**ITS Disaster Recovery Program**

University of Southern California Information Technology Services

[1. Executive Summary 2](#_Toc113438289)

[2. Business Value 3](#_Toc113438290)

[3. purpose & scope 3](#_Toc113438291)

[4. Overview of the Disaster Recovery Program 4](#_Toc113438292)

[4.1 Disaster Recovery Road Map 4](#_Toc113438293)

[4.2 USC Improvement Process: 4](#_Toc113438294)

[4.3 Downstream Process: 4](#_Toc113438295)

[4.4 Strategic Decisions: 5](#_Toc113438296)

[5. disaster planning team 5](#_Toc113438297)

[6. roles and responsibilities 6](#_Toc113438298)

[7. regulatory requirements 7](#_Toc113438299)

[8. DR Service Level matrix> also Cardinal red 8](#_Toc113438300)

[9. Disaster Recovery Strategy 8](#_Toc113438301)

[10. Backup Strategy 9](#_Toc113438302)

[10.1 Cohesity Cloudspin (Optional Add-on) 9](#_Toc113438303)

[10.2 Cohesity Runbook (Optional Add-on) 9](#_Toc113438304)

[10.3 Cohesity Cloud Edition – AWS 9](#_Toc113438305)

[11. Disaster Recovery Architecture 9](#_Toc113438306)

[12. Alternate DR Sites 11](#_Toc113438307)

[13. Subject Matter Experts 11](#_Toc113438308)

[14. Application and Dependency Mapping 11](#_Toc113438309)

[15. Recovery Procedures Development 12](#_Toc113438310)

[16. Recovery Validation & Functional Testing 12](#_Toc113438311)

[17. Application Recovery Lifecycle Management 12](#_Toc113438312)

[18. Vital Records 12](#_Toc113438313)

[19. Continuous Improvement 13](#_Toc113438314)

[20. Testing the IT Disaster Recovery Plan 13](#_Toc113438315)

[21. Reporting 13](#_Toc113438316)

[21.1 Risk Assessment 14](#_Toc113438317)

[21.2 Mitigation of Risks 14](#_Toc113438318)

[22. Troubleshooting and Resolution (Known Issues) Procedure Development 14](#_Toc113438319)

[23. Training 14](#_Toc113438320)

[23.1 Veoci 14](#_Toc113438321)

[23.2 FusionRM 14](#_Toc113438322)

[24. ITS Disaster Recovery as a Service (DRaaS) 15](#_Toc113438323)

[25. Failover (Actual Event) 17](#_Toc113438324)

[25.1 Incident Response (Event Occurs) 17](#_Toc113438325)

[25.2 Incident Communications 17](#_Toc113438326)

[25.3 Establishing the EOC 17](#_Toc113438327)

[25.4 Decision to Failover 17](#_Toc113438328)

[26. Roles 17](#_Toc113438329)

[26.1 Department Head / Alternate 17](#_Toc113438330)

[26.2 IT DRP Director / Alternate 17](#_Toc113438331)

[26.3 IT DRP Coordinator / Alternate 17](#_Toc113438332)

[26.4 Recovery Team 17](#_Toc113438333)

[27. Recovery of Applications and IT Services 17](#_Toc113438334)

[28. Fallback to Primary Site 18](#_Toc113438335)

[29. Table of Figures 18](#_Toc113438336)

[30. AppendiXs 19](#_Toc113438337)

[Appendix A: Documenting Recovery Procedures 19](#_Toc113438338)

[Example 19](#_Toc113438339)

[Procedure Group 20](#_Toc113438340)

[Appendix B: RACI – DAR Phase 2 20](#_Toc113438341)

[Appendix C: Training & Development 20](#_Toc113438342)

[Curriculum for ITS Senior Leadership 20](#_Toc113438343)

[Curriculum for ITS Directors, Managers & Staff 20](#_Toc113438344)

[Appendix D: Stakeholder Validation Testing 20](#_Toc113438345)

[Appendix E: Risk Assessment 20](#_Toc113438346)

[Appendix F: FusionRM and IT DRP Examples 20](#_Toc113438347)

# Executive Summary

The University of Southern California’s Information Technology Services (ITS) division has been participating in disaster recovery preparations and failovers since 2007. Documentation of manual recovery procedures and testing of capabilities in an out-of-state location is performed on an annual basis.

ITS is now entering a new phase of disaster recovery capabilities leveraging the university’s “Cloud Smart Initiative” as one of the cornerstones of the Digital Transformation strategic plan for ITS. Drivers for this project are from leadership and campus demand for ITS to advance and modernize our technology and reduce our data center footprint.

Making improvements to the technology is only one half of the strategy. The ITS Disaster Recovery Program seeks to bring awareness of the people, processes and tools needed to implement and maintain the lifecycle of IT Disaster Recovery.

# Business Value

The disaster recovery program is an essential function of the organization. If done correctly, it can prevent severe loss of data, which can have serious financial impact and damage to USC’s reputation. Loss of customer confidence and credibility may also occur and take years to reestablish.

Our goal is to accomplish the following:

* Significantly reduce restore times and lower Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). The new disaster recovery solution provides the ability to restore systems, services, and applications quicker than traditional backup solutions. Runbooks allow for automated failover to AWS, significantly lowering RTO and RPO for IT applications and services
* Minimize the interruption of critical IT services and safeguard university operations. A well-defined and implemented disaster recovery program will reduce possible interruptions and minimize loss to operations. By reducing restoration times of ITS systems, we can limit the losses, not only in terms of revenues, but also any impact to our ability to provide classes to students
* Define simplified processes to recover applications and IT services. A well-documented disaster recovery plan will have step-by-step processes to recover a service, regardless of whether the subject matter expert is available. Automating steps by consolidating many manual commands into a single program that can be executed by either the system at boot time or via a Cohesity runbook will simplify and speed up the recovery process
* Consistency across technologies. By incorporating the Cohesity runbook process into the design of the IT disaster recovery plan, ITS can quickly identify applications that can be easily converted to automated runbooks. The IT disaster recovery plan can then be updated to reflect the change in recovery procedures and reduced RTO/RPO

# purpose & scope

The objective of this plan is to ensure that USC can respond to a disaster or other emergency that affects information systems – and to minimize the effects of business operations.

# Overview of the Disaster Recovery Program

Working in conjunction with the Office of Fire, Safety and Emergency Planning, ITS performs yearly updates and testing of documented recovery steps to an out-of-state recovery site. With the new technology investments, we will move the recovery of ITS services to Amazon Web Services (AWS) cloud platform, replacing the SunGard data center in Arizona.

## 4.1 Disaster Recovery Road Map

Recovery Roadmap, Hardware Replacement, Basic backups and hosts in the cloud, Improve DR documentation, Failover via automation runbooks

Description automatically generated

Figure : IT Disaster Recovery Roadmap

## USC Improvement Process:

Improvement to the way USC (including ITS) documents its recovery procedures is critical to the success of the overall university’s ability to recover services. Soon, ITS will be moving away from Word documents or wiki pages for documenting recovery procedures. Leveraging FusionRM, ITS and other departments on campus will document their disaster recovery steps. Having a centralized repository of plans will allow the university to see relationships between services offered and downstream processes affected by an outage of that service.

## 4.3 Downstream Process:

The ability to see the downstream functions or processes may affect the previously defined amount of data loss acceptable by the university, otherwise known as Recovery Point Objectives (RPO) for an application. Recovery Time Objectives (RTO), the amount of time it takes to recover the application or service, may need to be revised. Inversely, the RTO/RPO of a function or process by a business unit may need to be changed to match the RTO/RPO of the application or IT service.

4.4 Strategic Decisions:

Strategic decisions have been made to establish appropriate disaster recovery RTO/RPO of a service or application, matches technology capabilities. Goals have been set to simplify, consolidate, and automate the current environment, and to rethink the approach to disaster recovery and backups, leveraging Cohesity runbooks for failover. ITS has considered the following:

* Simplifying the architecture of an application or service will increase the chance of a successful and timely failover to AWS
* Consolidating the infrastructure and backup solutions allow for resources to focus their time on making sure the environment and DR capabilities are running at peak efficiency
* The use of runbooks will allow the university to failover an application or service in the event the Subject Matter Experts (SMEs) are not available

These decisions also consider the Total Cost of Ownership (TCO) to develop and maintain the solution put in place to support the following tiers:

# disaster planning team

|  |  |
| --- | --- |
| **Planning Team Members** | |
| Administration | Policies, procedures, resources |
| IT | Business continuity, connectivity, information security issues |
| Human Resources | Staff contacts, training, |
| Communications | Internal and external, immediate and over time response |
| Facilities | Anything to do with the building and services to it |
| Content Managers | Print and digital, depending on the organization's records/assets |
| Operations Team | The Operations Team is entirely responsible for recovering assets like data centers and other important computer locations |
| Network | The Network Team manages all computer communications and networking protocols during a period of outage or disaster |
| Other (if required) | Other |

# roles and responsibilities

|  |  |
| --- | --- |
| **The following roles and responsibilities may apply to this document:** | |
| **Role** | **Responsibility** |
| Crisis Manager | The primary Crisis Manager, alternate Crisis Manager, or designee is responsible for directing the recovery of business operations and has full authority to make decisions related to recovery efforts. The Crisis Manager will be responsible for communications with the insurance provider. |
| Recovery Management Team | The Recovery Management Team members are responsible for implementing the portions of the Recovery Plan for their functional areas and are given authority to do so by the Crisis Manager. |
| IT Manager | The Information Technology Manager will implement the IT Systems Recovery program and maintain all IT operations. |
| Physical Plant Manager | The Physical Plant Manager will direct the reestablishment and maintenance of basic utility services (e.g., communications, water, electric, waste disposal) and ensure that critical equipment remains in service. |
| Media Relations Manager | The Media Relations Manager will establish and maintain contact with the news media and other organizations concerning disaster recovery operations. |
| Vendor/Contractor Manager | The Vendor/Contractor Manager will reestablish and maintain contact with vendors and contractors to provide supplies and services during recovery from a disaster. |
| Facility Security Manager | The Facility Security Manager will ensure that facility surveillance is maintained, prevent unauthorized entry to the facility, and maintain communications with government enforcement authorities as needed to protect employees and property. |
| Human Resources Manager | The Human Resources Manager will implement any changes or amendments to personnel policies during disaster recovery and administer personnel relocation or layoff programs. |
| Customer Service Manager | The Customer Service Manager will reestablish and sustain communications with customers and resume other customer services as soon as feasible. |
| Recovery Command Center Supplies Manager | The Command Center Supplies Manager will provide basic supplies and services for Command Center operations. |
| EHS Manager | The EHS Manager will ensure that appropriate safety programs are implemented to protect employees from workplace injuries and illnesses. The EHS Manager will also administer the disaster recovery training programs and the disaster recovery integrity test. |
| Suppliers and contractors | Suppliers and contractors who have agreed to provide supplies and services following a disaster or any major business disruption will perform work and provide materials and equipment necessary to return to normal operations. |
| Critical operations support staff. | Critical operations staff, which consists of key employees that are considered critical for the continuation of business operations after a disaster, will work together as a team to keep the business going during the recovery. |
| Operations Team | The Operations Team is entirely responsible for recovering assets like data centers and other important computer locations |

# regulatory requirements

Regulatory Requirements are strictly followed as it relates to the following ISO Standards:

|  |  |
| --- | --- |
| ISO 27001 | Requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS) [International Standard] |
| ISA 35.020: | Guidelines for Information Technology |
| ISO 14001 | Guidelines for environmental safety |
| ISO /IEC DIS 8183 | Guidelines for Artificial Intelligence – Data Life Cycle Framework |
| ISO/IEC TR 13233:1995 | Interpretation of accreditation requirements in ISO/IEC Guide 25 — Accreditation of Information Technology and Telecommunications testing laboratories for software and protocol testing services |
| ISO/IEC 17788:2014 | Cloud computing — Overview and vocabulary |
| ISO/IEC 24091:2019 | Power efficiency measurement specification for data center storage |
| ISO/IEC 27013:2021 | Cybersecurity and privacy protection |
| Other | Reference USC IT Regulatory Requirements for IT |

# DR Service Level matrix> also Cardinal red

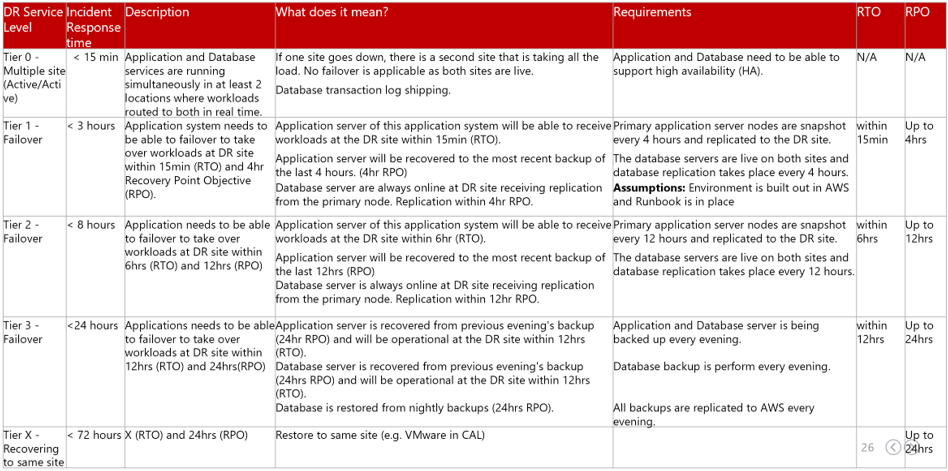


Figure : DR Service Level Tiers

These DR Service Level tiers also dictate the backup policy assigned to the servers hosting the services and applications. Defined success for the disaster recovery program is if the applications and services have the correct RTO/RPOs assigned, and ITS can meet customer expectations by performing successful failover and fallback to the original site that match those assigned RTO/RPOs.

# Disaster Recovery Strategy

In the event of an outage of the USC network and centrally managed USC information systems, ITS will be responsible for system recovery and will strive to have critical systems operational within 24 hours. ITS maintains several critical systems at the Arizona backup site and will coordinate restoration of systems to ensure the most critical university needs are met.

Recently, ITS has established a hybrid cloud model in AWS that can be activated to resume critical business systems if the CAL data center is unavailable. Leveraging state-of-the-art technology, ITS can back up virtual machines using Cohesity and restore them in AWS. Additionally, Cohesity runbooks can automate the failover process from USC to AWS with a push of a button.

For Student Information Systems (SIS), we are currently evaluating the functionality of the system on a virtualized Linux (x86) platform vs. a physical Solaris (SPARC) platform. Testing the replication of the new SIS virtual machine to AWS is also underway.

# Backup Strategy

Using Cohesity, ITS will perform nightly backups on all virtual servers hosted by ITS in the CAL datacenter. These “Protection Policies” (projection jobs) come in four different levels. Gold, Silver, Bronze, and Copper. These protection jobs provide the ability to restore the Operating System (VM Snapshot) back to a VMware host.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Level** | **Scope** | **Backup Cycle** | **Retention in CAL** | **Retention in AWS** |
| Gold | Tier 1 Production Servers | Every 4 hours | 14 days | 30 days |
| Silver | Tier 2 Production Servers | Every 8 hours | 14 days | 30 days |
| Bronze | Tier 3 Production Servers | Every 24 hours | 14 days | 30 days |
| Copper | Tier 4 or lower (test/dev servers) | Every 24 hours | 7 days | 30 days |

## 10.1 Cohesity Cloudspin (Optional Add-on)

For the ITS CAL virtual servers that need to be able to fail over and run in AWS, Cohesity CloudSpin will provide that backup and conversion into AWS EC2. Not available for the Copper backup level

## 10.2 Cohesity Runbook (Optional Add-on)

Cohesity Runbook provides the automation for executing a failover in a DR event. Cohesity Runbook contains the steps scripts, and commands to be issued to various environments to orchestrate each server’s failover steps. For example, making changes on DNS for specific server names or application URLs during a DR failover.

## 10.3 Cohesity Cloud Edition – AWS

Cohesity Cloud Edition is the same as the on-prem Cohesity, but physically located in AWS. This provides EC2 instance snapshots so EC2 instances can be restored back into an AWS Virtual Private Cloud (VPC) as needed. The protection levels are the same as CAL, but the main difference is the backup is only retained in AWS and will not be replicated to CAL.

# Disaster Recovery Architecture

The disaster recovery architecture in Amazon Web Services (AWS) consists of multiple Virtual Private Cloud (VPC) instances within the USWest2 region. Centralized services (firewall, DNS, NTP, and load balancers) will reside in the “Services” VPC. A VPC is a dedicated virtual network capable of supporting two hundred subnets, each customer or team will be assigned a VPC based on the server functionality and data classification using ITS’ standard nine-block zoning system.

* USWest2 – This AWS region consists of multiple availability zones (datacenters), each customer or team will have multiple VPCs spanned across multiple availability zones or regions for redundancy (depending on the application)
* VPN between AWS and campus terminates at the transit gateway (AWS service offering) in AWS and the border firewall on campus
* Centralized Palo Alto firewalls will provide firewall services and data security
* Centralized Firewalls and Load Balancers for communications between VPCs
* The Cohesity backup system has its own VPC within AWS
* The nine-block zoning system will exist in AWS like what is in the primary network

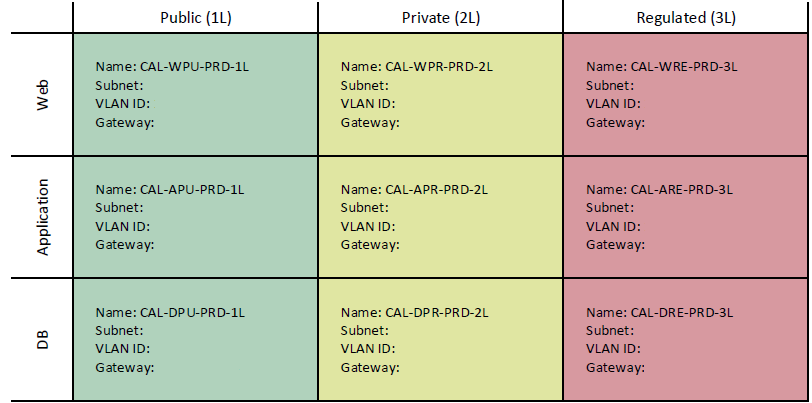


Figure : Nine-Block Zoning System Example (Redacted)

* Future state
* Network Time Protocol (NTP) – Architecture (TBD - most likely on DNS servers but sync with AWS NTP servers)
* Virtual Private Networking (VPN) – Scope (TBD- most likely for management only)

Diagram

Description automatically generated with medium confidence

Figure : Trojan Cloud High Level View

# Alternate DR Sites

Additionally, ITS has established a reciprocal agreement with Clemson University, located in South Carolina. The Clemson datacenter is a cold site for the Center for Advanced Research Computing (CARC). A second hosting services agreement with shared cost has been established by the Shoah Foundation’s Visual History Institute teams and the Library Digital Repositories for disaster recovery.

# Subject Matter Experts

Understanding who the Subject Matter Experts (SME) are for an application or service is very important to the success of the university’s ability to failover applications and IT services. There should be a minimum of two SMEs per application. This helps minimize the risk of losing the knowledge of the application or service if one of those resources is unavailable or leaves the university. The SMEs will be instrumental in establishing the procedures for proper failover. A properly built disaster recovery plan for an application will allow for a failover without the SMEs intervention.

# Application and Dependency Mapping

How an application works and how it communicates with other applications or servers is key to being able to perform a successful failover to another site. Ideally, when the application is built, everything is documented. However, there are many factors that can affect the accuracy of the data. Tight deadlines, changes made to the application or personnel over time, or a failure to document a key dependency, can affect the ability to successfully failover. All applications that make up an IT service should have the same RTO/RPO to ensure customer expectations for all facets of the IT service are consistent.

Dependencies on other IT services and the RTO/RPO assigned to them are important and may influence the RTO/RPO for your application or IT service.

There are discovery capabilities built into monitoring tools or ServiceNow that can help validate existing dependency documentation or identify if there are gaps. Another source for some of this information, especially for older applications, are the logs from the network firewall closest to the servers that support the application. The firewall will capture all traffic in and out of the VLAN and ports utilized. Traffic within the VLAN will be unknown, but that narrows the scope of troubleshooting.

Understanding dependencies that your application has on other services is important. By documenting these dependencies, it allows recovery teams to identify the order of recovery for applications. When documenting applications in FusionRM for the IT disaster recovery plan, it is possible to associate dependencies for applications.

# Recovery Procedures Development

Recovery procedures and steps are the blueprint for either a successful or disastrous failover of an application or IT service. Relying on specific people or documentation residing in disparate systems to recover applications and IT services is not a recommended approach. Instead, the SMEs for the application or IT service should document the recovery procedures in a way where anyone can pick up the IT disaster recovery plan and recover the application or IT service. Simplified processes and structured recovery procedures and steps are key. For example, instead of having to issue multiple commands manually, is it possible to automate those processes? An assessment to determine recovery priorities for the various applications and IT services will need to be performed. For additional information, see *Appendix A: Documenting Recovery Procedures*.

# Recovery Validation & Functional Testing

The defined recovery procedures should contain verification steps so the university can verify the application or IT service has been recovered correctly. Ideally, these validation steps will be built into the recovery procedures and steps. Reference *Appendix A: Documenting Recovery Procedures*. Additionally, key stakeholders from the various business units will need to perform functional testing of applications following a failover. These stakeholders will be required to document each validation step they performed and result. For tests that failed, the stakeholder needs to provide a risk assessment and impact analysis.

# Application Recovery Lifecycle Management

Whenever changes to production are made, it is possible that the change may affect recovery procedures. If the change to production alters the way the application starts up, then the IT disaster recovery documentation needs to be modified to account for the change in procedure. Any new component that is introduced (API, server, application, firewall rule changes, dependency, etc.) can also alert the way the application performs in production, versus a failover to a different site. Ideally, teams will incorporate the documentation of what changed in production to the IT disaster recovery procedures as well.

# Vital Records

Vital records such as contracts, Service Level Agreements (SLA), and contact lists should be in the IT disaster recovery plan. Failure to document service level agreements with third party service providers may result in an inability to restore systems according to business requirements. By uploading vital records into the IT disaster recovery plan, the department can understand what agreements they have in place and communicate more efficiently with vendors during an event.

# Continuous Improvement

Continuous training and testing of the recovery procedures, validation of results, risk assessments and mitigation are important for the organization to successfully respond to incidents that impact production services.

Diagram

Description automatically generated

Figure : Continuous Improvement

# Testing the IT Disaster Recovery Plan

Testing of IT disaster recovery procedures is required by the university. By testing the recovery of applications and IT services, the university can determine if the documented procedures are sufficient, or if there are gaps that need to be addressed. Over time, the recovery process will be easier for the staff since they will have practiced the failover procedures.

Following the test of the failover process, a team of key stakeholders should then test the application to ensure that it is working as expected from the alternate site. Documented tests and results should be turned in to the recovery team and a debrief with participants should be performed. Reference *Appendix D: Stakeholder Validation Testing* for an example form that should be completed by stakeholders during the testing phase.

# Reporting

On an annual basis, the university requires proof of testing for each department’s IT Disaster Recovery Plan. The Department of Fire, Safety and Emergency Planning will send out the Debrief and Results exercise form with a reference to where to upload the document upon completion. Departments are expected to perform failovers or tests to ensure their plans and procedures work as expected and to document results. Finally, a written evaluation of the test (Debrief and Results Form) must be submitted to USC Fire, Safety, and Emergency Planning.

## 21.1 Risk Assessment

After every test or failover of an application or IT service, an assessment of the overall process and results needs to be performed. Leveraging the stakeholder validation forms and any notes documented during the failover process, perform an assessment of what went well and where challenges occurred. Reference *Appendix D: Stakeholder Validation Testing* for an example form that must be completed by stakeholders during the testing phase.

A plan to mitigate the identified risks will need to be built, including any potential costs. Refer to *Appendix E: Risk Assessment*.

## 21.2 Mitigation of Risks

Once risks have been identified, the plan to remove or reduce the risk must be executed. Alternatively, the department leadership may choose to accept the risk. Determining factors would be if part of the application or service is outside of our control, costs, complexity of the mitigation, etc. If the department leadership (ACIO or higher), chooses to accept the risk, the risk and decision should be fully documented in the IT disaster recovery plan. See *Appendix A: Documenting Recovery Procedures* for where the “accepted risk” would be inserted into the document.

# Troubleshooting and Resolution (Known Issues) Procedure Development

Even the best documented procedures can result in issues after a failover. It is recommended to establish a set of common troubleshooting techniques for your application or IT service. This documentation should be updated after every attempt to failover or fallback an application or IT service. This will help the university understand how to identify and resolve potential issues.

Leveraging knowledge from any troubleshooting and resolution during a Priority 1 outage including an After-Action-Report would benefit the failover and future incident recovery procedures. Reference *Appendix A: Documenting Recovery Procedures*.

# Training

Recurring training of the various phases of IT disaster recovery is important for teams to be in sync when a real disaster scenario occurs. A formal training curriculum will be built and enforced to help ensure readiness in a major incident or disaster. Training for the software platforms Veoci, incident response preparedness and FusionRM (described below) will also occur. Reference *Appendix C: Training and Development* to see the training curriculum and frequency.

## 23.1 Veoci

Veoci ([www.veoci.com](http://www.veoci.com)) allows for effective communication during crisis management and emergency response. This software allows USC to have a virtual Emergency Operations Center (EOC) for USC’s Senior Leadership to meet and discuss major events affecting the university. Departments are also able to update status of staff safety and accountability, buildings, services, etc. Prior to the purchase of Veoci, USC Senior Leadership would convene at Tudor Campus Center (EOC primary location) or use Zoom. Unlike Zoom, Veoci can retain what was discussed in chat and it can be revisited when the EOC reconvenes.

## 23.2 FusionRM

FusionRM ([www.fusionrm.com](http://www.fusionrm.com)) is a risk management software solution used as a centralized repository for the USC Business Impact Analysis (BIA), Business Continuity (BCP), and IT Disaster Recovery plans (ITDRP). It allows the university to gain better insight into application dependencies, risks, and recovery strategies. The IT disaster recovery plan in FusionRM was designed to assist with identifying applications and IT services that may be easily converted to the ITS Disaster Recovery as a Service (DRaaS) model. Refer to *Appendix A: Documenting Recovery Procedures*.

# ITS Disaster Recovery as a Service (DRaaS)

The university has become an always-on, information-driven organization, and depends on IT infrastructures that are available 24/7. The cost of downtime is a negative student experience and potential loss of revenue to the university. Data loss can be caused by natural disasters, software issues, power outages, hardware failure and user errors, but recently there has been a huge spike in cybersecurity-related disasters. Therefore, extensive security and business continuity strategies including a disaster recovery solution, are crucial for USC.

Not all IT departments across the university have the resources (financial, knowledge, or staffing) to fully implement a working disaster recovery solution. The ITS DRaaS solution is a robust, flexible, and cost-effective cloud-based disaster recovery solution that offers end-to-end protection for systems and applications. Leveraging state-of-the-art technology, ITS can backup virtual machines using Cohesity and restore them in AWS. Additionally, Cohesity runbooks can be leveraged to automate the failover process from USC to AWS with a push of a button.

When creating the template for the USC IT Disaster Recovery Plan in FusionRM, the ITS DRaaS solution was considered, and it was structured in a way that when completed properly, can be easily converted to Cohesity runbooks. Reference *Appendix A: Documenting Recovery Procedures* for more details.

*(<insert>) <Add Catalog of service offerings)>*

*(<insert>) <Add context regarding ITS SLA’s>*

Once a customer commits to the IT DRaaS, a series of meetings may be required depending on the quality of the customer’s existing IT disaster recovery plan and needs. If the customer’s IT disaster recovery plan meets the criteria for the existing Cohesity design, runbooks will be created for those servers. If they do not meet the criteria, additional meetings with the customer will take place to discuss new requirements and recovery steps. Those new steps would then be converted into runbooks and documented in the customer’s IT disaster recovery plan. Reference *Figure 7: Customer Request - New Server(s)/Application(s) Workflow* below.



Figure 6: Customer Request - New Server(s)/Application(s) Workflow

For ITS teams, the responsibility assignment matrix is defined in *Appendix B: RACI – DAR Phase 2.*

# Failover (Actual Event)

The decision to failover ITS systems and applications will be made by an ACIO or higher position within ITS. This decision will be made after a thorough assessment and input from various ITS leaders.

*Re-Format failover Events Overview for visual clarity*

Failover Events Overview graphic

Description automatically generated

Figure : Failover Events Overview

## 25.1 Incident Response (Event Occurs)

When an event of any kind (i.e., application down) occurs, typically the first step taken by ITS is to determine the severity of the incident based on impact and urgency. The priority matrix listed below is a guide to help understand impact and urgency.

Graphical user interface

Description automatically generated with medium confidence

Figure 8: Incident Priority Reference Guide

If the incident has a high urgency to resolve and impacts a significant number of customers (Critical Priority), a Priority 1 (P1) major incident response bridge is established by the ITS Operations Center (OC) and all ITS Infrastructure Services Directors and ACIO are called to the bridge, in addition to the on-call staff for the service that is affected.

During this bridge, an assessment is made, and the team troubleshoots and resolves the incident as quickly as possible.

## 25.2 Incident Communications

Notifications to the ITS Leadership, Opt-in Faculty and staff, and University Technology Council members (IT leaders across USC) occur via the mass notification system Blackboard Connect. These stakeholders are kept apprised of the situation via an hourly established cadence.

Table

Description automatically generated

Figure 9: Incident Communications Matrix

## 25.3 Establishing the EOC

If the incident is more severe, then simultaneously to the P1 bridge described above, the university will activate the USC Emergency Operations Center (EOC) leveraging the Veoci virtual EOC software to bring the university’s senior leadership team into a separate bridge with ITS senior leadership to assess the impact and determine next steps. This leadership team will then decide to monitor the situation while the localized incident is being resolved or declare an emergency for parts of, or potentially, the entire university.

## 25.4 Decision to Failover

If a prolonged outage is expected and the decision to failover has been made, ITS will begin the failover process to AWS. Depending on the scope, it could be one application or all DR capable ITS services.

# Roles

There are defined roles that will help ITS manage the disaster/failover:

## 26.1 Department Head / Alternate

* Currently assigned to the CIO / ACIO
* Has overall responsibility of the unit
* Authorized to declare disasters and authorizes recovery operations to the remote site
* Will participate in EOC discussions

## 26.2 IT DRP Director / Alternate

* Currently assigned to the Director of Data Center, Operations Center and DR / Director of Platform Services
* Declares activation of the ITS Disaster Recovery Plan
* Oversees the process and provides updates to the Department Head or Alternate

## 26.3 IT DRP Coordinator / Alternate

* Currently assigned to the Manager of Data Center and Operations Center / Manager of Platform Services
* Upon approval, activates the remote site
* Monitors recovery team activities until services are fully recovered
* Ensures that recovery operations are performed consistent with SLAs
* Provides status updates to the IT DRP Director or Alternate

## 26.4 Recovery Team

* Currently assigned to all ITS teams required to recover the affected service(s)
* Prioritizes the sequence of the failover to AWS
* Performs all system recovery and resumption activities
* Validates that the application(s) and service(s) are functional

# Recovery of Applications and IT Services

Utilizing the IT Disaster Recovery plan, perform recovery procedures to bring applications and IT services online at an alternate site. If a step fails or is not accurate, notes should be taken so that recovery step can be corrected. The notes should be turned in as part of the risk assessment process described above. Following the failover process, a team of key stakeholders should then test the application to ensure that it is working as expected from the alternate site prior to releasing the application to the general population.

Documented application tests and results should be turned in to the team and a debrief of participants should be performed. Reference *Appendix D: Stakeholder Validation Testing* for an example form that should be completed by stakeholders during the testing phase.

# Fallback to Primary Site

Once the issue with the primary site is resolved, then the same process will be used to bring services back to the primary site, but at a scheduled time that is convenient for the university. There is a possibility that an application will remain in AWS. If this occurs, updates to the ITS DR document must be made with new recovery procedures (i.e., multiple availability zones).

# Table of Figures

[Figure 1: IT Disaster Recovery Roadmap 7](#_Toc112421660)

[Figure 2: DR Service Level Tiers 8](#_Toc112421661)

[Figure 3: Nine-Block Zoning System Example (Redacted) 10](#_Toc112421662)

[Figure 4: Trojan Cloud High Level View 11](#_Toc112421663)

[Figure 5: Continuous Improvement 13](#_Toc112421664)

[Figure 6: Customer Request - New Server(s)/Application(s) Workflow 17](#_Toc112421665)

[Figure 7: Failover Events Overview 18](#_Toc112421666)

[Figure 8: Incident Priority Reference Guide 18](#_Toc112421667)

[Figure 9: Incident Communications Matrix 19](#_Toc112421668)

[Figure 10: Example IT Service Diagram 25](#_Toc112421669)

[Figure 11: Example Cohesity Runbook based on Recovery Procedures 28](#_Toc112421670)

[Figure 12: Example FusionRM Procedure Group 38](#_Toc112421671)

[Figure 13: Example FusionRM Procedure (Recovery) 39](#_Toc112421672)

[Figure 14: Example FusionRM Procedure (Accepted Risk) 40](#_Toc112421673)

[Figure 15: Example FusionRM Procedure Step (Accepted Risk) 40](#_Toc112421674)

[Figure 16: Example FusionRM PDF IT DRP (Shows Procedure Group and Procedure) 41](#_Toc112421675)

[Figure 17: Example FusionRM IT DRP (Shows Procedure Steps and New Procedure) 42](#_Toc112421676)

[Figure 18: Example FusionRM IT DRP (Shows Validation Procedure) 43](#_Toc112421677)

# list of AppendiX

## Appendix A: Documenting Recovery Procedures

Documenting your recovery steps in a thorough but concise way will help the organization identify which applications or IT services can be automated easily, and which ones need to be re-architected to accommodate disaster recovery failovers.

With FusionRM, we are looking to add consistency to the recovery procedures. IT DR recovery procedures will be broken out into “Procedure Groups,” “Procedures,” and “Procedure Steps.”

**Procedure Groups**

* + Use Procedure Groups to give a high-level overview of the IT service that the application is supporting. A diagram of the service and brief description is all that is needed here.

**Procedures** (All procedures groups (above) should have at least one procedure)

* + Use Procedures for the following:
    - Recovery Procedures
      * Each of the applications supporting the IT service, including diagrams of the application. This is where you would want to identify SMEs for the application
    - A testing and validation section for each application
    - A troubleshooting section for each application
    - Accepted risks determined by the department (each acceptable risk should be separate)
    - Ransomware (Future State, not in production yet)

**Procedure Steps** (All procedures (above) should have at least one step)

* + Use Procedure steps to document the recovery procedures for the application
  + In the testing and validation procedure, these would be the steps to test the application following the recovery of the application to AWS
  + In the troubleshooting section, these would be the scenario and triage steps
  + In the accepted risks section, these would be the step that you expect an issue, and the supporting statements
  + In the ransomware section, these would be the steps to take in the event of a ransomware attack on your application

Leveraging the information above, let us build an example.

**Example**

*Scenario:* An IT service named Rockin’ Trojans, it consists of two applications, one of which is a dependency and is not in our control. The other has a database server, application server, an application user interface server.

Using this scenario, we will create one “Procedure Group” to describe the IT service, then four “Procedures,” one for checking the dependency, one for the application, one for testing the application, and finally a troubleshooting procedure. Each procedure will have one or more steps.

### Procedure Group

**Name:** Rockin’ Trojans Service

**Description:** This service allows Trojans of all ages to show off their garage band’s talent

#### Procedure

**Number:** Procedure 1.01

**Name:** Recover rockintrojans application

**Description:** Recovery of the main application for the Rockin’ Trojans IT Service

**Diagram of the service:**

Example Diagram for an IT service

Description automatically generated

Figure 10: Example IT Service Diagram

##### Procedure Steps

**Number:** Step 1.0

**Name:** Recover the Application Database VM

**Description:** These are the recovery steps for the Database server. If this recovery is okay, then proceed to the next step

1. Recover/Restore the Database VM (rt-db-prod) to secondary site
2. All necessary services will start up automatically on boot

**Number:** Step 2.0

**Name:** Recover the Application VM

**Description:** These are the recovery steps for the Application server. If this recovery is okay, then proceed to the next step

1. Recover/Restore the Application VM (rt-app-prod) to secondary site
2. All necessary services will start up automatically on boot

**Number:** Step 3.0

**Name:** Recover the Application User Interface VM

**Description:** These are the recovery steps for the Application User Interface server. If this recovery is okay, then proceed to the next step

1. Recover/Restore the Application User Interface VM (rt-ux-app-prod) to secondary site
2. Issue **sudo /opt/local/wordpress.sh -e conf -s /etc /etc/hosts &** to start up the application.

#### Procedure

**Number:** Procedure 1.02

**Name:** [Accepted Risk] Validate that SC-rocks.usc.edu is available

**Description:** There is a dependency on this service, if it is down, then parts of my application does not work correctly, but is not a hard dependency.

##### Procedure Steps

**Number:** Step 1.0

**Name:** Test connection to sc-rocks.usc.edu

**Description:** Regardless of if this test is successful, it is okay to start up our servers

1. This risk was accepted by the department’s ACIO (Jane Doe) on 05/04/2021 since this host belongs to another department.
2. Use a web browser and go to <https://sc-rocks.example.usc.edu/api>

#### Procedure

**Number:** Procedure 1.03

**Name:** [Validation] Validate that my IT service rockintrojans.usc.edu is available

**Description:** Used to test if the service is working as expected.

##### Procedure Steps

**Number:** Step 1.0

**Name:** Test connection to rockintrojans.usc.edu

**Description:** Just a web browser test

1. Use a web browser and go to <https://rockintrojans.example.usc.edu>
2. View content on the page, does it match what the site normally looks like?
3. Click Add my band
4. Fill out the form and submit for review
5. Log in to Admin Portal and view the submitted form
6. Exit Admin Portal
7. Click link in upper left corner for Famous Trojans (Connects to sc-rocks.usc.edu API and displays content on our page)
8. End of testing

#### Procedure

**Number:** Procedure 1.04

**Name:** [Troubleshooting] This application or IT Service

**Description:** Troubleshooting this service

##### Procedure Steps

**Number:** Step 1.0

**Name:** Connection to sc-rocks.usc.edu fails

**Description:** If this test is not successful, it is okay to start up our servers

1. Use a web browser and go to <https://sc-rocks.example.usc.edu/api>
2. If this test still fails, contact the administrator for that application: [gary@example.usc.edu](mailto:gary@example.usc.edu)

**Number:** Step 2.0

**Name:** Connection to rockintrojans.usc.edu fails

**Description:** Check servers for basic connectivity

1. Open a command window, and type in ping rock-prd1.example.usc.edu
2. Using the same window, type in ping rock-app-ui-prd1.example.usc.edu
3. Using the same window, type in ping rockdb-prd1.example.usc.edu
4. Etc.

To see these steps in FusionRM and associated IT Disaster Recovery Plan, reference *Appendix F: FusionRM and IT DRP examples*. Additionally, based on what we see in the procedures above, we can build an automated runbook to failover the VMs to AWS. The items on the left are the Cohesity runbook steps, the items on the right are the steps defined in “Procedure 1.01” above.

Associating Recovery Steps into Cohesity Runbooks, diagram

Description automatically generated with medium confidence

Figure 11: Example Cohesity Runbook based on Recovery Procedures

## Appendix B: RACI – DAR Phase 2

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Accountable (A)** = Carries the “yes” or “no” authority and has full veto power for an activity. Only one “A” can be assigned to a task or activity, and authority must accompany accountability | | | | | | | | |
|  | **Responsible (R)** = Completes the task/activity and are responsible for action/roll-out. Responsibility is often shared, with each individual’s degree of responsibility determined by the individual with the “A” | | | | | | | | |
|  | **Support (S)** = Provides resources or data in support of the activity. There can multiple “S” | | | | | | | | |
|  | **Consulted (C)** = Consulted prior to a final decision or action being taken. Implies two-way communication | | | | | | | | |
| **Informed (I)** = Informed after a decision or action is taken. Implies “FYI” and only one-way communication | | **ACIO - Susan** | **Platform Dr - Nick** | **Data Center Dr - Lou** | **Platform Service team** | **Data Center team** | **BC/ DR Program Mgr.** | **Operations Center** | **Networking** |
| **Activity** | |
| Vision | | A | R | R | I |  | I | I | I |
| Strategy | | A | R | R | C |  | C | I | I |
| Change controls/Standards | | A | R | R | R |  | R | S | R |
| Financial | | A | R | R | I |  | I | I | I |
|  | |  |  |  |  |  |  |  |  |
| **Post implementation support** | |  |  |  |  |  |  |  |  |
| DR Event - (In a disaster. Only an ACIO or higher can make the decision to failover) | | A | R | R | R | S | S | S | S |
| Run book - updates | |  | A | S | R |  | S |  |  |
| Patching - Cohesity software (DC Team puts a ticket into Cohesity to patch) | |  | A | R | C | R |  |  |  |
| Customer Facing - provide service (BC/DR program manager) | |  | C | A | C |  | R |  | C |
| Build and tech Design DR (new customer)- Onboarding new services | |  | A | C | R |  | C |  | S |
| Oversee Disaster Recovery Document updates & failover testing | |  | R | A | S | S | R | S | R |
| Backups of servers | |  | A |  | R | S |  |  |  |
| Restore (operational) | |  | A |  | R | S |  |  |  |
| Non-platform hosted devices backup related DR requests - DR as a service | |  | A | S | R |  | S |  |  |
| Update/maintain standards - DR policies | |  | S | A | S |  | R |  | S |

## Appendix C: Training & Development

**Curriculum for ITS Senior Leadership**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Course Title | Description | Est. Duration | Type of Course | Interval |
| Disaster Recovery Program Overview | Overview of the IT Disaster Recovery Program. What it is, why it is important | 1 Hour | In-person / Virtual | Annual |
| Emergency Operations Center | Overview of the Emergency Operations Center, tabletop exercises | 1 Hour | In-person / Virtual | Bi-annual |
| Department Operations Center | Overview of the Department Operations Center, tabletop exercises | 1 Hour | In-person / Virtual | Bi-annual |
| Incident Response & Disaster Recovery | Overview of the overall process, what is expected, tabletop exercises | 1 Hour | In-person / Virtual | Bi-annual |
| Ransomware Incident Management | Overview of the process, what is expected, tabletop exercises. (In conjunction with ITS Security Operations) | 1 Hour | In-person / Virtual | Bi-annual |
| Introduction to Veoci virtual EOC | Overview of the product, how to login, tabletop exercises | 1 Hour | In-person / Virtual | Bi-annual |
| Advanced Veoci | Overview of the more advanced features, how to populate areas of the tool during a university wide event | 1 Hour | In-person / Virtual | Bi-annual |
| Disaster Recovery Plan updates in FusionRM | Overview of the product. How to login, make updates and generate a PDF copy | 1 Hour | In-person / Virtual | Annual |

**Curriculum for ITS Directors, Managers & Staff**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Course Title | Description | Est. Duration | Type of Course | Interval |
| Disaster Recovery Program Overview | Overview of the IT Disaster Recovery Program. What it is, why it is important | 1 Hour | In-person / Virtual | Annual |
| Emergency Operations Center Overview | Overview of the Emergency Operations Center, what it is, why is it important | 30 Mins | In-person / Virtual | Bi-Annual |
| Department Operations Center | Overview of the Department Operations Center, tabletop exercises | 1 Hour | In-person / Virtual | Bi-Annual |
| Incident Management & Disaster Recovery | Overview of the overall process, what is expected, tabletop exercises | 1 Hour | In-person / Virtual | Bi-Annual |
| Ransomware Incident Management | Overview of the process, what is expected, tabletop exercises. (In conjunction with ITS Security Operations) | 1 Hour | In-person / Virtual | Bi-Annual |
| Disaster Recovery Plan updates in FusionRM | Overview of the product. How to login, make updates and generate a PDF copy | 1 Hour | In-person / Virtual | Annual |

## Appendix D: Stakeholder Validation Testing

IT Application Name: FusionRM

Tester Name: John Doe

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test Name  (Application, link, etc) | Result | Additional Information | Est. Duration | Impact or Priority |
| [Example] Generate PDF from FusionRM for Sample-IT DR Plan | Partially Successful | PDF generated successfully, but some data is missing from the PDF plan. Especially, recovery steps. | 2 min | Critical |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

IT Application Name: xyz

Tester Name: Jane Doe

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test Name  (Application, link, etc) | Result | Additional Information | Est. Duration | Impact or Priority |
| [Example] Startup procedure did not function properly | Workaround implemented | Manually started up the application. Startup script failed, and website shows HTTP 500 error | 12 min | Critical |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Appendix E: Risk Assessment

Below is just a sample of a risk assessment

IT Application Name: FusionRM

Assessment Performed by: Jim Dean

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Possible Risk | Reported by | Priority | Additional Information | Remediation Plan | Cost | Start | End |
| [Example] Generate PDF from FusionRM for Sample-IT DR Plan | John Doe | High | The plan is not up to date and key information on application recovery steps is missing | Talk to the SMEs, allocate and schedule time for them to build the recovery steps into FusionRM. | $0 | July 2022 |  |
| Application xyz did not start up properly | Jane Doe | Critical | TCP port between web server and database server was blocked | Open ticket with Firewall Services to ensure that port is open for the next failover test | $0 | May 20, 2022 | May 21, 2022 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

## Appendix F: FusionRM and IT DRP Examples

Below are some screenshots from the FusionRM application and the resulting output when the PDF version of the plan is generated. In the screenshots below, we have leveraged the recovery procedures defined in *Appendix A: Documenting Recovery Procedures.*

* **FusionRM Procedure Group**

Below is a sample of the procedure group defined in FusionRM. A procedure group should be where a brief description of the overall IT service is defined.

Graphical user interface, text, application, email

Description automatically generated

Figure : Example FusionRM Procedure Group

**FusionRM Procedure**

Below is a sample of a procedure. Each procedure should be one of the following: an application that makes up part of the service, an accepted risk, validation criteria, troubleshooting, or ransomware strategy.

This screenshot is for a “procedure” or the overall description of one of the applications that make up the IT service.

Shape, rectangle

Description automatically generatedGraphical user interface

Description automatically generated

Figure : Example FusionRM Procedure (Recovery)

This screenshot is for a “procedure” or the overall description of one of the “accepted risks” for the recovery of the IT service. Troubleshooting and ransomware strategies can be documented in a similar fashion.

Shape, rectangle

Description automatically generatedGraphical user interface, text, application, email

Description automatically generated

Figure 14: Example FusionRM Procedure (Accepted Risk)

* **FusionRM Procedure Step**

Each procedure should have supporting procedure steps. The steps should be broken out by the recovery of a component of the application. For accepted risks, troubleshooting, ransomware strategies, then the procedure steps would be the steps to perform for those categories.

This example is for an “Accepted Risk”:

Shape, rectangle

Description automatically generatedGraphical user interface, text, application, email

Description automatically generated

Figure 15: Example FusionRM Procedure Step (Accepted Risk)

* **FusionRM PDF Example**

Within FusionRM is a button to generate a PDF version of the IT Disaster Recovery Plan. Leveraging the information in *Appendix A: Documenting Recovery Procedures* and the screenshots above, below is an example of what would be in the IT Disaster Recovery Plan.

This initial page contains the procedure group (top two lines) and one of the procedures that were defined (Recover application).

Diagram

Description automatically generated

Figure : Example FusionRM PDF IT DRP (Shows Procedure Group and Procedure)

This second page displays the defined Procedure Steps to recover the application, then moves to the next documented “Procedure,” which is an accepted risk.

Text

Description automatically generated

Figure : Example FusionRM IT DRP (Shows Procedure Steps and New Procedure)

This page further shows how procedures and procedure steps are documented. This page shows how a validation procedure is built.

Graphical user interface, text, application

Description automatically generated

Figure : Example FusionRM IT DRP (Shows Validation Procedure)