Banner Disaster Recovery Plan

Table of Contents

---

1. Introduction

Information systems are vital to the Ventura County Community College District mission/business processes; therefore, it is critical that services provided by Banner$^©$ can operate effectively without excessive interruption. This Disaster Recovery Plan (DRP) establishes comprehensive procedures to recover Banner quickly and effectively following a service disruption.

1.1 Background

This Banner DRP establishes procedures to recover Banner following a disruption.

The following recovery plan objectives have been established:

- Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
  - **Activation and Notification phase** to activate the plan and determine the extent of damage
  - **Recovery phase** to restore Banner operations
  - **Reconstitution phase** to ensure that Banner is validated through testing and that normal operations are resumed.
- Identify the activities, resources, and procedures to carry out Banner processing requirements during prolonged interruptions to normal operations.
- Assign responsibilities to designated COS personnel and provide guidance for recovering Banner during prolonged periods of interruption to normal operations.
- Ensure coordination with other personnel responsible for COS contingency planning strategies. Ensure coordination with external points of contact and vendors associated with Banner and execution of this plan.

1.2 Scope

This DRP has been developed for Banner, which is classified as a high-impact system. Procedures in this DRP are for high-impact systems and designed to recover Banner within 3 hours. This plan does not address replacement or purchase of new equipment, short-term disruptions lasting less than 3 hours, or loss of data at the onsite facility or at the user-desktop levels.

The following assumptions were used when developing this DRP:

- Banner has been established as a high-impact system.
- Recovery of Banner in a timely manner is a very high priority due to system unavailability impacting services to students and the public.

- The primary production processing site and offsite storage reside at Amazon Web Services™ (AWS) in the `us-west-2` region in Oregon, in Availability Zone `us-west-2a` (AZ1).
- Alternate processing sites and offsite storage are required and have been established for this system at AWS region `us-west-2` in Availability Zone `us-west-2b` (AZ2).
- The Banner Production database server, named `x`, is running Oracle$^{©}$ version 19C and is located in AZ1.
- A Banner Development database server, named `x`, is running Oracle version 19C and is located in AZ2. This server hosts the Banner TEST environment database, the Banner DEVL environment database, and the Banner DR system database.
- Data is continuously replicated from `x` to `x` using the Oracle Enterprise feature Data Guard.
- Current backups of the system software and data are intact and available in an AWS Simple Storage Service (S3) bucket in the `us-west-2` region.
- The Recovery Point Objective (RPO) is 3 hours.
- Access to the Banner system at AWS AZ1 has been determined to exceed the Recovery Time Objective (RTO) of **3** hours.
- Key Banner personnel have been identified and trained in their emergency response and recovery roles; they are available to activate the Banner DR Plan.

This Banner DRP does not apply to the following situations:

- Overall recovery and continuity of mission/business operations: Other college plans will address the continuity of business operations.
- Emergency evacuation of personnel: The college's Emergency Preparedness Handbook addresses employee evacuation. The Handbook is available on the college's website at:
  - Link to emergency preparedness plan.

---

2. Concept of Operations

The Concept of Operations section provides details about Banner, an overview of the three phases of the DRP (Activation and Notification, Recovery, and Reconstitution), and a description of the roles and responsibilities of COS personnel during a contingency activation.

2.1 System Description

Banner Description

The core software application for a higher education institution is its Enterprise Resource Planning (ERP) system, which is a platform used by such organizations to manage day-to-day business activities. The ERP system used by COS is Banner from Ellucian, a system which is currently deployed worldwide at over 1,400 higher education sites. The Banner platform includes a Student Information System and modules for Finance, Human Resources, and Financial Aid.

Users of Banner include:

- Students can access Banner via the Self-Service system over the Internet, providing features to register for classes, pay fees, submit financial aid documents, and check grades.
- Faculty can access Banner via the Self-Service system over the Internet, providing features to track student attendance, access class rosters, and enter grades.
- Counselors can review student academic progress.
- Staff can manage student records, administer course information, process purchasing requisitions and purchase orders, and manage employee records.

Hosting Environment Description

The COS Banner platform is hosted in the Amazon Web Services (AWS) `us-west-2` Region located in Oregon. System components are located within that region in two Availability Zones. The AWS Availability Zone AZ1 is where COS hosts its production systems, including Banner, Portal Guard™, and DegreeWorks©. COS hosts Banner development systems and databases in AZ2, along with Banner DR system components and replicated data.

The Banner environment includes multiple components, including EC2 servers running Oracle Enterprise databases, EC2 servers hosting application software, RDS databases, S3 storage buckets for backups, and load balancers.

A full list of DR Components can be found here: [Banner Component Summary](#)

Functional capabilities of Banner needed during DR plan

The following core systems and applications will be available during a DR event:

- Banner Admin for staff access
- Banner Self-Service for student and faculty access
- Banner modules: Student, Finance, HR, Financial Aid

2.2 Overview of Three Phases

This DRP has been developed to recover the Banner system using a three-phased approach. This approach ensures that system recovery efforts are performed in a methodical sequence to maximize the effectiveness of the recovery effort and minimize system outage time due to errors and omissions.

The three system recovery phases are:

Activation and Notification Phase

Activation of the DRP occurs after a disruption or outage that may reasonably extend beyond the RTO established for a system. The outage event may result in severe damage to the facility that houses the system, severe damage or loss of equipment, damage that typically results in long-term loss, or loss of connectivity to the facility.

Once the DRP is activated, system owners and users are notified of a possible long-term outage, and a thorough outage assessment is performed for the system. Information from the outage assessment is presented to system owners and may be used to modify recovery procedures specific to the cause of the outage.

Recovery

The Recovery phase details the activities and procedures for recovery of the affected system, otherwise known as a Run Book. Activities and procedures are written at a level that an appropriately skilled technician can recover the system without intimate system knowledge. This phase includes notification and awareness escalation procedures for communication of recovery status to system owners and users.

Reconstitution

The Reconstitution phase defines the actions taken to test and validate system capability and functionality at the DR location. This phase consists of two major activities: validating successful reconstitution and deactivation of the plan.

During validation, the system is tested and validated as operational prior to returning the operation to its normal state. Validation procedures may include functionality or regression testing, concurrent processing, and/or data validation. The system is declared recovered and operational by system owners upon successful completion of validation testing.

Deactivation includes activities to notify users of system operational status. This phase also addresses recovery effort documentation, activity log finalization, incorporation of lessons learned into plan updates, and readying resources for any future events.

2.3 Roles and Responsibilities

The DRP establishes several roles for Banner recovery and reconstitution support. Persons or teams assigned DRP roles have been trained to respond to a contingency event affecting Banner.

COS has two DRP co-Directors:

Name	Title
	Manager Infrastructure & Security
	Applications Manager

The DRP co-Directors have overall management responsibility for the plan and are responsible to oversee recovery and reconstitution progress, initiate any needed escalations or awareness communications, and establish coordination with other recovery and reconstitution teams as appropriate.

DRP Team Members:

Name	Title	Area of Responsibility
	Cloud Applications Engineer	Applications host at AWS
	Cloud Infrastructure Engineer	AWS infrastructure
	Database Administrator	Oracle Database
	Network Analyst	Network Issues

3. Activation and Notification

The Activation and Notification Phase defines initial actions taken once a Banner disruption has been detected or appears to be imminent. This phase includes activities to notify recovery personnel, conduct an outage assessment, and activate the DRP. At the completion of the Activation and Notification Phase, Banner DRP staff will be prepared to perform recovery measures.

3.1 Activation Criteria and Procedure

The Banner DRP may be activated if one or more of the following criteria are met:

1. The type of outage indicates Banner will be down for more than 3 hours
2. The infrastructure (data center, network, etc.) may not be available within 3 hours
3. *Other criteria, as appropriate.*

The following persons or roles may activate the DRP if one or more of the above criteria are met:

- Dan Watkins – Associate Vice Chancellor of Information Technology

3.2 Notification

The first step upon activation of the Banner DRP is a notification of appropriate business and system support personnel. Contact information for appropriate POCs is included in *Appendix A: Personnel Contact List*.

For Banner, the notifications will be sent by the DRP Co-Director through email to faculty, staff, and students. Communication with key college personnel will be coordinated through phone by the Dean of Technology.

3.3 Outage Assessment

Following notification, a thorough outage assessment is necessary to determine the extent of the disruption, any damage and expected recovery time. This outage assessment is led by DRP Co-Directors. Assessment results are provided to the DRP Coordinator to assist in the coordination of the recovery of Banner.

The DRP team will check the AWS Service Health Dashboard here:
https://status.aws.amazon.com/

If the Dashboard does not provide sufficient information, then an AWS support ticket will be opened:

To Open a Support Ticket with AWS Support:

1. Sign in to the AWS Console.
2. On the upper right hand corner, click **Help** and select **Support**.
3. Click the blue box that says, **Open a new case**.
4. Select what your case is regarding and complete the required details.
5. Select your contact method to submit your case.

Return to Table of Contents

Jump to Appendix C: Detailed Recovery Procedures (Run Book)

4. Recovery

The Recovery Phase provides formal recovery operations that begin after the DRP has been activated, outage assessments have been completed (if possible), personnel have been notified, and appropriate teams have been mobilized. Recovery Phase activities focus on implementing recovery strategies to restore system capabilities, repair damage, and resume operational capabilities at the original or an alternate location. At the completion of the Recovery Phase, Banner will be functional and capable of performing the functions identified in Section 2.1 of this plan.

4.1 Sequence of Recovery Activities

The following activities occur during recovery of Banner:

Click on each high-level step to see detailed procedures for completing the activity.

- 1. Verify integrity of AD Domain Controller in AZ2.
- 2. Restore Banner Components from Backups
- 3. Verify Oracle database data replication status and DB availability in AZ2
- 4. Recover Banner Job Submission Server (EC2)
- 5. Verify integrity of EFS shared file system in AZ2
- 6. Update internal DNS entries for the Database
- 7. Verify integrity of PortalGuard IDP (Database and Front End Webserver)
- 8. Verify ECS cluster is running and each application is functional
- 9. Recover reporting and integration EC2 server instances from Veeam backup
- 10. Verify nightly processing jobs are working correctly

To edit the sequence steps, go to Appendix C: Detailed Recovery Procedures (Run Book) and change the names on the child pages and edit their content as necessary. The steps will be automatically updated here.

4.2 Recovery Procedures

Detailed procedures are provided in Appendix C: Detailed Recovery Procedures (Run Book).

4.3 Recovery Escalation Notices/Awareness

The DRP Co-Director will send out notification via COSeNews as necessary.

---

5. Reconstitution

The Recovery Phase provides formal recovery operations that begin after the DRP has been activated.

Reconstitution is the process by which recovery activities are completed and normal system operations are resumed. A determination must be made on whether the system has undergone significant change and will require reassessment and reauthorization. The phase consists of two major activities: validating successful reconstitution and deactivation of the plan.

5.1 Validation Data Testing

Validation data testing is the process of testing and validating recovered data to ensure that data files or databases have been recovered completely and that data is correct and up to date. During this process, an assessment will be done to confirm the time of the last transactions that were posted to determine if any data loss has occurred.

Detailed data test procedures can be found in Appendix E, System Validation Test Plan. All test results will be documented.

5.2 Validation Functionality Testing

Validation functionality testing is the process of verifying that Banner functionality has been tested, and the system is ready to return to normal operations. Details for functional testing are included in Appendix E, System Validation Test Plan. All test results will be documented.

Banner Test Plans can be found here: Banner Test Plans

5.3 Recovery Declaration

Upon successfully completing testing and validation, the one of the DRP Co-Directors will formally declare recovery efforts complete, and that Banner is in normal operations. Banner business and technical POCs will be notified of the declaration by the DRP Coordinator.

5.4 Notifications (Users)

Upon return to normal system operations, Banner users will be notified by one of the DRP Co-Directors using COS e-News and email notifications.

5.5 Data Backup

As soon as reasonable following recovery, the system should be fully backed up and a new copy of the current operational system stored for future recovery efforts. This full backup is then kept

with other system backups. While the system has an automated backup policy in Veeam to backup everything on a set time schedule, a manual backup should be conducted after the all the systems have been recovered in AZ2 and before functional user testing. This ensures a clean copy of the recovery efforts exists prior to functional users accessing the recovery system.

The procedures for conducting a full system backup are:

1. Manually run the backup processes in Veeam.
    1. Log into the the web version, on premise client, or the bastion host and click on **Back up now**.
        1. The preferred method would be to back it up on-premise so you can back up everything all at once.
    2. As long as the restored instance has the correct tags, it will get picked up by the backup job.
    3. Monitor the process and ensure there is a successful backup.
        1. If you back up from the web version, your backup will go to the S3 bucket assigned to the backup policy.
        2. If you back from on-premise, your backup will go to one of three backup storage servers on-prem and will push out to S3 after 30 days.
        3. If you back up from the bastion host, there will be a snapshot and then the backup will go to the S3 bucket assigned to the backup policy.
            1. This will only work for the servers in AWS.

5.6 Event Documentation

It is important that all recovery events be well-documented, including actions taken and problems encountered during the recovery and reconstitution effort, and lessons learned for inclusion and update to this DRP. It is the responsibility of each DRP team or person to document their actions during the recovery and reconstitution effort and to provide that documentation to the DRP Coordinator.

Types of documentation that should be generated and collected after a contingency activation include:

- Activity logs: Including recovery steps performed and by whom, the time the steps were initiated and completed, and any problems or concerns encountered while executing activities.
- Functionality and data testing results: Including the specific steps performed and by whom, the date the steps were initiated and completed, and any problems or concerns uncounted while executing activities.
- Lessons learned documentation
- After Action Report

Event documentation procedures will detail responsibilities for development, collection, approval, and maintenance.

In the event of a disaster, document each event individually in Confluence under the Banner Disaster Recovery Event Documentation pages.

5.7 Deactivation

Once all activities have been completed and documentation has been updated, one of the DRP Co-Directors will formally deactivate the DRP recovery and reconstitution effort. Notification of this declaration will be provided to all business and technical POCs through COS e-News and email notification.

Return to Table of Contents

Appendix A: Personnel Contact List

- [Banner DRP Key Personnel](#)
- [Banner DRP Key College Contacts](#)
- [Banner Functional Testing Key Personnel](#)

Banner DRP Key Personnel

Key Personnel	Contact Information	
All COS personnel may be contacted in Microsoft Teams, through their desktop or smartphone application, as well.		
DRP Co-Director	Work	
Applications Manager	Cellular	
Insert Street Address	Home	N/A
	Email	
DRP Co-Director	Work	
Manager Infrastructure & Security	Cellular	
N/A	Home	N/A
	Email	
DRP Team – Team Members		
Database Administrator	Work	
	Cellular	
	Home	
	Email	
Cloud Infrastructure Engineer	Work	
	Cellular	
	Home	
	Email	
Cloud Applications Engineer	Work	
N/A	Cellular	
Visalia, CA 93277		
	Email	
Network Analyst	Work	

	Cellular	
	Home	
	Email	
Dean, Technology Services	Work	
	Cellular	
	Home	
	Email	

Return to Table of Contents

Banner DRP Key College Contacts

This contact list is for disaster communications that are non-global announcements. Communication will take place via Teams. If Teams is down, move to email, and if email is unavailable, move to phone or Zoom. If members of the team need to be contacted by cell phone, the Dean of Technology Services will contact them.

Title	Name	Phone
College President		
Vice President of Academic Services		
Vice President of Administrative Services		
Vice President of Student Services		
Provost - Hanford Educational Center		
Provost - Tulare College Center, Dean of Agriculture		
Dean of Fine Arts and English		
Dean of Business, Social Science, and Consumer Family Studies		
Dean of CTE and Workforce Development, Nursing and Allied Health		
Dean of Educational Support Services		
Dean of Physical Education, Director of Athletics		
Dean of Human Resources		
Dean of Facilities		
Dean of Natural Sciences, Mathematics, and Engineering		
Dean of Research, Planning And Institutional Effectiveness		
Dean of Student Services		
Dean of Student Services		
Dean of Student Services		
Dean of Technology Services		
Registrar functions		
Financial Aid Director		

Banner Functional Testing Key Personnel

For a comprehensive list of testing plans see the Banner Test Plan pages.
In the event of a disaster, complete the Banner Disaster Recovery Event Documentation page.

Banner Functional Testing Key Personnel		
Key Personnel	**Contact Information**	
[Banner-Evisions Reporting and Research Test Cases](#)		
	Work	
	Email	
	Work	
	Email	
[Banner File Transfer Inventory](#)		
	Work	
	Email	
	Work	
	Email	
	Work	
	Email	
	Work	
	Email	
	Work	
	Email	
[Banner Finance Test Cases](#)		
	Work	
	Email	
	Work	
	Email	
	Work	
	Email	

	Work	
	Email	
	Work	
	Email	
[Banner Financial Aid Test Cases](#)		
	Work	
	Email	
	Work	
	Email	
[Banner General-Technical Test Cases](#)		
	Work	
	Email	
	Work	
	Email	
	Work	
	Email	
	Work	
	Email	
	Work	
	Email	
	Work	
	Email	
	Work	
	Email	
	Phone	
	Email	
	Phone	
	Email	
[Banner Payroll-HR Test Cases](#)		

	Work	
	Email	
	Work	
	Email	
	Work	
	Email	
	Work	
	Email	
[Banner Self Service Test Cases](#)		
	Work	
	Email	
	Work	
	Email	
	Work	
	Email	
	Work	
	Email	
	Work	
	Email	
	Work	
	Email	
[Banner Student Test Cases](#)		
	Work	
	Email	
	Work	
	Email	
	Work	
	Email	
	Work	

	Email	
	Work	
	Email	
	Work	\
	Email	\

Appendix B: Vendor Contact List

Key Personnel	Contact Information	
AWS™	Support	Open support tickets in AWS Console
	Phone	
	Email	
	Phone	
	Email	
Cumulus		
	Phone	
	Email	
	Phone	
	Email	
	Phone	
	Email	
	Phone	
	Email	
	Phone	
	Email	
Milton Security	Main Office	
	General Email	
	Support/Ticket	
MS-ISAC	Main Office	
	Work	
	Email	
	Email	
	Email	

	Work	
	Email	
	Support	
Strata Information Group	Main Office	
	Cellular	
	Work	
	Email	
	Cellular	
	Work	
	Email	
CENIC	Support - Open a case on website	
Ellucian©	Support - Call or Open a case on website (preferred)	•
Evisions©	Support - Call, email, or Open a case on the support portal (preferred)	
Heartland ECSI©	Email	
Oracle©	Open a case online	•

Courseleaf		
Support	Open case via email/website	
	Email	
	Chat	

PortalGuard (IDaaS) - https://www.bio-key.com - **MyGiant**		
Support	Open case via email/website	
	Phone	
	Cell	
	Email	
	Phone	
	Email	

Veeam©	Support - Open a case on website	

Ready Education	
Email	
Email	
Email	

Return to Table of Contents

Open a support ticket with Ellucian

Follow these steps to open a support ticket with Ellucian.

Log into Ellucian.com
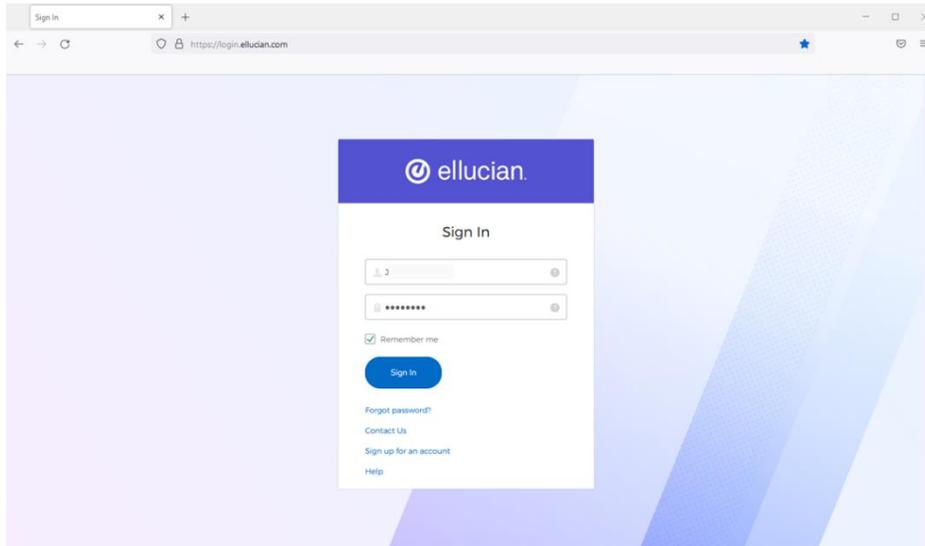
Click on **Create a Case**.
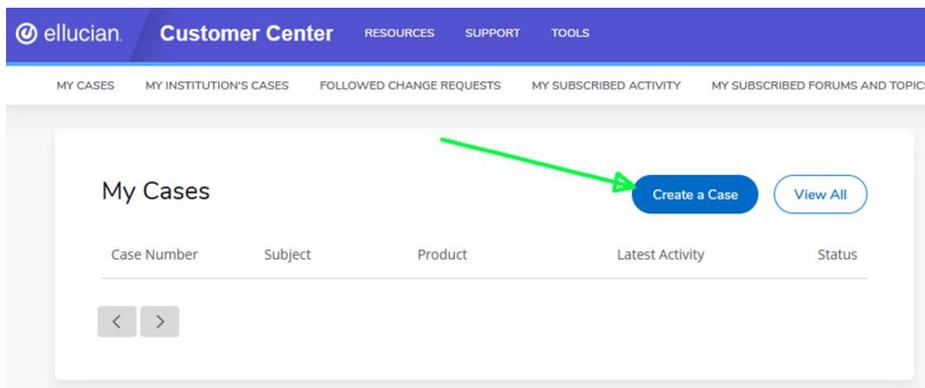
Open a support ticket in Oracle

Follow these steps to open an Oracle support ticket.

The easiest way to open a Ticket with Oracle is to use the Feature within Oracle Enterprise Manager:
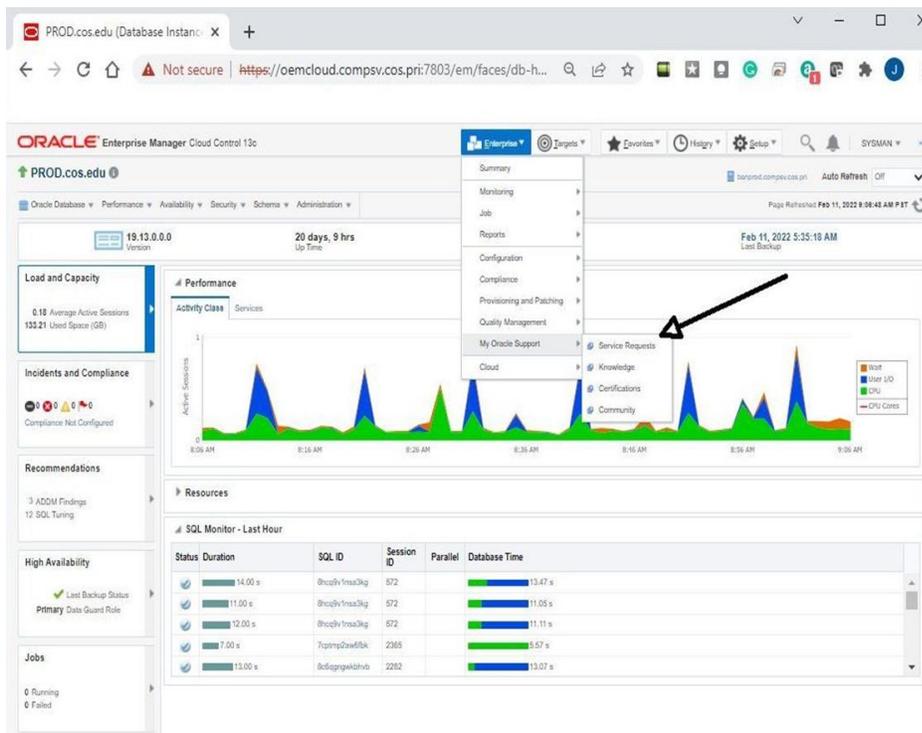
Once you click on the "Service Request" it will open your Oracle Account Login:

Once Logged in you will select the "Create Technical SR" and submit your Request for Support

Appendix C: Detailed Recovery Procedures (Run Book)

The following procedures are provided for the recovery of Banner in AWS AZ2. Recovery procedures are outlined per team and should be executed in the sequence presented to maintain an efficient recovery effort.

Access credentials for executing disaster recovery steps

Where to access

The credentials are kept in KeePass

As part of the testing and maintenance schedule, KeePass will be exported from on-prem and imported to AZ2 so it will be available in the event on-prem services cannot be accessed.

Who can access

The following people have the credentials to KeePass. One of these contacts will need to access the credentials to start disaster recovery.

Name	Title
	Manager Infrastructure & Security
	Cloud Applications Engineer
	Cloud Infrastructure Engineer
	Network Analyst
	Database Administrator
	Webmaster

General procedures for the recovery of the system

The following activities occur during recovery of Banner:

Click on each high-level step to see detailed procedures for completing the activity.

- 1. Verify integrity of AD Domain Controller in AZ2.
- 2. Restore Banner Components from Backups
- 3. Verify Oracle database data replication status and DB availability in AZ2
- 4. Recover Banner Job Submission Server (EC2)
- 5. Verify integrity of EFS shared file system in AZ2
- 6. Update internal DNS entries for the Database
- 7. Verify integrity of PortalGuard IDP (Database and Front End Webserver)
- 8. Verify ECS cluster is running and each application is functional
- 9. Recover reporting and integration EC2 server instances from Veeam backup
- 10. Verify nightly processing jobs are working correctly

To edit the steps, go to the child pages, change the name of the page, and edit the content as necessary. The changes will be updated on this page when the child pages are published.

Return to Table of Contents

1. Verify integrity of AD Domain Controller in AZ2.

These must be up and functional before restoring anything else.

1. Below are the screen shots for checking AD replication from `COS-DC01` which is the on-prem top level domain controller.
   1. Launch the AD Replication Status Tool.
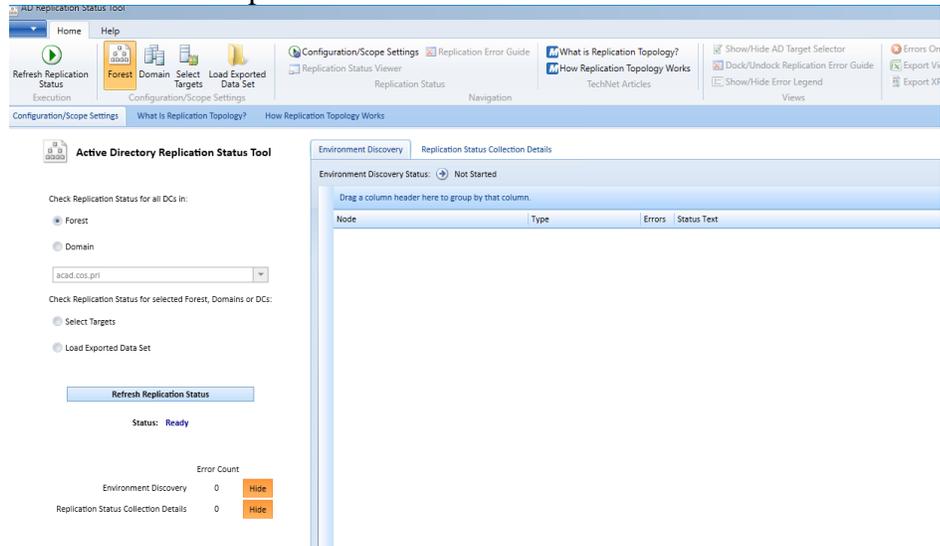
   2.

      Keep the radio button on **Forest** and click **Refresh Replications Status**.
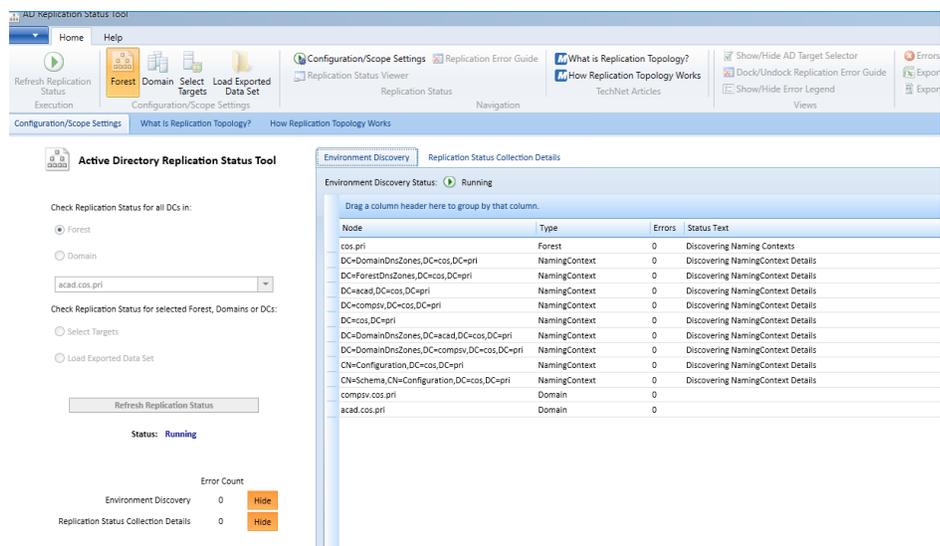
   3.

      You should only see the one error coming from the server it is running on since it can't replicate with itself.

These steps will confirm that the AD sync is happening to the servers in AZ2, which we have ADs in both servers so it shouldn't require restoration of any kind in the event of one AZ going down.

Return to Table of Contents

Jump to Appendix C: Detailed Recovery Procedures (Run Book)

2. Restore Banner Components from Backups

Step 2a - Veeam restore process

There are three possible methods to restore Banner Management Tools from Veeam: either using the on-prem tools or the web UI from within the AWS account or Bastion host (if working remotely).

Pick of the steps from the list below:

- [On-prem restore](#)
- [Web UI restore](#)
- [Bastion host restore](#)

Whether you completed the on-prem, web UI, or Bastion host restore, you will need to complete this step below.

Step 2b - AWS backup to restore OEM server

1. Log into AWS and go to the **Dev account** > **AWS Backups**.
2. Go to **Backup vaults** and select that latest Recovery point ID for Resource ID
   `instance/i-05f1263d8c20195a9`.

	Recovery point ID	Status	Resource ID	Resource type	Backup type	Creation time	Source account ID	Reten
☐	image/ami-03fc3e1077debffae	⊘ Completed	instance/i-05f1263d8c20195a9	EC2	Image	April 4th, 2022, 10:00 PM (UTC-07:00)	–	35 day
☐	image/ami-081e3c3ce2f79110c	⊘ Completed	instance/i-05f1263d8c20195a9	EC2	Image	April 3rd, 2022, 10:00 PM (UTC-07:00)	–	35 day
☐	image/ami-06e61fb2d09136c37	⊘ Completed	instance/i-05f1263d8c20195a9	EC2	Image	April 2nd, 2022, 10:00 PM (UTC-07:00)	–	35 day

3. Click **Restore** in the upper right corner.
4. Specify a different subnet if needing to move to a different Availability Zone on the private network and click **Restore** at the bottom of the page.

5. Go to the EC2 service and wait for the server Instance state to be **Running** and attempt to log in.

Step 2c - Verify that Oracle Enterprise Manager is available in AZ2

These are notes about using Oracle Enterprise Manager to "Switchover" or "Failover" to a Standby database. A Switchover is done when both the Primary and Standby databases are operating normally. This might occur so that maintenance can be done on the Primary server while database activity continues in the Standby (temporarily Primary). The goal would be to switch back to the Primary database once maintenance is done. A Failover is performed when the Primary is no longer available. This would likely be the option in a DR situation.

- https://docs.oracle.com/en/database/oracle/oracle-database/19/sbydb/managing-oracle-data-guard-role-transitions.html#GUID-44F26D5F-E036-4ACD-B8F0-224F5498FBCE
- https://docs.oracle.com/en/database/oracle/oracle-database/19/dgbkr/using-data-guard-broker-to-manage-switchovers-failovers.html#GUID-0C37ACF2-4399-49B0-B9B4-982157FCDDED

1. Verify that Oracle Enterprise Manager is available in AZ2.
    1. To verify Enterprise Manager is running, go to this URL.
    2. This should display the following screen. To continue, enter a valid username and password.
    3. If you can log in and everything appears normal, Oracle Enterprise Manager is verified to be available in AZ2.
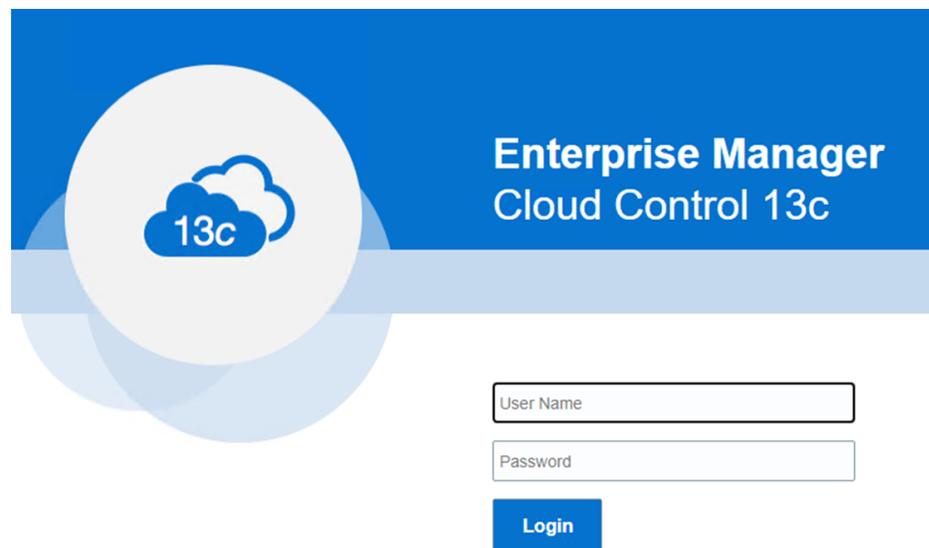
Return to Table of Contents
Jump to Appendix C: Detailed Recovery Procedures (Run Book)

On-prem restore

There is a known issue with the OEM server not connecting correctly when restoring from Veeam. You will complete the Veeam restores and restore the lacie drive from an AWS backup to ensure all the Banner Management Tools are working.

Veeam restore

1. Log into xxxxxxxxx. The IP address is xxxxxxxxx.
2. Launch the Veeam Backup application and log in.

3. From the **Home** tab, open **Backups** and then **External Repository** and find the servers you are looking to restore.

4. Right click on the server and click **Restore to Amazon EC2**.

5. Choose the restore point you need to restore from.

6. Choose if you are restoring over the original, or into a new location.
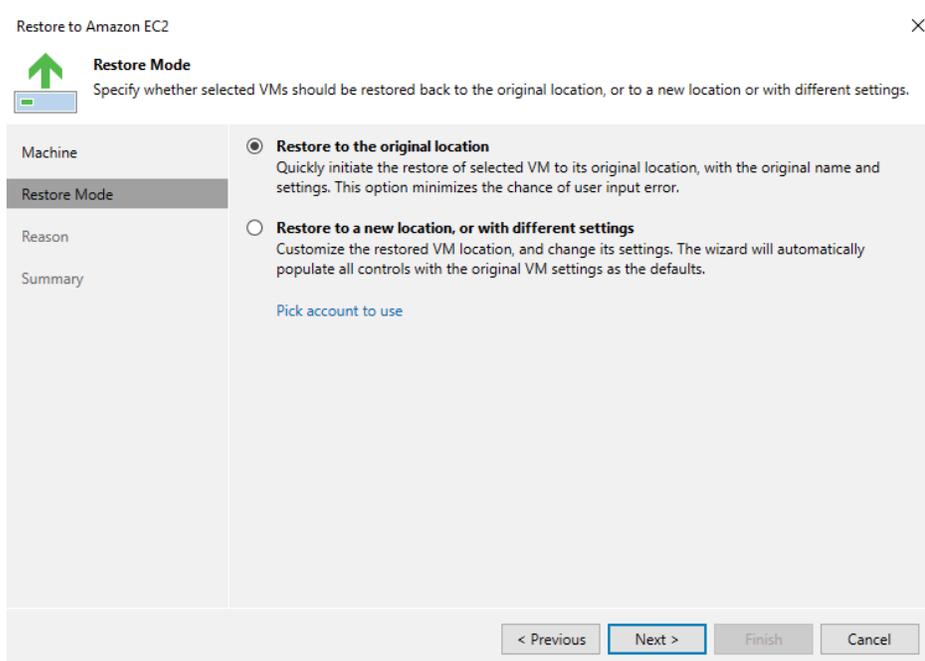
7. If going to the original location, click **Next**, give a reason, and then **Finish** to begin the restore.
8. If going to a new location, continue on from here, choosing the **Data Center** to restore to.

9. Specify the instance size using the screenshot below for reference.

10. Name the new instance.

11. Select which VPC, AZ and security group you wish to restore into.

12. Enter the reason and then **Finish**.

Final step - Verify that Oracle Enterprise Manager is available in AZ2

1. Continue to the at the bottom of the parent page.

Bastion host restore

1. Login to the AWS console.
2. The cos-dev account has an EC2 bastion host called `xxxxxxxxxx`.
3. On AWS console, go to **EC2 service** and find the bastion host instance.

4. Verify that the bastion host instance is in the `Running` state.
5. *If instance is Stopped, click on the checkbox and select **Instance state>Start instance** from the pull-down button at the top of the page.
6. When the instance is in the Running state, click the checkbox to show more detailed information.

7. Note the Public IPv4 address. This is the address you will need to connect to with your Remote Desktop client.
8. Next you need the Windows login credentials (this may be available in the department password repository).
9. If the credentials are not on file, they can be obtained from the AWS EC2 console.
10. To obtain the Windows credentials from the AWS console you need to have the key pair file associated with this instance. To find that information, scroll down to the **Instance details** section (after **Instance summary**).

11. Make note of the key pair name. You need to find the corresponding .PEM file.
12. Once you have this key pair file available, you can proceed to the next step.
13. With the same checkbox clicked for the bastion host instance, click on the **Connect** button at the top of the page.

14. This will bring up the **Connect to instance** page.
15. Click on the **RDP client** tab.

16. Next click on the **Get password** link towards the bottom of the page.

17. This will now prompt you for the key pair used to launch this EC2 instance.

18. Click on the **Browse** button to select the file with the corresponding key pair for this instance.
19. When the key pair file has been imported, click on the **Decrypt Password** button.
20. Next you will see the **Connect to instance** page showing the decrypted password.

21. You can now click on the **Copy** button to the left of the password to copy it to the clipboard.
22. Note that the windows username is xxxxxxx.
23. You can use the IP address, User name, and Password with your Remote Desktop client.
    1. Alternatively, you can click the **Download remote desktop file** button which will save a clickable RDP file with all of the required login information embedded. Once saved locally, clicking on this file will launch your Remote Desktop client and connect to the bastion host instance. If you've taken this route, jump to step 44.
24. Click on the **Cancel** button to exit this page and return to the EC2 instances page.
25. The final step is to grant your current workstation access to the bastion host.
26. On the EC2 Instances page, once again locate and click the checkbox for the bastion host instance.
27. Next click on the **Security** tab to review the Security Group for this instance.

28. The **Security details** page is now displayed.

29. Click on the highlighted security group.
30. This will bring up the security group details and rules.

31. Scroll down to review the **Inbound rules**. In order to access the bastion host from the Internet, your local IP address must be allowed access in the Security Group. Review the entries to see if your IP has been used previously. If not, you will need to add a new rule to allow your IP access over the RDP port 3389.
32. **The last piece of information you need is your own public IP address.**
    1. If you don't know your current IP address, you can go to the following web site: https://whatsmyip.com/
33. This web site will display your current public IP address. Copy this address so you can enter it into a new rule.
34. To add a new rule to the bastion host security group, click on the **Edit inbound rules** button.

35. This will display the **Edit inbound rules** page.

36. Click the **Add rule** button to add a new entry to the security group inbound rules.

37. Click on the **Type** drop-down menu and select **RDP** for Remote Desktop Protocol (port `3389`).
38. This will automatically populate the Protocol and Port range fields.
39. Leave the **Source** field as **Custom**.
40. Enter your IP address into the next field in the following format: `xx.xx.xx.xx/32`.
41. Use the **Description** field to document the owner and use case for this rule.
42. Verify all information has been entered correctly and click the **Save rules** button.
43. You now should have everything set to access the bastion host.
44. If you saved the RDP file, you can click it and it will automatically log you into the bastion host.
45. You may also manually enter the bastion host public IP, user name and password into your RDP client.
46. Once connected you will be presented with the Windows desktop of the bastion host, residing within the AWS account.

47. You can now use tools such as Putty (for SSH access) or Chrome to access web-based resources. You can also use RDP from within the bastion host to connect to other Windows servers located within the AWS environment.
48. For DR purposes, you will be launching Chrome to access the web-based GUI of the AWS Veeam instance.
49. Continue to the final step at the bottom of the parent page.

3. Verify Oracle database data replication status and DB availability in AZ2

1. Bring up Oracle Enterprise Manager and verify status of the standby database.
   1. To verify Enterprise Manager is running, go to this URL.
   2. This should display on the following screen. To continue, enter a valid username and password.
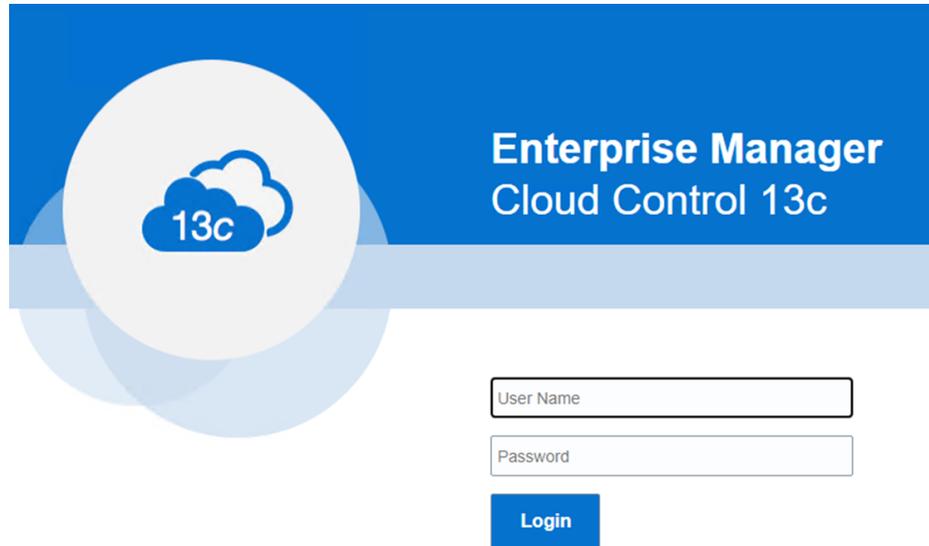
3. If your initial page is not the list of databases, go to the databases page by selecting **Databases** from the **Targets** menu:

4. On the databases page, you should see the Primary and Standby databases listed. Click on the link for the Standby database (**XXXX**):

5. On the Standby database home page, select **Data Guard Administration** from the **Availability** menu:
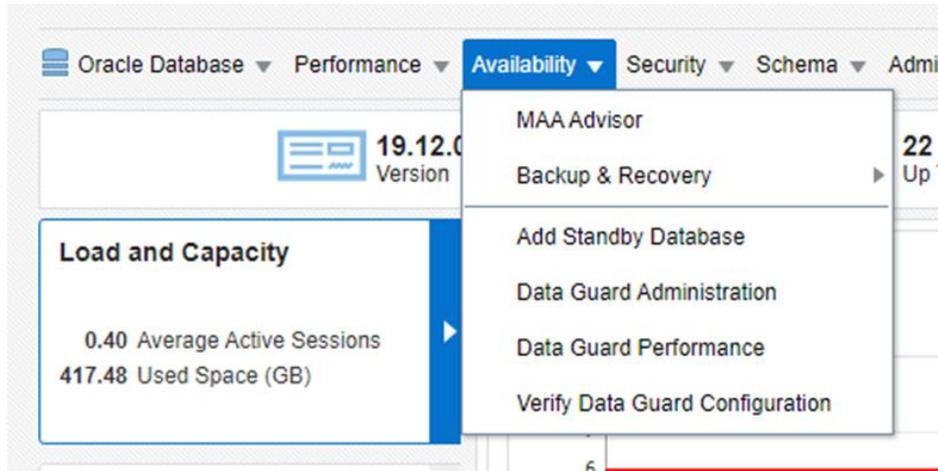
6. If you had not previously saved preferred credentials, you will be presented the **Database Login** screen. Enter the credentials for the SYS user, set as preferred SYSDBA credentials, and then click Login.

7. The subsequent screen lists details of the Primary and Standby databases. Currently, we have only one Standby. In this image, everything is normal. Note the **Current Log** is listed for the Primary database. This log file will be shipped to the Standby at the next log switch. Here you also see the 2 options to perform a Switchover or a Failover. Choose the one appropriate for the situation.

4. Recover Banner Job Submission Server (EC2)

There are two possible methods to restore, whichever method you pick, you have to follow the same method for .

- Method 1: Restore from Veeam, **or**
- Method 2: Redirect using the DEV job submission server.

Method 1: Restore from Veeam

- Refer to Step 2 for Veeam restore instructions.

Method 2: Redirect using the DEV job submission server

- Configure DEV job submission server to connect to standby.

Verify the file systems are restored correctly

After recovering the job submission server, execute a `df` command in PROD and DEV to view the directories. Verify the recovered directories match the screenshots below of how the directories look "normally."

DEV Job Submission Server File Systems:

```
[root@banevaljs ~]# df -h
Filesystem                                Size  Used  Avail  Use% Mounted on
devtmpfs                                  3.7G     0   3.7G    0% /dev
tmpfs                                     3.7G     0   3.7G    0% /dev/shm
tmpfs                                     3.7G  8.6M   3.7G    1% /run
tmpfs                                     3.7G     0   3.7G    0% /sys/fs/cgroup
/dev/nvme0n1p2                             64G  9.5G    55G   15% /
/dev/nvme1n1                              160G   94G    67G   59% /u01
fs-96234b93.efs.us-west-2.amazonaws.com:/ 8.0E   35G   8.0E    1% /lacie
10.22.48.145:/                            8.0E  664M   8.0E    1% /u02
tmpfs                                     753M     0   753M    0% /run/user/0
tmpfs                                     753M     0   753M    0% /run/user/501
tmpfs                                     753M     0   753M    0% /run/user/1000
```

PROD Job Submission Server File Systems:

```
[root@banprodjs ~]# df -h
Filesystem                                Size  Used Avail Use% Mounted on
devtmpfs                                  3.7G     0  3.7G   0% /dev
tmpfs                                     3.8G     0  3.8G   0% /dev/shm
tmpfs                                     3.8G  361M  3.4G  10% /run
tmpfs                                     3.8G     0  3.8G   0% /sys/fs/cgroup
/dev/nvme0n1p2                             64G  9.9G   55G  16% /
/dev/nvme1n1                              160G   95G   66G  60% /u01
10.20.51.200:/                           8.0E   35G  8.0E   1% /lacie
fs-9b596a9e.efs.us-west-2.amazonaws.com:/ 8.0E  5.9G  8.0E   1% /u02
tmpfs                                     761M     0  761M   0% /run/user/1000
tmpfs                                     761M     0  761M   0% /run/user/1002
tmpfs                                     761M     0  761M   0% /run/user/0
[root@banprodjs ~]# █
```

Return to Table of Contents
Jump to Appendix C: Detailed Recovery Procedures (Run Book)

5. Verify integrity of EFS shared file system in AZ2

- If you followed **Method 1**: Restoring from Veeam in the previous step, you will also follow **Method 1**: Remount EFS in this step.
- If you followed **Method 2**: Redirect using the DEV job submission server, in the previous step, you will also follow **Method 2**: EFS is already mounted.

You're looking for `/u02` and `/lacie` here:

```
oracle@PROD-JS [/home/oracle]
$ df -h
Filesystem                                Size  Used Avail Use% Mounted on
devtmpfs                                  3.7G     0  3.7G   0% /dev
tmpfs                                     3.8G     0  3.8G   0% /dev/shm
tmpfs                                     3.8G  361M  3.4G  10% /run
tmpfs                                     3.8G     0  3.8G   0% /sys/fs/cgroup
/dev/nvme0n1p2                             64G  9.1G   55G  15% /
/dev/nvme1n1                              160G   95G   66G  60% /u01
10.20.51.200:/                           8.0E   33G  8.0E   1% /lacie
fs-9b596a9e.efs.us-west-2.amazonaws.com:/ 8.0E  5.3G  8.0E   1% /u02
tmpfs                                     761M     0  761M   0% /run/user/1000
tmpfs                                     761M     0  761M   0% /run/user/0
```

Method 1: Remount EFS

1. Verify drives are mounted.
2. CD into the volume to see if files are attached to verify you have the full volume, with all your data.
3. Update internal DNS entries for Jobsub.
   1. Find the name entry, xxxxxxx, and double click on it to update with the new IP address. See Step 6 for details.

Method 2: EFS is already mounted

1. Verify drives are mounted.
2. CD into the volume to see if files are attached to verify you have the full volume, with all your data.

---

6. Update internal DNS entries for the Database

1. Once the restore is complete, log into the AWS Console and go to the EC2s to discover the IP address the newly restored server has been given.

2. Log into one of the domain controllers and open DNS. Find the name entry, `xxxxxxxxxxx`, and double click on it to update it with the new IP address.

---

7. Verify integrity of PortalGuard IDP (Database and Front End Webserver)

Portal Guard IDP

IIS Server - Configured on one Availability Zone (AZ) but is load-balanced. This will need DR steps. One method may be to point to our dev IDP which should be configured in another AZ and we can make DNS changes to allow our users to go through.

Database (Amazon RDS) - It is being replicated across two Availability Zones. Because of this replication, there are no recovery steps that are needed. You will login to Portal Guard on AZ2 and verify you can login and see the expected applications. This confirms the replication is working and Portal Guard is functional.

1. Log into PortalGuard.
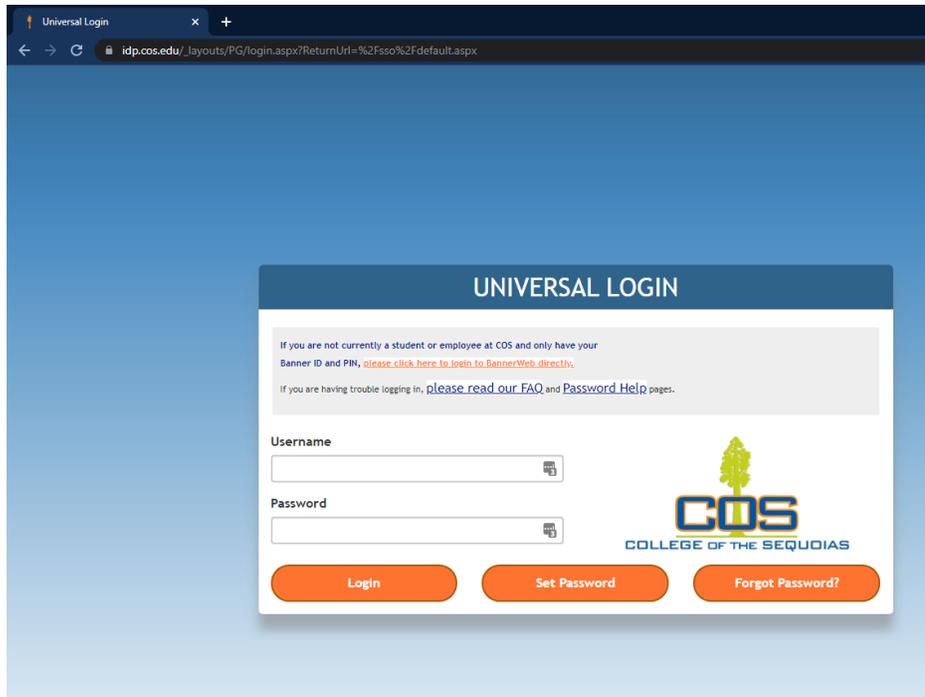
2. Verify the home screen shows all the expected applications. If all the expected applications are showing after you log in, you've verified the integrity of PortalGuard in the recovered site.
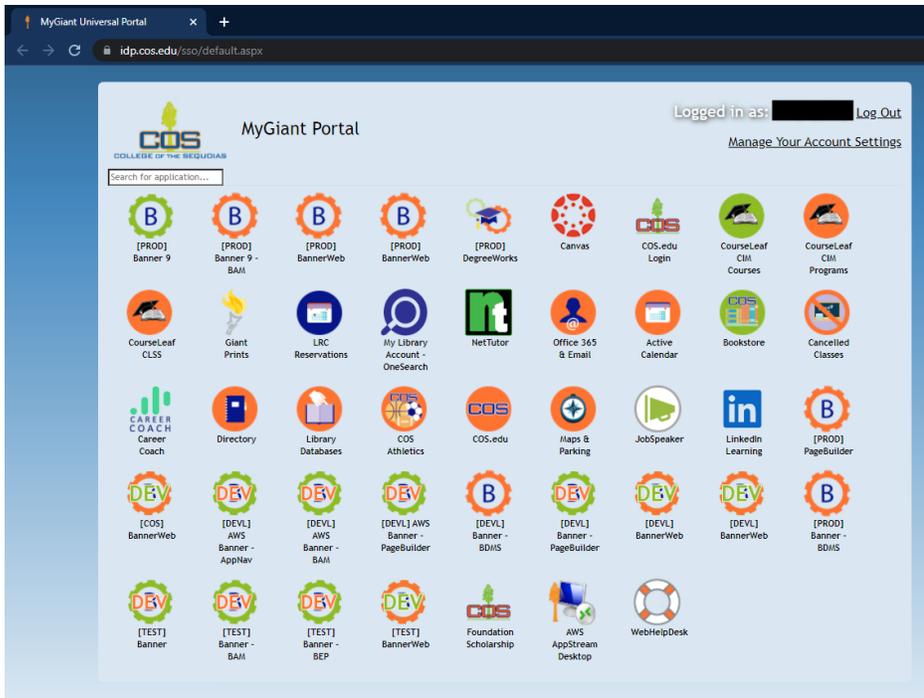
Return to Table of Contents

8. Verify ECS cluster is running and each application is functional

1. From the AWS console, navigate to **Elastic Container Service** in the **prod** account.
2. Verify the region is `Oregon` (or the correct DR region). Verify the `xxxxxxxxxx....` exists. You should see services and running tasks under **EC2**.

3. Open the `xxxxxxxx` cluster and verify all services. **Running task** counts should match **Desired task** counts.

4. Use this page to verify each application is available and functional: [Banner Environments](#) .

---

9. Recover reporting and integration EC2 server instances from Veeam backup

1. Banner component summary web page
2. Ensure the connection to SFTP is functioning after all the other servers come up.
    1. Login to the SFTP server to verify the share on the server. Confirm you can get access to these folders. If you can confirm a file is generated, it's working.
    2. Complete this step for each component listed below.

AIM

1. When the file is created from Oracle Database:

2. Where the scripts are located:

3. After the file was submitted:

Accudemia

1. When the file is created from Oracle Database:
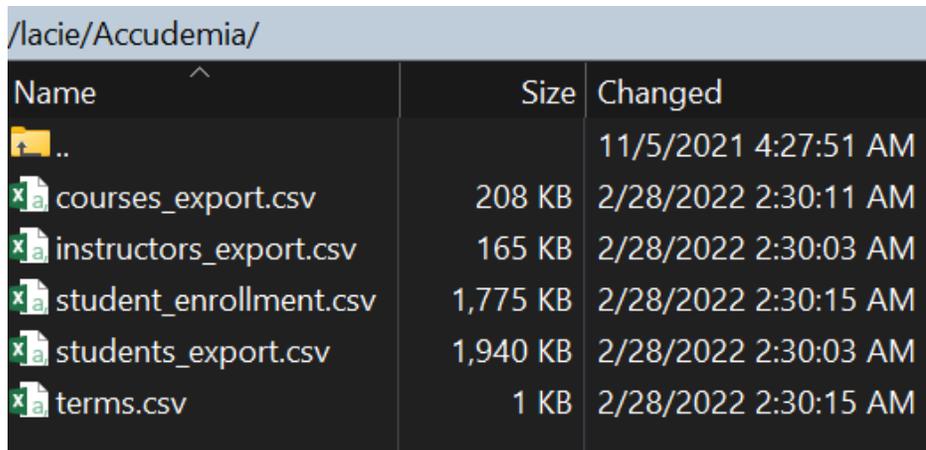
/lacie/Accudemia/		
Name	Size	Changed
..		11/5/2021 4:27:51 AM
courses_export.csv	208 KB	2/28/2022 2:30:11 AM
instructors_export.csv	165 KB	2/28/2022 2:30:03 AM
student_enrollment.csv	1,775 KB	2/28/2022 2:30:15 AM
students_export.csv	1,940 KB	2/28/2022 2:30:03 AM
terms.csv	1 KB	2/28/2022 2:30:15 AM

2. Where the scripts are located:

/u01/Accudemia/
Name
..
Archive
Logs
COS_Accudemia.sh
COS_Accudemia.sql
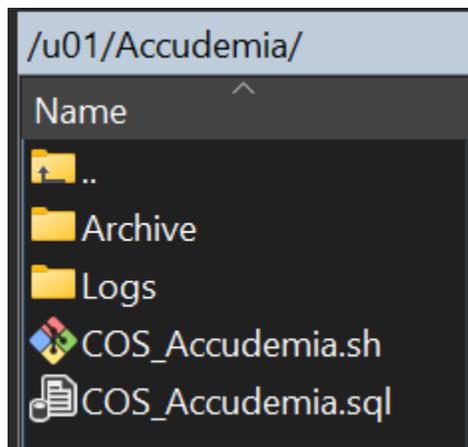
3. Make sure the data is being moved to the Accudemia server:

Name	Date modified
📁 from_Accudemia	1/11/2022 8:52 AM
📊 courses_export	2/28/2022 2:30 AM
📊 instructors_export	2/28/2022 2:30 AM
📊 student_enrollment	2/28/2022 2:30 AM
📊 students_export	2/28/2022 2:30 AM
📊 terms	2/28/2022 2:30 AM

Bankmobile

1. When the file is created from Oracle Database:
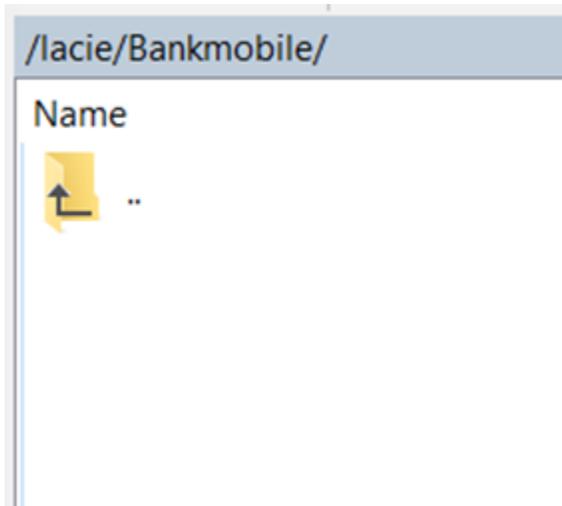
/lacie/Bankmobile/

Name

..

2. Where the scripts are located:

/u01/Bankmobile/

Name	Size	Changed
..		9/23/2021 9:08:20 AM
Sent		2/1/2022 10:00:08 AM
save		5/3/2021 5:35:40 PM
Logs		4/1/2017 10:00:01 AM
temp		3/10/2017 2:37:31 PM
cos_enrollment.shl	2 KB	8/27/2021 12:20:16 PM
CosTestToken.txt	1 KB	1/28/2020 2:02:16 PM
cos_enrollment.shl_orig	1 KB	3/10/2017 2:34:46 PM
EF_SFTP.cmd	1 KB	3/10/2017 8:51:08 AM
cos_enrollment.sql	1 KB	3/10/2017 8:34:10 AM

3. After the file was submitted:

/u01/Bankmobile/Sent/

Name	Size	Changed
..		2/1/2022 10:00:08 AM
COS202202011000.enr	483 KB	2/1/2022 10:00:03 AM

Cornerstone

1. When the file is created from Oracle Database:
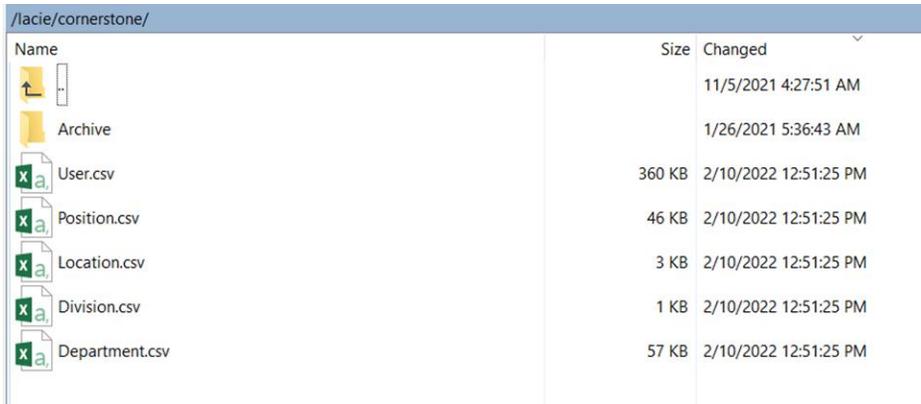
/lacie/cornerstone/		
Name	Size	Changed
↟ [..]		11/5/2021 4:27:51 AM
📁 Archive		1/26/2021 5:36:43 AM
📄 User.csv	360 KB	2/10/2022 12:51:25 PM
📄 Position.csv	46 KB	2/10/2022 12:51:25 PM
📄 Location.csv	3 KB	2/10/2022 12:51:25 PM
📄 Division.csv	1 KB	2/10/2022 12:51:25 PM
📄 Department.csv	57 KB	2/10/2022 12:51:25 PM

2. Where the scripts are located:

/u01/CornerStone/		
Name	Size	Changed
↟ [..]		9/23/2021 9:08:20 AM
📁 Archive		2/10/2022 11:00:09 AM
📁 Log		6/30/2020 12:09:44 PM
📁 Key		5/31/2019 2:35:17 PM
CS_Export.sh	3 KB	1/29/2021 5:16:05 AM
cos_cs_export.sql	1 KB	1/26/2021 5:43:16 AM
Control.sftp	1 KB	5/31/2019 4:26:05 PM

3. After the file was submitted:

/u01/CornerStone/Archive/		
Name	Size	Changed
↟ [..]		12/10/2021 5:11:40 AM
📁 02_10_2022		2/10/2022 11:00:09 AM

Maxient

1. When the file is created from Oracle Database:

/lacie/maxient/		
Name	Size	Changed
⬆ ..		11/5/2021 4:27:51 AM
COS_SCHEDULES_DATA.txt	3,882 KB	2/10/2022 1:12:23 PM
COS_DEMOGRAPHICS_DATA.txt	3,739 KB	2/10/2022 1:12:23 PM

2. Where the scripts are located:

/u01/Maxient/		
Name	Size	Changed
⬆ ..		9/23/2021 9:08:20 AM
Archive		2/10/2022 1:12:34 PM
Key		10/29/2019 11:43:04 AM
Log		8/21/2019 11:15:01 AM
Max_Export.sh	3 KB	2/2/2021 11:38:30 AM
rootACLs_09_03_2020.txt	44 KB	9/3/2020 10:31:21 AM
Control.sftp	1 KB	8/20/2019 10:08:29 AM
cos_max_export.sql	1 KB	7/1/2019 8:59:22 AM

3. After the file was submitted:

/u01/Maxient/Archive/		
Name	Size	Changed
⬆ ..		12/10/2021 5:34:33 AM
02_10_2022		2/10/2022 1:12:34 PM

Pyramed

1. When the file is created from Oracle Database:

/lacie/pyramed/		
Name	Size	Changed
..		11/5/2021 4:27:51 AM
Demographic.txt	2,332 KB	2/11/2022 4:05:07 AM

2. Where the scripts are located:

/u01/Pyramed/		
Name	Size	Changed
..		9/23/2021 9:08:20 AM
Archive		2/11/2022 4:05:09 AM
Logs		2/11/2022 4:05:01 AM
COS_Pyramed.sh	4 KB	9/29/2021 8:18:49 AM
COS_Pyramed.log	1 KB	9/24/2021 9:18:21 AM
COS_Pyramed.sql	1 KB	9/23/2021 10:42:38 AM

3. After the file was submitted:

/u01/Pyramed/Archive/		
Name	Size	Changed
..		11/10/2021 4:13:05 PM
2022_02_11-040501		2/11/2022 4:05:09 AM
2022_02_10_040501		2/10/2022 4:05:10 AM

---

10. Verify nightly processing jobs are working correctly

List of nightly jobs

Background

If you have a good backup of the cron tab file you should have all the information you need.

cron runs on the database server that is backed up nightly.

The nightly jobs generally run on the job sub servers.

Verification steps

If the cron tab file has the list of jobs, they should be recovered as part of the other recovery steps.

Verify the next day, in the logs, if the jobs ran.

Appendix D: Alternate Processing Procedures

This section identifies any alternate manual or technical processing procedures available that allow the business unit to continue some processing of information that would normally be done by the affected system. Examples of alternate processes include manual forms processing, input into workstations to store data until it can be uploaded and processed, or queuing of data input.

The Cumulus and COS teams have not identified any items for this section, but this section will stay intact in case it is needed in the future.

Appendix E: System Validation Test Plan

This appendix includes system acceptance procedures that are performed after the system has been recovered and prior to putting the system into full operation and returned to users. The system validation test plan may include the regression or functionality testing conducted prior to the implementation of a system upgrade or change.

For a list of testing personnel, see Appendix A.

Banner Functional User Testing Contacts

Banner Functional Testing Key Personnel		
Key Personnel	**Contact Information**	
[Banner-Evisions Reporting and Research Test Cases]		
	Work	
	Email	
	Work	
	Email	
[Banner File Transfer Inventory]		
	Work	
	Email	
	Work	
	Email	
	Work	
	Email	
	Work	
	Email	
	Work	
	Email	
[Banner Finance Test Cases]		
	Work	
	Email	
	Work	
	Email	
	Work	
	Email	
	Work	
	Email	

	Work	
	Email	
[Banner Financial Aid Test Cases](#)		
	Work	
	Email	
	Work	
	Email	
[Banner General-Technical Test Cases](#)		
	Work	
	Email	
	Work	
	Email	
	Work	
	Email	
	Work	
	Email	
	Work	
	Email	
	Work	
	Email	
	Work	
	Email	
	Phone	
	Email	
	Phone	
	Email	
[Banner Payroll-HR Test Cases](#)		
	Work	
	Email	

	Work	
	Email	
	Work	
	Email	
	Work	
	Email	
[Banner Self Service Test Cases]()		
	Work	
	Email	
	Work	
	Email	
	Work	
	Email	
	Work	
	Email	
	Work	
	Email	
	Work	
	Email	
[Banner Student Test Cases]()		
	Work	
	Email	
	Work	
	Email	
	Work	
	Email	
	Work	
	Email	
	Work	

	Email	
	Work	
	Email	

To edit the Banner Functional User Testing Key Personnel, go to [Appendix A](#) and update the child page. It will automatically update here.

Banner Functional User Testing Procedures

To view specific testing plans click on the test plan by module or system. Testing procedures will be used in the regular testing of the DRP as well as in the event of a disaster as part of the reconstitution phase.

Banner Test Plans

Test Plans by Module or System

- [Banner-Evisions Reporting and Research Test Cases](#)
- [Banner File Transfer Inventory](#)
- [Banner Finance Test Cases](#)
- [Banner Financial Aid Test Cases](#)
- [Banner General-Technical Test Cases](#)
- [Banner Payroll-HR Test Cases](#)
- [Banner Self Service Test Cases](#)
- [Banner SMTP Inventory](#)
- [Banner Student Test Cases](#)

Appendix F: Diagrams (System and Input/Output)

COS Banner AWS Architecture

Return to Table of Contents

Appendix G: AWS Resources Inventory

An inventory of AWS resources for the Banner system can be found here: [Banner System Inventory](#).

Appendix H: Interconnections Table

This appendix includes information on other systems that directly interconnect or exchange information with the system. Interconnection information should include the type of connection, information transferred, and contact person for that system.

Vendor/Project	Technical Contact	Source System	Destination System	Transfer Method	Scheduling Method	Scripts	

Return to Table of Contents

Appendix I: Test and Maintenance Schedule

The DRP should be reviewed and tested yearly or whenever there is a significant change to the system, for example any software upgrade. Be sure to review the DRP every time a software upgrade occurs, to ensure all the DR steps continue to be accurate.

A formal test plan is developed prior to the functional test, and test procedures are developed to include key sections of the DRP, including the following:

- Notification procedures
  - o Functional testers are notified by the DRP Directors through college email.
- System recovery on an alternate platform from backup media;
- Internal and external connectivity; and
- Reconstitution procedures.

Results of the test are documented in an After Action Report, and Lessons Learned are developed for updating information in the DRP. After Action Reports and Lessons Learned templates are available in Appendix L: Banner Disaster Recovery Functional Test Documentation.

Full functional tests of systems normally are failover tests to the DR site and may be very disruptive to system operations if not planned well. Other systems located in the same AZ may be affected by the full functional test. It is highly recommended that several functional tests be conducted and evaluated prior to conducting a full functional (failover) test.

Examples for functional tests that may be performed prior to a full functional test include:

- Full notification and response of key personnel to recovery location;
- Recovery of a server or database from backup media; and
- Setup and processing from a server at an alternate location.

Testing schedule

Step	Date Due by	Responsible Party	Date Scheduled	Date Held
Identify failover test facilitator.	March 1	DRP Coordinator		
Determine scope of failover test.	March 15	DRP Coordinator, Test Facilitator		
Develop failover test plan.	April 1	Test Facilitator		
Invite participants.	July 10	Test Facilitator		
Conduct functional test.	July 31	Test Facilitator, DRP Coordinator, POCs		
Finalize after action report and lessons learned.	August 15	DRP Coordinator		
Update DRP based on lessons learned.	September 15	DRP Coordinator		
Approve and distribute updated version of DRP.	September 30	DRP Director, DRP Coordinator		

Disaster Recovery credentials backups

As part of a yearly test, the DR team will need to export KeePass, where the disaster recovery credentials are stored, and import it to AZ2, ensuring the information is backed up to the cloud, since it is normally only available on-prem. In the event of a disaster where on-prem services are unavailable, the DR team will be able to access KeePass credentials on AZ2 to carry out the DR plan.

Export KeePass

Website instructions:

- The password list can be exported to various formats like TXT, HTML, XML and CSV.
- The XML output can be easily used in other applications.
- The HTML output uses cascading style sheets (CSS) to format the table, so you can easily change the layout.
- The CSV output is fully compatible with most other password safes like the commercial closed-source Password Keeper and the closed-source Password Agent, also the CSVs can be imported by spreadsheet applications like Microsofts Excel or OpenOffice's Calc.
- Many other file formats are supported through KeePass plugins.

Upload KeePass CSV on AZ2

The file is protected with the master password, so it should be kept in `kdbx` format.

Save and upload to an S3 bucket.

Appendix J: Business Impact Analysis

Ventura County Community College Ditrict has not completed a Business Impact Analysis.

The impact on the organization of an outage of the Banner system:

- Would result in significant loss of productivity, for administrative users as they rely on the system to do their job functions
- Would affect the ability to deliver services to students, as the Student module in Banner is used heavily by many departments, including Admissions and Records and Counseling
- Could result in the delay of financial aid to students due to the unavailability of the Financial Aid module
- During registration could potentially result in loss of revenue for the college due to lower enrollment

---

Appendix K: Banner Disaster Recovery Event Documentation

In the event of a disaster, document key information and steps taken. Create a new child page for each disaster event.

- [TEMPLATE: MM/DD/YYYY - Disaster recovery event](#)

TEMPLATE: MM/DD/YYYY - Disaster recovery event

In the event of a disaster, document key information and steps taken. Create a new child page for each disaster event.

- [Activation and Notification Phase](#)
  - [Activation](#)
  - [Notification](#)
  - [Outage Assessment](#)
    - [Assessment completed by: Enter name here](#)
    - [Expected recovery time: Enter time here](#)
- [Recovery Phase](#)
  - [Activity log](#)
  - [Communication log](#)
- [Reconstitution Phase](#)
  - [Validation](#)
  - [Test Plans by Module or System](#)
  - [Recovery Declaration and User Notification](#)
  - [Data Backup](#)
  - [Lessons learned documentation](#)
  - [After action report](#)
  - [Deactivation](#)

Activation and Notification Phase

Activation

Record the time and scope of the outage(s) resulting in an activation of the DRP.

Time of Outage	Affected systems	Reported by	Notes

Notification

Record the notifications sent out to inform the college contacts and students of the outage.

Time of Notification	Group Notified	Method of Notification	Notification performed by	Notes

Outage Assessment

Assessment completed by: *Enter name here*

Expected recovery time: *Enter time here*

Add the outage assessment here.

Include the extent of the disruption and any damage. Be sure to include how the cause of the outage was determined, if any additional disruption or damage was identified, and assessment of affected physical area(s); and determination of infrastructure status, resource functionality, and inventory. Note any items that will need to be replaced.

Recovery Phase

Activity log

Include recovery steps performed and by whom, the time the steps were initiated and completed, and any problems or concerns encountered while executing activities.

Date of disaster	Time of disaster	Recovery step	Recovery step performed by	Time step initiated	Time step completed	Problems or concerns	Additional notes

Communication log

Include any communication sent to college contacts or students regarding the progress of the DRP.

Time of Communication	Group Communication sent to	Communication summary	Method of Communication	Communication sent by

Reconstitution Phase

Validation

Validation Data Testing

Test and validate the recovered data to ensure that data files or databases have been recovered completely and that data is correct and up to date. Complete an assessment to confirm the time of the last transactions that were posted to determine if any data loss has occurred.

Time of Last Transaction	Type of Transaction	Data Loss (Y/N)	Performed by	Notes
Time of Last Transaction	Type of Transaction	Data Loss (Y/N)	Performed by	Notes

Validation Functionality Testing

Test Banner functionality with the Banner Functional Testing Key Personnel to verify the system is ready to return to normal operations. Document all testing steps taken in the tables below.

Detailed testing procedures are outlined in Appendix E: System Test Validation Plan.

Participants:

Name	Title	Role / Responsibilities

Document all the testing procedures taken and the results below for each module or system.

Banner Test Plans

Test Plans by Module or System

- [Banner-Evisions Reporting and Research Test Cases](#)
- [Banner File Transfer Inventory](#)
- [Banner Finance Test Cases](#)
- [Banner Financial Aid Test Cases](#)
- [Banner General-Technical Test Cases](#)
- [Banner Payroll-HR Test Cases](#)
- [Banner Self Service Test Cases](#)
- [Banner SMTP Inventory](#)
- [Banner Student Test Cases](#)

Add testing documentation here.

Recovery Declaration and User Notification

Upon successfully completing testing and validation, the DRP Director will formally declare recovery efforts complete, and that Banner is in normal operations.

Time of Notification	Group Notified	Method of Notification	Notification performed by	Notes

Data Backup

As soon as reasonable following recovery, the system should be fully backed up and a new copy of the current operational system stored for future recovery efforts. This full backup is then kept with other system backups.

Snapshot backups of the system will be used to conduct a full system backup.

Date and Time of Backup	Backup Performed by	Notes

Lessons learned documentation

Add lessons learned here.

After action report

Add after action report here.

Deactivation

Once all activities have been completed and the documentation has been updated, the DRP Director will formally deactivate the DRP recovery and reconstitution effort. Notification of this declaration will be provided to all business and technical points of contact through campus email.

Time of Notification	Group Notified	Method of Notification	Notification performed by	Notes

Appendix L: Banner Disaster Recovery Functional Test Documentation

Follow the testing plan in Appendix E and the testing schedule in Appendix I. Copy the testing plan into a child page and fill out a page each time a test is completed.

- TEMPLATE: MM/DD/YYYY - Disaster recovery functional test

TEMPLATE: MM/DD/YYYY - Disaster recovery functional test

- [Summary](#)
  - [MM/DD/YYYY TIME: Failover, restoring servers and databases](#)
  - [Participants:](#)
  - [Key points:](#)
  - [MM/DD/YYYY TIME: Functional user testing](#)
  - [Participants:](#)
  - [Functionality and data testing results](#)
- [Test Plans by Module or System](#)
- [Lessons learned and after-action report](#)

Summary

MM/DD/YYYY TIME: Failover, restoring servers and databases

Participants:

Name	Title	Role / Responsibilities

Key points:

Document the key points and issues that arise while testing the fail over of the systems to the disaster recovery servers.

MM/DD/YYYY TIME: Functional user testing

Participants:

Name	Title	Role / Responsibilities

Document the key points and issues that arise while testing the disaster recovery system.

Functionality and data testing results

Document all the testing procedures taken and the results below for each module or system.

Banner Test Plans

Test Plans by Module or System

- [Banner-Evisions Reporting and Research Test Cases](#)
- [Banner File Transfer Inventory](#)
- [Banner Finance Test Cases](#)
- [Banner Financial Aid Test Cases](#)
- [Banner General-Technical Test Cases](#)
- [Banner Payroll-HR Test Cases](#)
- [Banner Self Service Test Cases](#)
- [Banner SMTP Inventory](#)
- [Banner Student Test Cases](#)

Add testing documentation here.

Lessons learned and after-action report

Summarize the lessons learned from the test and outline actions that need to be taken after the test.

Appendix M: Version Info and Changes

Modifications made to this plan since the last printing are as follows:

Record of Changes			
Section	**Change Comment**	**Date of Change**	**Name of person making change**

Every time the cloud version of the DRP is updated, be sure to export a new backup PDF copy as well.

Return to Table of Contents

Jump to Appendix C: Detailed Recovery Procedures (Run Book)