



Cloudification - Disaster Recovery

1 Background and Purpose

The purpose of this document is to detail the specific procedures required to recover the Cloudification service following a disaster. The Cloudification service provides professional services to Cornell staff and faculty to help develop and/or move applications and services to cloud-based platforms. It also facilitates basic cloud service account configuration and integration with Cornell services.

2 Services

For information such as Service Owner, Service Delivery Manager, and Vendor Contacts; view the service records in the IT Service Portfolio. For information about Systems such as the Technical Lead, RTO/RPO, and technical information; view the Systems List or view the CI in TDX Asset Management directly.

[[Indicate specific services covered within this procedure, and any dependent services that may be affected.]]

Business Service	Systems Depended On	Dependent Services and Systems
<u>Cloud Consultation</u>	<ul style="list-style-type: none"> • <u>AWS Account</u> – Public cloud service • <u>Azure Subscription</u> – Public cloud service • <u>Email & Calendar Clients</u> – Communication, reporting of incidents and service requests • <u>Telephone</u> – Communication, incidents and service requests • <u>TDX SM Suite</u> – Incidents and service request management • <u>Jira Project</u> – Service request and project management • <u>Confluence</u> – Documentation. Note: An export of our Confluence space is kept in AWS S3 at: cu-cloud-devops-backups • Slack and Teams – Internal Communication 	N/A

Business Service	Systems Depended On	Dependent Services and Systems
<p><u>AWS Account</u></p>	<ul style="list-style-type: none"> • <u>Network for Internet & AWS Direct Connect links</u> • <u>Authentication and Authorization – Including Cornell NetID, Secure Password Management, Single Sign-On and Two-Factor Authentication</u> • <u>Identity and Access Management Data Services – Including Active Directory Management, Identity and Access Management Data Store</u> • <u>Email & Calendar Clients – Communication, reporting of incidents and service requests</u> • <u>Telephone – Communication, incidents and service requests</u> • <u>TDX SM Suite – Incidents and service request management</u> • <u>Jira Project – Service request and project management</u> • <u>Confluence – Documentation. Note: An export of our Confluence space is kept in AWS S3 at: cu-cloud-devops-backups</u> • <u>Slack and Teams – Internal Communication</u> 	<p>All services dependent on AWS cloud services – see individual DR Plans for dependency. These services are independently managed and we can't know the full scope.</p>
<p><u>Azure Subscription</u></p>	<ul style="list-style-type: none"> • <u>Network for Internet & Azure ExpressRoute links</u> • <u>Authentication and Authorization Services – Including Cornell NetID, Secure Password Management, Single Sign-On and Two-Factor Authentication</u> • <u>Identity and Access Management Data Services – Including Active Directory Management, Identity and Access Management Data Store</u> • <u>Email & Calendar Clients – Communication, reporting of incidents and service requests</u> • <u>Telephone – Communication, incidents and service requests</u> • <u>TDX SM Suite – Incidents and service request management</u> • <u>Jira Project – Service request and project management</u> • <u>Confluence – Documentation. Note: An export of our Confluence space is kept in AWS S3 at: cu-cloud-devops-backups</u> • <u>Slack and Teams – Internal Communication</u> 	<p>All services dependent on Azure cloud services – see individual DR Plans for dependency. These services are independently managed and we can't know the full scope.</p>

3 Scope

Disaster scenarios in scope for this document:

1. Major loss of operational integrity at AWS and/or Azure such as loss of an Availability Zone, the Direct Connect/ExpressRoute, or a similar mission critical function impacting a significant number of campus services.
2. Loss of over 50% of Cloud Team Staff.

Scenarios NOT in scope:

- Major incidents affecting a single customer or a handful of customers.
- Complete loss of a cloud service that is not mission critical.

The Cloud Team and Cloud and Infrastructure Managers will make a judgement about whether to activate the disaster plan based on the type, severity, and geographic extent of reported issues.

4 Procedure Overview

Following the detection of a disaster incident, the cloud team will enact the procedure described below.



4.1 Major Incident

- Open High-severity, Major Incident in accordance with CIT's procedure defined here: <https://tdx.cornell.edu/TDCClient/39/Portal/KB/ArticleDet?ID=734>

4.2 Team Conference

- Initiate a Zoom meeting or conference call to organize the Response Team. This team will be dynamically established and made up of the IT managers and Cloud & Infrastructure staff with skills most relevant for responding to the incident at hand.
- Assign individuals to the following roles on the Response Team:
 - **Response Lead** – One person acting as the lead for the disaster incident who will coordinate the activities of the Response Team and Reporter.

- **Response Team Members** – Multiple people with relevant technical skills and expertise who will execute the required assessment, restoration and recovery activities.
- **Reporter** – One person solely dedicated to communicating status to CIT and the University through the channels specified in the Communication Plan. This person cannot be the Response Lead or a Response Team Member.

4.3 Assessment Activities

- Response Lead and Response Team will assess the circumstances, risks and impacts of the disaster scenario in progress including:
 - Current state of business functions
 - IT services impacted
 - Required vendor involvement
 - Estimated time to restore (if available)
 - Workarounds (if available)
 - Risks associated with restoration measures
- Reporter will briefly and succinctly document and communicate this information as it becomes available in accordance with the communication plan.

4.4 Restoration Activities

- Response Lead and Team will develop an action plan for system restoration, including any necessary coordination with other CIT or University resources that must be involved. The plan will address:
 - Action items and assignments
 - Sequencing/timing/scheduling
 - Vendor interactions
 - Major risks
 - Required communication
- Reporter will briefly and succinctly document the information in the plan as it becomes available and communicate it through the channels identified in the communication plan. During plan execution, the Reporter will provide status updates to CIT and University in accordance with the communication plan.

4.5 Recovery Activities

- Response Lead and Response Team will enact measures for recovering data, accounts, images, etc.
- Reporter will document the recovery activities and communicate status through appropriate channels.

5 Procedure

A detailed description of the procedure is provided below.

5.1 Major Loss of Operational Integrity at AWS or Azure

This includes loss of an Availability Zone, the Direct Connect/ExpressRoute, or a similar mission critical function impacting a significant number of campus services.

5.1.1 AWS

1. Open an incident with "Business-critical System Down" priority as detailed in [AWS Support and Escalation](#)
2. Contact our AWS support team: aws-cornell-team@amazon.com and the [cloud-team-aws](#) Slack channel.
3. Provide the AWS case number, communicate the scope and impact and escalate the issue to the extent possible.

4. Following disaster incident, [assess SLAs](#) to determine if credits are due.

5.1.2 Azure

1. Open an incident with "Severity 1" priority in the [Microsoft Azure Portal](#). For help see: [Create an Azure Support Request](#)
2. Contact our [Microsoft support team](#).
3. Provide the case number, communicate the scope and impact and escalate the issue to the extent possible.
4. Following disaster incident, [assess SLAs](#) to determine if credits are due.

5.2 Loss of Over 50% of the Cloud Team

The service will continue to operate. Critical functions will be prioritized, and less critical functions will operate at reduced capacity. This will be messaged as a Service Alert through the CIT Communications Team.

6 People

CIT Cloud & Infrastructure Managers

One manager will likely assume the role of *Response Lead*. Other managers may assume the role of *Response Team Member* or *Reporter* based on the availability of staff and the nature of the disaster scenario.

- Eric Johnson
- Chris Manly
- David Shirk
- Scott Sorrentino
- Sean Walsh

CIT Cloud & Infrastructure Engineering Staff

Engineering staff members will likely be primary in the technical aspects of a disaster incident and may assume the role of *Response Team Member*, *Reporter* or *Response Lead* based on the availability of staff and the nature of the disaster scenario.

- Paul Allen
- Dan Klinger
- Gus Mamakos
- Roy Petrie
- Michael Sprague
- Jason Stuart
- Marty Sullivan

AWS Contacts

- See [AWS Support and Escalation](#)

Microsoft Team Contacts

- See [Azure Support and Escalation](#)

7 Communications Plan

The person in the role of Reporter is responsible for executing the Communications Plan.

Follow all communications requirements for a High-severity, Major Incident.

All 'official' communication to the campus community will be channeled through the CIT Communications Team. Their messaging will be the "single source of truth" regarding the disaster incident.

- CIT Communications will post on the IT@Cornell website, net-announce-l and the "Major Incident" Teams channel.
- Our role is to provide facts to the CIT Communications Team and actively work with them to develop accurate messaging.
- Status is to be reported to CIT Communications every 30-minutes even if the update is "still working to resolve."
- Messaging through channels outside of CIT (Cornell TSPs, cloud-community-l, etc.) must be limited to the "official" language of the CIT Communications Team or refer to the IT@Cornell alert.

Audience	Purpose	Message	Method	Responsible	Freq./Triggers
All of campus	Notify	Provide information about extent and potential impact of issues, including known or expected impacts on Cornell-contracted SaaS vendors.	Work with CIT Communications as specified in the <u>Major Incident Procedure</u> to post Service Alert on the IT@Cornell website, net-announce-l and the "Major Incident" Teams channel.	Person in role of Reporter	Trigger: At the time a high-severity, major incident is logged Updates: Anytime there is new information. Every 30-minutes even if the status is "Still working to resolve."
Cornell TSPs	Notify and seek information	Notify channel about apparent issues and ask for information on what impacts are being felt locally. Reference IT@Cornell alert as the single source of truth	Microsoft Teams <ul style="list-style-type: none"> • Cornell TSPs <ul style="list-style-type: none"> ◦ <u>Cloud channel</u> 	Person in role of Reporter	Trigger: Upon notification of issues or direct experience of impacts. Updates: Anytime the Service Alert is updated with new information.
AWS/Azure Customers and Practitioners	Notify	Provide information about extent and potential impact of issues. Reference IT@Cornell alert as the single source of truth	Email <u>Cloud-Community-L@cornell.edu</u>	Person in role of Reporter	Trigger: Upon notification of issues or direct experience of impacts. Updates: Anytime the Service Alert is updated with new information.
Internal CIT Staff	Discussion and coordination	Facilitation of communication regarding service restoration efforts and level of service functionality	Microsoft Teams <ul style="list-style-type: none"> • CIT <ul style="list-style-type: none"> ◦ <u>Major Incident channel</u> Email Teams Ring Central Cell phones	Any Response Team members	When impacts are widespread or impact multiple Cornell-contracted SaaS vendors

8 Business Continuity (Optional)

This is an optional section that can be filled out with a business continuity plan for how to maintain service if the system is down.

Example: Temporary system or instruction for support teams on how to maintain service if the system is down.

9 Glossary

- **TSPs:** Technical Service Providers – Cornell IT staff who are employed by college IT units and not part of CIT.
- **AWS:** Amazon Web Services - Amazon's public cloud service.
- **Azure:** Azure is Microsoft's public cloud service.
- **Direct Connect:** A dedicated network link that connects Cornell's campus network to AWS.
- **ExpressRoute:** A dedicated network link that connects Cornell's campus network to the Azure cloud service.

Approvals (Section No Longer Required)

Role	Name	Comments	Date
Accountable Director	Sarah Christen		02/17/2021
Service Owner	Chris Manly		02/16/2021
Service Delivery Manager	Sean Walsh		02/16/2021
Product Manager	Eric Johnson		02/16/2021

10 Appendix

Item	Additional Information	Date
2024 DR Refresh Ticket	https://tdx.cornell.edu/TDNext/Apps/32/Tickets/TicketDet.aspx?TicketID=1526711	9/11/2024
2023 DR Refresh Ticket	https://tdx.cornell.edu/TDNext/Apps/32/Tickets/TicketDet.aspx?TicketID=1120280	2023
2022 DR Refresh Ticket	https://tdx.cornell.edu/TDNext/Apps/32/Tickets/TicketDet?TicketID=749516	2022
Test - Tabletop exercise	Reviewed and tested with Engineering/Cloud Team staff (See attached document)	02/25/2021
Training	Reviewed and tested with Engineering/Cloud Team staff (See attached document)	02/25/2021
Backup Copy	PDF copies of the DR plan and linked documents provided to all staff members as local back-up copy	02/25/2021
Archived Plan in Confluence	https://confluence.cornell.edu/pages/viewpage.action?pageId=334790788	Pre 2019

Was this helpful?

Yes

No

100% helpful - 1 review



Comment

All

Communications

Edits Status Changes Comments

Search...



EJ

Eric Johnson

Committed Revision 19.

Thu 9/26/2024 12:09 PM

CM

Chris Manly

Changed Next Review Date from "9/1/2024" to "10/1/2024".

Fri 9/20/2024 2:10 PM

JO

Jackson Oates

Committed Revision 18.

Wed 9/11/2024 1:22 PM



Will Schultze

Committed Revision 17.

Thu 4/18/2024 9:38 AM



Will Schultze

Committed Revision 16.

Thu 4/18/2024 9:27 AM

EJ

Eric Johnson

Changed Next Review Date from "9/1/2023" to "9/1/2024".

Sat 11/11/2023 2:57 PM

EJ

Eric Johnson

Committed Revision 15.

Thu 10/12/2023 2:29 PM

EJ

Eric JohnsonCommitted Revision 14.
Mon 10/9/2023 1:18 PM

JO

Jackson OatesCommitted Revision 13.
Mon 8/28/2023 11:23 AM

CM

Chris ManlyChanged Next Review Date from "10/3/2022" to "9/1/2023".
Fri 9/30/2022 1:32 PM

EJ

Eric JohnsonCommitted Revision 12.
Fri 9/23/2022 10:50 AM

CC

Chang ChenCommitted Revision 11.
Adding link to the 2022 DR Refresh Ticket for this system in the Appendix.
Sat 7/16/2022 4:21 PM

CC

Chang ChenCommitted Revision 10.
Updating table header in section 2 to match DR template
Mon 6/27/2022 9:29 PM

CM

Chris ManlyChanged Article Ownership from "CIT - INFR - Managed Cloud Services Engineering" to "CIT - INFR - Cloud Infrastructure & Solutions Engineering".
Mon 2/21/2022 9:57 AM

EJ

Eric JohnsonChanged Next Review Date from "10/29/2021" to "10/3/2022".
Mon 11/29/2021 11:29 AM

EJ

Eric JohnsonCommitted Revision 9.
Wed 10/6/2021 2:56 PM

LH

Laurie HemmingsChanged Status from "Submitted" to "Approved".
Changed Published from "No" to "Yes".Notified: Chris Manly <cam2@cornell.edu>, David Shirk <dps23@cornell.edu>, Eric Johnson <ej4@cornell.edu>, Mariann Carpenter <mgc1@corne...
Show More

Fri 7/9/2021 12:37 PM

KC

Kelly ChenCommitted Revision 8.
Wed 7/7/2021 1:41 PM

KC

Kelly Chen

Committed Revision 7.
Wed 7/7/2021 1:40 PM



Sean Walsh

Committed Revision 6.
Mon 6/28/2021 9:55 AM

KC

Kelly Chen

Committed Revision 5.
Wed 6/23/2021 3:15 PM



Sean Walsh

Changed Status from "**Approved**" to "**Submitted**".
Changed Published from "Yes" to "No".
Changed Next Review Date from "7/21/2020" to "10/29/2021".
Fri 2/26/2021 2:05 PM



Sean Walsh

Edited draft revision.
Fri 2/26/2021 10:56 AM



Sean Walsh

Added related article "Major Incident (MI) Procedure Guide" (ID: 734).
Fri 2/26/2021 10:34 AM



Sean Walsh

Edited draft revision.
Fri 2/26/2021 9:17 AM

Share

Edit Article

Add to Favorites

Print Article

Details

Article ID: 758

Status: Approved

Revision Number: 19

Draft Status: None

Owner

CIT - INFR - Cloud Architecture

Created

Tue 7/21/20 1:59 PM by [Jacob Davis](#)

Modified

Thu 9/26/24 12:09 PM by [Eric Johnson](#)

Next Review Date

10/1/2024

Content Type 

DR - Disaster Recovery Plan

Related Articles (1)

Major Incident (MI) Process

Procedural steps for identifying, recording, working with, and resolving a major incident.

Attachments (1)

Sort By: **Name** Date 

Cloudification DR Plan Training and Tabletop 2-25-2021.docx



Fri 2/26/21 10:49 AM [Sean Walsh](#)