# Banner INB Event – March 26, 2018

Problem Solving Analysis

## Background

Monday morning, March 26, 2018, following an upgrade to the BEIS SSO Manager the previous day, multiple users reported difficulties logging into Banner through Internet Native Banner (INB). OIT Technical Services (TS) resolved the majority of the issues by about 3:00 PM Monday. An additional issue, related to bookmarks which were made obsolete by the upgrade persisted into Tuesday morning but were resolved by the Service Desk/TS. An unrelated Banner connection issue caused by a known INB server java logging bug persisted into Wednesday.

## Break Down of the Problem

During the BEIS SSO Manager upgrade, a step was omitted which resulted in incorrect JVM setting on the INB servers. Additionally, an incorrect configuration file was used as the source for Oracle Forms. This disabled all but one of the load balanced INB servers and resulted in login failures when users began logging into Banner on Monday morning. Technical Services updated the INB servers to use the correct configuration file and JVM parameter and rebooted the servers.

## Target State / Goal

Banner databases and services should remain operational at all times outside of a published outage maintenance window. Upgrade procedures should be thoroughly tested through pre-production instances before promotion to production. Post upgrade testing should be rigorous enough to expose any operational deficiencies.

## Root Cause Analysis

An Ellucian consultant led the BEIS SSO Manager Upgrade with assistance from TS DBA. During the upgrade, the implementation team determined that part of the procedure would need to be accomplished by a Windows Systems Administrator. The on-call Windows SA was called in at that time. The TS Windows SA performed the procedure and validated the change by rotating the server back into the load balancer. The TS Windows SA then repeated the procedure on the remaining 10 servers. The SA inadvertently missed a step on the remaining servers to update a JVM parameter (jvmcontroller). The remaining servers were then rotated back into the load balancer without validating each server independently. The problem was masked by the fact that one properly configured server was online which allowed for limited authentication services.

## Develop Countermeasures

Ensure the whole team is included and aware of their role prior to the upgrade. Additionally, a final peer review, in collaboration with the Ellucian contractor, of all of proposed changes and procedures prior to the day of scheduled activity is warranted. This would help to ensure everyone is on the “same page” for body of work, expected resource availability, well-defined testing/validation procedures, and well-defined decision gates/framework if decisions need to be made in-flight.

The documented test plan was not adequate as documented in the change record which was reviewed by the CAB. The test plan states that “Once the upgrade is complete, several OIT personnel can verify that SSO is functioning…”. The test plan should indicate the steps that will be taken to validate the change. In this case, it could have indicated that each server would be validated using a pre-documented process and then spell out what that process is. The CAB members should verify that the information contained in the Change record is detailed enough to help eliminate negative impacts following service changes.