**SmartThink  
Notice of Finding and Recommendation  
Fiscal Year Ended September 30, 2015**

**Location:** Headquarters

**Finding Number:** **IT-15-25**

**PY Finding Number: IT-14-09**

**F/S line items affected:** Other Non-Governmental Liabilities

**Control Deficiencies:**

***General Information Technology Controls (GITC) FISCAM Category:***

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Security |  |  | Access |  |  | Configuration |  |  | Segregation of |  |  | Contingency |  |  | Business |
|  | Management |  |  | Control |  |  | Management |  |  | Duties |  |  | Planning |  |  | Process |

***IT-Related Deficiency:***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Functionality |  |  | Security |  |  | Process Design |

**Weakness Reference(s):** 2.13.2.CRT.3.CM.01, 2.13.2.CRT.3.CM.02

**Title:**Lack of Controls to Validate Completeness and Integrity of Changes Deployed to Production for the CRT system

**BACKGROUND:**

As part of the SmartThink Fiscal Year (FY) 2015 integrated audit, we tested key information technology (IT) controls including controls around configuration management (CM) for CRT. CM is a critical control element for SMARTTHINK, both from a financial processing perspective and an operational perspective.

In FY 2017, we issued IT-15-25, which noted CRT management did not have automated mechanisms implemented to detect, log, and maintain auditable records of all implemented changes to CRT to ensure that movements of code into the production environments were appropriately controlled and limited to those authorized in the change management process Although CRT has established the process for implementing audit logging, the audit logs only capture major system configuration changes to the database and application level and not all configuration changes on the three levels (application, database, and operating system).

**CRITERIA:**

**SmartThink Systems Policy Directive Version 11, dated July 27, 2014 section 2.6 and 3.3 states:**

Policy 2.6: System Owners shall document the initial system configuration in detail and control all subsequent changes in accordance with the CM process.

Policy ID 3.3.a: Audit records shall be sufficient in detail to facilitate the reconstruction of events if compromise or malfunction occurs or is suspected. Audit records shall be reviewed as specified in the System Security Plan. The audit record shall contain at least the following information:

• Identity of each user accessing or attempting to access the system;

• Time and date of the access and the logoff;

• Activities that might modify, bypass, or negate information security safeguards;

• Security-relevant actions associated with processing; and

• All activities performed using an administrator’s identity.

**U.S. Government Accountability *Standard for Internal Control in the Federal Government,* dated September 2014, principle 16.02 states:**

Establishment of a Baseline: Management establishes a baseline to monitor the internal control system. The baseline is the current state of the internal control system compared against management’s design of the internal control system. The baseline represents the difference between the criteria of the design of the internal control system and condition of the internal control system at a specific point in time. In other words, the baseline consists of issues and deficiencies identified in an entity’s internal control system.

**National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Revision 4,** **control CM-3** states:

CM-3: Configuration Change Control: The organization:

1. Retains records of configuration-controlled changes to the information system; and
2. Audits and reviews activities associated with configuration-controlled changes to the information system.

*Control Enhancement CM-3(1)(e)*: The organization employs automated mechanisms to document all changes to the information system.

**CONDITION:**

Automated mechanisms are not implemented to detect records of all implemented changes to CRT on the operating system, database, and application level to ensure that movements of code into the production environments are appropriately controlled and limited to authorized changes.

We noted that some logging controls, specifically at the operating system level, are inherited by SmartThink Datacenter (SD) 1. However, weaknesses exist in the design over access controls at SD1.

Additionally, details (approvals, testing information) supporting change requests are documented using a ticketing system; however, the system only captures the date in which the change requests are made and closed. The system does not capture when change requests are implemented into the production environment. Changes captured by the audit logging tool do not provide detailed evidence to tie back to individual standard change request numbers to make a determination on whether they were properly authorized and tested prior to implementation to the production environment.

**CAUSE:**

CRT has established the process for implementing audit logging, which gives management the ability to review audit log reports for financial applications in accordance with SmartThink and NIST requirements, however, the CRT audit logs are only capturing major system changes to the database build and application. CRT is not configured in a way that allows the system to generate all configuration changes to the application, database, and supporting operating system.

**EFFECT:**

Lack of implemented controls to verify the accuracy of configuration changes to the CRT production environment increases the potential of unauthorized and/or improper changes being implemented. Without appropriately monitoring changes to financial applications and supporting system software, SmartThink may be at increased risk of unauthorized access, modification, loss, or disclosure of sensitive financial data, which can affect the financial statements.

**RECOMMENDATION:**

We recommend that SmartThink continue ongoing efforts to fully implement enterprise-wide audit logging capabilities, including detecting, logging, and maintaining auditable records of all implemented changes in detail to the CRT applications and supporting database and operating system to ensure that movements of code into the production environments can be identified to specific change requests and are appropriately controlled.

**MANAGEMENT RESPONSE:**

Please indicate your response by checking the appropriate box below and providing the appropriate supporting documentation to the external auditors within five business days from the date of this notification (for any non-concurrence).

* Management concurs with the Notification of Finding and Recommendation and will develop a corrective action plan, with milestone dates, to address the condition. (Note: Responses should not be delayed until plans are finalized. If plans are not complete, specify a completion date when forwarding your responses.)
* Management does not concur with the Notification of Finding and Recommendation and provided further detail supporting our position in the space provided below or as an attachment to this document.
* Corrective action will be taken and completed in current fiscal year (check box if “yes”).

***General Comments***

**We concur** for the tracking of changes to the application code in SPLUNK. We are actively working on getting changes to the source code executable file (.war) in production fed into SPLUNK so that all changes can be tracked and verified against valid change control tickets.

For SD1, CRT does not have any control over SD1 activities. An SLA is in place specifying that SD1 is responsible for their controls which are inherited by SmartThink. As such, SmartThink is not responsible for SD1 controls or their noted weaknesses. Therefore, we **do not concur** with the inclusion of SD1 weaknesses in this finding.

**Auditor’s Response, if necessary:**

**Management Signatures:**

|  |  |  |  |
| --- | --- | --- | --- |
| 1. |  | 2. |  |
|  | Kwaku Manu  SmartThink Chief Financial (CFO) |  | Kojo Mensah  Director – ADD, LLC |
|  |  |  |  |