Chief Information Office

IT General Controls Assessment BidStamp

Internal Audit Report 19-102

April 2019

Department of Information Resources

Internal Audit Mission Statement

To collaborate with DIR leadership to fulfill the agency's core mission by providing independent and objective audit services designed to add value and improve the effectiveness of risk management, control, and governance processes.

DIR Internal Audit Staff

Cathy Sherwood, Interim Internal Audit Director

Victoria Lei, Audit Intern

Vicki Yang, Audit Intern

Table of Contents

Executive Summary

This report summarizes the scope, results, and recommendations from the work performed in conducting the BidStamp e-procurement system audit.

This performance audit project was included in the Fiscal Year 2019 Internal Audit Annual Plan. The **audit objective** was to assess whether BidStamp IT general controls were properly designed and working as intended. The **audit scope** included user access and configuration management control activities from September 1, 2018 through April 1, 2019. *User access* controls refer to controls that limit or detect access to computer resources (data, programs, equipment, and facilities), thereby protecting them against unauthorized modification, loss and disclosure. *Configuration management* refers to the control that prevents unauthorized changes to information system resources (for example, software programs and hardware configurations) and provides reasonable assurance that systems are configured and operating securely and as intended. The **audit methodology** is described in the Background section of this report.

Overall, IT general controls could be improved with regard to user access and configuration management controls for BidStamp. Supporting documentation for user profile changes was not always available for review. Based on the results of audit work performed, more comprehensive policies and procedures should be developed to provide assurance on the effectiveness and reliability of IT general controls for BidStamp, the application that supports both vendor and DIR user accounts for procurement activities. The following were issues identified related to logical access:

- A defect in the BidStamp logic in Salesforce caused Internal Audit's test vendor account to be associated with an existing account erroneously. A new vendor account could be automatically linked to another account if the tax ID used to create the new account is the same with that of an existing vendor, allowing the new account user to view information uploaded by the existing vendor user.
- There is currently no formalized standard operating procedure to perform periodic user access reviews for BidStamp. Internal Audit recommended that the policies and procedures include consideration of user account changes when employees change jobs within the agency.

Background

The BidStamp application is DIR's e-procurement system that supports solicitations and contracts throughout the procurement lifecycle. It facilitates and adds automation to the following procurement processes: 1) Solicitation creation and posting; 2) Collecting vendor responses; 3) Evaluation of responses and recommendation, and 4) Contract creation, award, and management. BidStamp elements are described below:

- Solicitation Library – DIR employees can create, manage, approve, and post solicitations in the solicitation library.

- Vendor Information System Portal – Vendors can create a profile to view and respond to DIR solicitations.
- Evaluation & Tabulation – Evaluators and contract managers can create scorecards and pricing forms, configure evaluations, perform evaluations, and calculate total scores for vendor solicitations.
- Contract Award & Administration – DIR employees can create contract documents at the final stage of the procurement process.

This audit project was performed as part of the Fiscal Year 2019 Internal Audit Annual Plan. The **audit objective** was to assess whether BidStamp IT general controls were properly designed and working as intended. The **audit scope** included access control and configuration management control activities from September 1, 2018 through April 1, 2019.

The **audit methodology** included conducting interviews, reviewing relevant system documentation and audit criteria, including DIR policies and procedures for established controls. Internal Audit:

- Interviewed the BidStamp system administrator and internal account holders,
- Reviewed relevant criteria, such as Federal Information Security Controls Audit Manual and Global Technology Audit Guide published by the Institute of Internal Auditors,
- Set up a test vendor account to assess effectiveness of user access controls,
- Reviewed the BidStamp password policy to compare with the agency password policy, and
- Reviewed BidStamp internal user accounts (active and deactivated accounts) to determine whether system access was required based on the user's role in the organization and to determine whether user accounts were deactivated timely for employees who a) changed roles within the agency or b) terminated employment with the agency during the period under review.

We conducted this audit in conformance with the International Standards for the Professional Practice of Internal Auditing and in accordance with Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our issues and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our issues and conclusions based on our audit objectives.

Detailed Results

Overall, IT general controls are present in BidStamp system. Some access controls, such as user authentication and user accounts management, could be improved by establishing and implementing stronger control processes.

Logical Access:

Internal Audit requested and reviewed the following documents

- From BidStamp system administrator: BidStamp user list generated 3/11/19 that contains active and inactive users as of 3/11/19, and
- From Human Resources: DIR employee list generated 3/4/19 that contains all current and terminated employees between 9/1/18 to 3/4/19.

For the six terminated employees, we validated that all user accounts were appropriately deactivated in BidStamp. Because there is no date and time stamp to validate whether the action was performed timely, we reviewed Last Login Date for each terminated employee to compare the Last Login Date with the Termination Date. See the table below.

Term. Employees	Was System Access Removed? (Y/N)*	Last Login Date	Termination Date	Was the Last Login Date before the Termination Date? (Y/N)
Employee 1	Y	9/24/2018 9:22	1/1/2019	Y
Employee 2	Y	12/14/2018 15:47	1/1/2019	Y
Employee 3	Y	4/30/2015 16:33*	11/1/2018	Y
Employee 4	Y	4/30/2015 10:12*	10/15/2018	Y
Employee 5	Y	8/5/2015 12:27*	11/1/2018	Y
Employee 6	Y	1/17/2019 14:48	3/1/2019	Y

Based on this review, we noted that several Last Login Dates were several years in the past. Internal Audit recommended to management that user access be revoked for user accounts with no activity for six months (or some other time period that is deemed reasonable by management).

Based on the results of the audit work performed, formalized policies and procedures should be developed to strengthen IT general controls, including those related to the retention of supporting documentation for changes to user accounts based on changing needs for BidStamp access. Several key recommendations were made to improve processes that will help strengthen internal controls to better address these issues. Some of the high and priority recommendations included:

- Upgrade the matching test for account setting to a two-field matching test. Enable the linkage among accounts only if both company title and tax ID are the same.
- Formalize the internal access review procedure to ensure the appropriateness of role changes.

DIR management concurred with the results and recommendations reported by Internal Audit and provided action plans, estimated completion dates, and assigned responsibility to management staff for implementing the recommendations.

- Logical access controls refer to controls that limit or detect access to computer resources (data, programs, equipment, and facilities), thereby protecting them against unauthorized modification, loss and disclosure.
- Configuration management refers to the control that prevents unauthorized changes to information system resources (for example, software programs and hardware configurations) and provides reasonable assurance that systems are configured and operating securely and as intended.

Section 1: Access Control Issues

Access controls limit or detect access to computer resources (data, programs, equipment, and facilities), thereby protecting them against unauthorized modification, loss, and disclosure.

Issue 1: Correct BidStamp Logic in New Vendor Account Setup Process

Elements of a Finding	**Results**
Condition	When Internal Audit set up a test vendor account, the vendor tax identification (ID) field was populated with a zero (0). As a result, the system associated this test account to a real vendor with a tax ID (0). After receiving the email notification that the account had been set up in BidStamp, because of the erroneous assignment, Internal Audit could view the solicitations this vendor had ever bid on in the past.
Criteria	FISCAM(AC-3.1): access should be limited to individuals with a valid business purpose (least privilege). Unnecessary accounts (default, guest accounts) should be removed, disabled, or otherwise secured. GTAG 5.3.7: Input controls should be used to check the integrity of data entered into a business application, whether the source is input directly by staff, remotely by a business partner, or through a Web-enabled application. Input is checked to ensure that it remains within specified parameters.

Cause	The system should not have associated the test account with the existing account, and the logic will be corrected.
Effect	User of the account that was wrongly assigned to an existing vendor account have access to the information displayed to the real vendor, including the biding history.
Audit Recommendations	Upgrade the BidStamp logic to ensure that the intended matching test for account setup is corrected. If the company title and tax ID of a new account doesn't match that of an existing vendor, then the new account should be set up as a new vendor and not linked to an existing vendor account.
Management Response	
Statement of Agreement	Management agreed with internal audit recommendation(s).
Action Plans	Management will upgrade the BidStamp logic to ensure that the intended matching test for account setup is corrected. If the company title and tax ID of a new account doesn't match that of an existing vendor, then the new account should be set up as a new vendor and not linked to an existing vendor account.
Planned Implementation Date	Implemented May 31, 2019
Responsible Leadership	Director of IT Services

Issue 2: Establish Formalized Internal Access Review Procedures

Elements of a Finding	**Results**
Condition	No standard access review procedures are in place for the system administrator to periodically review access rights.
Criteria	GTAG 3.3.3: As part of its IAM monitoring process, the organization should establish a methodology to periodically review

	the access rights granted to all identities residing in its IT environment. This review, while facilitated by the IT department, should be conducted primarily by the organization with approvals received from each responsible business owner. In addition, privileged and IT account identities should be reviewed by an appropriate manager or system owner.
Cause	The BidStamp system administrator indicated there is no formalized access review procedures for internal user accounts. When the system administrator generates reports to see who is or is not logging in (internally), the system administrator may move the user account holder from a higher level of access license to the Force.com license (a license with a lower access to certain objects in Salesforce), or she will remove their access from Salesforce altogether, although this happens rarely.
Effect	Changing user account holder roles without a formal notification from the account holder's manager can result in erroneous changes that go undetected. It would be difficult for managers to discover the mistake timely if there is no documentation for the action.
Audit Recommendations	Formalize the internal access review procedures.
Management Response	
Statement of Agreement	Management agreed with internal audit recommendation(s).
Action Plans	Management will document a standard operating procedure for periodic internal access review procedures.
Planned Implementation Date	August 31, 2019
Responsible Leadership	Director, IT Services

Issue 3: Notify System Administrator when Employees Changes Job Roles

<table>
<tr><th>Elements of a Finding</th><th>Results</th></tr>
<tr><td><b>Condition</b></td><td>No standard procedures were in place to regulate the process of making changes to internal user roles when there were changes to DIR employee jobs.

In comparing the active employees list provided by HR department and active user list provided by the BidStamp system administrator, Internal Audit found four active employees who were active users in the BidStamp system who had a job change in the past six (6) months.

According to system administrator, notices for adds/terminations are received but not for employees with changed roles. As a result, the system administrator changed the user roles for these job-changed employees when informal notifications were received.

<table>
<tr><th>Employees with Job Changes</th><th>Job Changed and Role in BidStamp Changed?</th><th>Method of Notification</th></tr>
<tr><td>Employee 1</td><td>Y</td><td>Informal</td></tr>
<tr><td>Employee 2</td><td>Y</td><td>Informal</td></tr>
<tr><td>Employee 3</td><td>Y</td><td>Informal</td></tr>
<tr><td>Employee 4</td><td>Y</td><td>Informal</td></tr>
</table>
</td></tr>
<tr><td><b>Criteria</b></td><td>FISCAM AC – 3.1 Listings of authorized users and their specific access needs and any modifications should be approved by an appropriate senior manager and directly communicated in writing by the resource owner to the security management function. A formal process for transmitting these authorizations, including the use of standardized access request forms, should be established to reduce the risk of mishandling, alterations, and misunderstandings.</td></tr>
</table>

Cause	The is currently no standard procedure in place to notify system administrators when employees transfer or get promoted into positions requiring level of access changes.
Effect	Without documentation to notify user role changes within the agency, system administrators rely on informal methods of collecting information and are not able to support role changes in the application.
Audit Recommendations	DIR Human Resources should route formal notification of employee job changes to IT Services to provide support for changes to user account holder role changes. Consider options that allow for automation.
Management Response	
Statement of Agreement	Management agreed with internal audit recommendation(s).
Action Plans	DIR Human Resources will formalize a process to notify IT Services about DIR employees who change jobs so that user access updates can be completed timely.
Planned Implementation Date	Implemented April 15, 2019
Responsible Leadership	Director, Human Resources (in coordination with IT Services)

Appendix A: Report Distribution

Internal Report Distribution

Department of Information Resources (DIR) Board

DIR Executive Director

DIR Chief Information Office (CIO)

DIR Chief Procurement Office (CPO)

DIR Chief Financial Office (CFO)

DIR CIO IT Services Director

DIR CPO Cooperative Contracts Director

DIR Human Resources Director

External Report Distribution

Texas Office of the Governor

Texas Legislative Budget Board

Texas State Auditor's Office

Texas Sunset Advisory Commission