commission) to identify

problems with software, equipment, or systems which may affect the security or compliance of the software, equipment, or systems.

2. Problem reports shall be an entry to the change control procedures.

2.2.4 Design

REGULATORY OBJECTIVE

Software, equipment, and systems should be designed to meet security and regulatory objectives.

2.2.4.1 Design requirements

1. Design requirements for software, equipment, and systems shall incorporate legal requirements.
2. Design requirements for software, equipment, and systems shall incorporate regulatory guidelines.
3. Design requirements fore software, equipment, and systems shall incorporate security requirements.

2.2.4.2 Approval of design requirements

1. Design requirements shall be approved by the licence holder's management.
2. If systems design is provided by a third party then the licence holder management shall approve the means to ensure requirements are suitable (see 2.2.4.2).

2.2.5 Development

REGULATORY OBJECTIVE

Software, equipment, and systems development and integration shall combine software, equipment, and systems units to provide integrated software, equipment, and systems which demonstrate that the functional and non-functional requirements are satisfied on an equivalent or complete operational platform.

2.2.5.1 Compliant development

1. Software, equipment, and systems shall be developed in a manner which ensures compliance with requirements (see 2.2.4.1).
2. Software, equipment, and systems functional and non-functional elements should be traceable to design requirements.

2.2.5.2 Integration

1. An integration strategy shall be developed for software, equipment, and systems units consistent with the software, equipment, and systems design and the prioritised requirements.

2.2.6 Testing

REGULATORY OBJECTIVE

Software, equipment, and systems shall be tested to ensure security and compliance is implemented and maintained as required.

2.2.6.1 Test criteria

1. Criteria for integrated software, equipment, and systems should be developed to enable software, equipment, and systems to demonstrate compliance with the software, equipment, and systems requirements (see 2.2.4.1).

2.2.6.2 Verification

1. Software, equipment, and systems shall be verified using the defined test criteria (see 2.2.6.1).

2.2.6.3 Test results

1. Test (aka verification) results shall be recorded.

2.2.6.4 Regression testing

1. There shall be an effective regression strategy for re-testing integrated software, equipment, and systems when changes are made.

2.2.7 Deployment

REGULATORY OBJECTIVE

Licence holders shall ensure that software, equipment, and systems and changes thereto are deployed in a manner that security and compliance requirements are achieved and maintained.

2.2.7.1 Contents

1. The contents of the entire release of a system version shall be predefined and documented.
2. Records of the contents should be maintained.

2.2.7.2 Assembled from configuration items

1. The release should be assembled entirely from configuration items (see 2.2.1.1).
2. There shall be a master copy of all source and deployed configuration items kept for each and every version of software, equipment, and systems. This copy shall be maintained for the same period as gaming records under the Regulations.

2.2.7.3 Release documentation

1. The release shall be documented.
2. All changes should be reflected in user documentation.
3. All changes should be described in Release Notes.

4. All changes should be considered in the configuration item risk management plan (see 2.2.1.2).
5. Release notes shall include the configuration plan as an attachment.

2.2.7.4 Roll back

1. All proposed deployments shall have a tested roll-back strategy and procedures to ensure security and compliance is not affected in the event that a deployment fails for any reason.

2.2.7.5 Release approval

1. Releases shall be approved against defined and approved criteria.

2.2.7.6 Release delivery and deployment

1. The release delivery and deployment method should be defined, documented, and proven.

2.2.7.7 Release shall be deployed

1. Where a release is approved, it shall be deployed in accordance with the release plan.

2.2.7.8 Confirmation of release deployment

2. The deployment of the release shall be scrutinised for satisfactory deployment in operational equipment and/or systems.
3. Confirmation of the deployment of the release, release notes, and licence holder management approval shall be notified to the Commission.
4. There shall be a unique identifier, to the satisfaction of the Commission, of all deployed configuration items (i.e. MD5 hash of software). This shall be provided to the Commission within seven (7) days of the deployment.
5. All release notes and identifiers shall be provided to the Commission whether current at the time of provision or not.

2.2.8 Monitoring and maintenance

REGULATORY OBJECTIVE

Licence holders shall ensure that software, equipment, and systems are monitored and maintained in a manner to ensure:

- **on-going security and compliance in the face of dynamic threat scenarios; and**
- **timely identification and correction of vulnerabilities which might compromise security or compliance.**

2.2.8.1 Monitoring strategy, policies and procedures

6. Licence holders shall ensure an effective monitoring programme relating to threats and vulnerabilities to software, systems, and equipment to ensure the requirements meet the changing threat environment in which systems operate.

7. Licence holders shall ensure an effective programme relating to software, equipment, and systems operations and requirements to ensure continuous compliance with requirements.

2.2.8.2 Approved changes

1. Changes and upgrades are undertaken in accordance with approved change management procedures.

2.2.8.3 Release timetable

1. There should be a schedule of proposed implementation dates of changes. This should be the basis of all non-emergency and non-urgent changes and should be included as a dynamic annexure to the change and configuration plan as a component of the approved control systems. (That is the Commission should be fully informed of proposed dates of planned changes to software, equipment, and systems).

2.2.8.4 Metrics

1. Change records should be analysed regularly to determine the effectiveness of t he change and configuration management systems – and appropriate enhancements made where necessary. The results, conclusions, and corrective action of analysis of metrics should be recorded and maintained.
2. Actions for improvement identified from change management should be recorded and input into a plan for improving the operations. These in themselves would be “change requests” for procedures!

End of document