UNT SYSTEM
IT Shared Services

Campus Business Impact Analysis and Business Continuity Planning Guide

Business continuity planning (BCP) is the process of identifying mission-critical information systems and business functions, analyzing the risks and probabilities of service disruptions and outages, and developing procedures to continue operations during outages and restore those systems and functions.

Colleges are required to develop and maintain business continuity plans for mission critical information resources. In addition, alternative procedures should be considered that enable personnel to continue critical day-to-day operations in the event of the loss of information resources.

Business continuity plans should include a business impact analysis, risk assessment, and disaster recovery plan, a minimum. Plans should also consider information security, be tested at least annually, and should be updated as frequently as needed.

Business continuity plans for mission critical enterprise information resources have been developed by IT Shared Services (ITSS). These services include Central Web Services, EIS, Faculty and Staff Email, Learning Management Systems (Blackboard Learn), and File Storage Systems (Virtualization Services). Continuity plans for other important applications and infrastructure services have also been developed and are maintained by ITSS.

Mission Essential Functions Provided by ITSS

The following enterprise information services have been identified by campus executive leadership as mission essential to the operation of the institutions and business units. These services are managed by ITSS and include associated service level agreements and recovery timeframes. See the ITSS Services website for more information, https://itss.untsystem.edu/services.

1. **Faculty and Staff Email**

   Service Level:
   Availability: 99.0%, 24x7, excluding planned downtime, calculated monthly.

Incident Response		
Severity	**Response**	**Target Close/Timeframe**
Critical Incident- an outage or issue that affects 50 or more users	1 hour	8 hours
Routine Incident- an outage or issue that affects 49 or fewer users	4 business hours	24 business hours

2. Central Web Services

Service Level:
Availability: 99.0%, 24x7**,** excluding planned downtime, calculated monthly. Maintenance window is identified as 10:00 pm Saturday to 2:00 am Sunday

Incident Response		
Severity	**Response**	**Target Close/Timeframe**
Critical Incident- one or more sites unavailable	1 hour	8 hours
Routine Incident- isolated to a single site, not affecting service availability	4 business hours	24 business hours

3. EIS (PeopleSoft) Financial Systems and Campus Systems

Service Level:
Availability: Support is provided 24x7, excluding planned downtime. Planned downtime can occur during maintenance windows which are identified as every Saturday, 7:00 pm-noon on Sunday and every Tuesday and Thursday from 7:00pm-9:30 pm.

Incident Response		
Severity	**Response**	**Target Close/Timeframe**
Campus Wide Outage	15 minutes	4 Hours, 24x7
Major Administrative Process Inoperable or Degraded	30 minutes	6 Hours, 24x7
Application Feature Error	2 hours	12 Hours, M-F 8am-5pm

4. Learning Management System (Blackboard Learn)

Service Level:
Availability: 98.9%, excluding planned downtime. Planned downtime is scheduled every Saturday 11:00 pm-Sunday 2:00 am. Extended downtimes (for infrastructure maintenance, major upgrades, etc.) are planned and scheduled as needed.

Incident Response		
Severity	**Response**	**Target Close/Timeframe**
Critical Incident- an outage or issue that affects 50 or more user	15 minutes	4 Hours, 24x7
Routine Incident- an outage or issue that affects 49 or fewer users	30 minutes	6 Hours, 24x7
Application Feature Error	2 hours	12 Hours, M-F 8am-5pm

5. File Storage (Virtualization Services)

Service Level:
Availability: 99.621%, 24/7

Incident Response			
Severity	**Description**	**Response Objective**	**Resolution Objective**
VM Cluster Down	A production server is either offline or is causing a production service to be unavailable for the entire system	30 minutes	4 hours
20+ People Out of Service	A production service unavailability is impacting more than 20 users	1 hour	6 hours
Critical Incident	An incident impacting a few users that has a major impact on production operations	4 hours	8 hours
Routine Incident	An incident impacting nonproduction service or minimal to no impact on production operations	4 business hours	8 business hours
Routine Request	Non-incident request for OS/patch/application installation server restart or other changes	8 business hours	3 business days

UNT SYSTEM
IT Shared Services

Complete a Business Impact Assessment of IT Services

A business impact analysis (BIA) identifies the potential impacts of an interruption or loss of information technology (IT) services due to the occurrence of an event or incident. A BIA identifies the following:

- Mission essential information resources;
- The impact of disruptions and maximum allowable outage times;
    - Maximum amount of time that an IT outage can be tolerated before business unit services are detrimentally impacted;
    - Effects of an outage across related information resources and dependent systems.
- Information resources recovery priorities; and
- Identification of IT system dependencies.

Colleges should conduct business impact assessments in order to identify the impact that a loss of an IT function may have on their operation. A BIA identifies the IT functions that are essential to the operation of a business unit. College-level business unit officials are responsible for identifying the information technology services that are essential to the operation of their business units. Note: A BIA, business continuity plans, and disaster recovery plans and services have already been created by ITSS for enterprise services based on input from executive leadership of the University of North Texas; however, colleges should include information in their BCP that address the impact of a temporary or brief loss of an enterprise information technology service that is managed by ITSS.

Instructions for Completing a Business Impact Analysis Questionnaire:
Below is an example of a BIA questionnaire used by ITSS to fulfill portions of its BCP requirement. The questions in the assessment are based on the UNT System Information Security Handbook and TAC 202.76, Security Control Standards Catalog CP-2.

Colleges an administrative IT units may use this questionnaire to conduct their own BIA. Fill in the information below describing the information technology services provided by your college-level IT units. Add additional rows if needed. Do not include enterprise information systems, services, network infrastructure, information security, telecommunications, EIS, learning management systems, or other functions provided by ITSS.

UNT SYSTEM
IT Shared Services

Business Impact Analysis Questionnaire

Business Unit Name:	
Description of Business Unit's Purpose in the Organization:	
Name of Unit Manager/Director:	
Contact Information:	

ID #	Identify the Information Technology Services Provided to You by Your College IT Unit that Supports Your Business Processes or Services	Rate the Importance of the IT Services to Your Business Operation				Do you have manual work-around processes to support your business operations if this IT service is unavailable for an extended period of time?	Estimate the financial impact that a loss of this IT service would impose on your business unit.	What are the maximum number of hours your business unit could tolerate a loss of this IT service?	Rate the impact that a loss of this service would have on non-tangible assets:			How many hours of data could you afford to lose before your business functions are severely impacted?	What are the critical time periods that this IT service must be available?
		Critical	Important	Somewhat Important	Not Important		Ex, $0, <$50,000, $50,000-$100,000, $100-250,000, >$250,000		Customer Service	Health and Safety	Reputation and Goodwill		Ex. during registration periods, seasonal, beginning of a semester, beginning of a fiscal year, mid-semester, etc..
1													
2													
3													
4													
5													
6													
7													
8													
9													
10													

UNT SYSTEM
IT Shared Services

Identify Mission Essential IT Functions Provided by College or Administrative IT Units

Colleges and administrative IT units should use the information on the following pages as a guide for developing their BCP. The information is taken from the UNT System Information Security Handbook and TAC 202.76, Security Control Standards Catalog, Section CP.

Obtain, acquire, or develop the information listed in subsequent pages and place in a secure location. The information should be acquired with input with collaboration from individuals that support continuity of operations, college level management, Risk Management, and internal and external service providers. When all information has been collected, mark the information as confidential and share only with the individuals that are authorized to perform a role in a recovery operation.

IT Unit Information

- Purpose of IT unit
- Support provided by IT unit to business unit

IT Service Priorities Identified based on Business Unit Needs

IT Service Recovery Strategy

IT Service Information

- IT Service Name
- IT Service Description
- IT Service Dependencies
- IT Service Criticality
- Vendor Supported Services (if applicable)

Create Asset Inventories

- Hardware Inventory (servers, desktops, laptops, printers, etc.)
- Software Inventory and Licenses
- Data Inventory
- Facilities Inventory
- Roles, Responsibilities, and Contact Information of Key Personnel, Emergency Response/Recovery Teams, Departments, Providers, and Vendors that are responsible for supporting IT Services
- Geographic Area
- Alternative Recovery Sites
- Replacement Equipment
- Protective Services (UPS, generator, backups, fire suppression, cooling systems, fire and smoke detectors, water sensors, etc.)

Identify Potential Disruptions or Risks to IT Services Provided by College or Administrative IT Units

- Identify the *impact to business units if IT services becomes degraded or unavailable
- Identify potential IT service disruptions and their impact (e.g., physical facility damage, natural disaster, human error, accidents, sabotage, power loss, environmental issues, technical impact, loss of personnel, etc.)

Protect Mission Essential IT Functions Provided by College or Administrative IT Units

Identify, develop, or create the following plans and documentation that support continuity of operations.

- Business Resumption Plan
- Disaster Recovery Plan
- Personnel Safety Plan
- Standard Operating Procedures for IT Services
- System Configurations for IT Services
- Communications Plan for IT Service Incidents
- Business Continuity Maintenance Plan
- IT Service Level Agreements (if available)
- Applicable IT Policies

Recover Mission Essential IT Functions Provided by College or Administrative IT Units

Identify IT Service Recovery Capabilities

- Identify customer expectations of recovery time objectives for IT services (in hours)
- Identify IT recovery time capability objectives for IT services (in hours)
- Identify customer expectations of recovery point objectives for data restoration (in hours)
- Identify IT recovery time capability objectives for data restoration (in hours)
- Identify Business Recovery Priorities for IT Services
- Identify Business Recovery Costs for IT Services

Identify Backup and Failover Strategies:

- Describe Data Backup Strategy
- Describe Failover Capability

UNT | SYSTEM
IT Shared Services

Appendix

Impact Guide and Important Resources

*Impact Guide

Low Impact- Information resources whose loss of confidentiality, integrity, or availability could be expected to have a *limited* adverse effect on organizational operations, organizational assets, or individuals. Such an event could:

- cause a *degradation in mission capability* to an extent and duration that the organization is *able to perform its primary functions*, but the effectiveness of the function is noticeably reduced;
- result in *minor damage to organizational assets*;
- result in *minor financial loss*; or
- result in *minor harm to individuals*

Moderate Impact- Information resources whose loss of confidentiality, integrity, or availability could be expected to have a *serious* adverse effect on organizational operations, organizational assets, or individual. Such an event could:

- cause a *significant degradation in mission capability* to an extent and duration that the organization is *able to perform its primary functions*, but the effectiveness of the function is significantly reduced;
- result in damage to organizational assets;
- result in *significant financial loss*; or
- result in *significant harm to individuals* that does not involve loss of life or serious life threatening injuries.

High Impact- Information resources whose loss of confidentiality, integrity, or availability could be expected to have a *catastrophic* adverse effect on organizational operations, organizational assets, or individual. Such an event could:

- cause a *severe degradation in or loss of mission capability* to an extent and duration that the organization is *not able to perform one or more of its primary functions*;
- result in *major damage to organizational assets*;
- result in *major financial loss*; or result in *severe or catastrophic harm to individuals* involving loss of life or serious life threatening injuries.

Important Resources

- Texas Administrative Code (TAC), Title 1, Part 10, Chapter 202, https://texreg.sos.state.tx.us/public/readtac$ext.ViewTAC?tac_view=4&ti=1&pt=10&ch=202
- Security Control Standards Catalog, http://publishingext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Security%20Control%20Standards%20Catalog.pdf
- UNT Information Security Policy, 14.002, https://policy.unt.edu/policy-manual?field_policy_chapters_tid=14&field_policy_owners_tid=All&field_applies_to_tid=All
- UNT System Information Security Handbook, https://itss.untsystem.edu/sites/default/files/unt_system_information_security_handbook_2016.pdf**2**
- ITSS Services website, https://itss.untsystem.edu/services
- ISO (International Standard) 27002, https://untranet.unt.edu/untsystem/itss/ITCompliance/Shared%20Documents/ISO%2027002.pdf (secure authentication required)

Direct questions about IT continuity planning to IT Shared Services, Disaster Recovery/Business Continuity Planning: drbcp@untsystem.edu