Business Continuity and Disaster Recovery

Table of Contents

Getting Started

Measures must be taken to ensure the integrity, security, accuracy, and privacy of all systems and data. Such measures include adherence to all governmental regulations and directives. As major disasters have brought acute awareness to campuses, higher education institutions recognize the need for extensive planning and coordination to assure preparedness by developing, testing, and refining plans to handle all types of disruptions to normal services. Use the following steps to get started with a business continuity plan.

1. **Obtain** commitment and authority from institutional Leadership. High level support is essential for building the cross functional teams that are needed to prepare and deploy the plan.
2. **Establish** a planning team for each business unit.
3. **Perform** a risk assessment in each unit.
4. **Identify** critical resources:
    a. People – Identify all support staff, and establish a chain of succession for key personnel.
    b. Places – Identify key buildings, and plan alternate locations for workers and equipment.
    c. Systems – Perform a business impact analysis to prioritize systems in terms of criticality.
    d. Other – Identify other critical assets required for normal business operations.
5. **Determine** continuity and recovery strategies within each unit.
6. **Train** students, faculty, and staff on what to do in case of a disaster.
7. **Test, test, test!** Test system recovery procedures. Generate scenarios and simulate them with table top exercises.
8. **Create** a communication plan.
9. **Review** the business continuity plan annually.

A well prepared institution should develop a plan addressing all key services and their administration, delivery, and support. This document presents guidance for institutions considering or embarking on the development of a plan, including commitments, procedures, technologies, resources, methodologies, and communications essential to planning development, support, and deployment. Sections below address the special needs of varied aspects of a plan.

Top of page

Overview

Colleges and universities are vulnerable to a variety of natural and man-made emergencies, disasters, and hazards. Recognizing that not all events can be prevented and some risks may be deemed acceptable, proper planning is essential to maintain or restore services when an unexpected or unavoidable event disrupts normal operations.

Business continuity planning includes the identification of vulnerabilities, priorities, dependencies, and measures for developing plans to facilitate continuity and recovery before, during, and after such a disruption. Comprehensive business continuity plans are designed and implemented to ensure continuity of operations under abnormal conditions. Plans promote the readiness of institutions for rapid recovery in the face of adverse events or conditions, minimize the impact of such circumstances, and provide means to facilitate functioning during and after emergencies.

The development process is usually based on a single framework, and involves key individuals in the functional areas. Plans are based on a risk assessment and business impact analysis and include a process for regular maintenance, including training, testing/drills, and updates. In addition, information security and privacy should be integrated within plans.

Examples of Incidents that Activate Business Continuity Plans

- A fire in a building with critical resources would prohibit normal functioning in a localized facility.
- An electrical power loss may cover several states or an extended time period. The northeastern states experienced an extended power loss during and after an unusual October 2011 snow/ice storm, Super Storm Sandy, and the numerous blizzards/ice storms/fires/floods of recent years. Outages of some kinds lasted nearly a month in some place; others are still in effect over a year later.
- Floods, massive fires, blizzards, tornadoes, hurricanes, tsunamis, earthquakes, pandemics, ice storms, or mud slides that results in evacuations and inaccessibility to critical resources.
- A criminal activity or terrorist incident may impact a wide geographic area for an extended period of time.
- A pandemic, nuclear, chemical, or biological incident may limit the mobility and accessibility of individuals for extended time periods.

Top of page

Information Security Continuity

Objective: Business continuity planning provides a managed, organized method for the deployment of resources and procedures to assure the continuity of operations under extraordinary circumstances, including the maintenance of measures to assure the privacy and security of its information resources.

Business Continuity Plans are an integral part of all organized Information Security activities. The plans are a well-reasoned, step-by-step approach to determine the how, when, where, who, and what will be needed should a disruption of normal operations occurs. Recent history has demonstrated that plans are a necessity regardless of the size, location, or mission of an organization. And the plan must address the continuity of security and privacy under less than ideal circumstances. Below are some references to further describe the intent of such plans.

The **United States Homeland Security Presidential Directive (HSPD-5), the Management of Domestic Incidents** states as its purpose "To enhance the ability of the United States to manage domestic incidents by establishing a single, comprehensive national incident management system to ... prevent, prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies, the United States Government shall establish a single, comprehensive approach to domestic incident management." While not all reasons for business continuity involve homeland security, this is an acknowledgment at the highest governmental level of the need to establish business continuity plans.

A mandate from the **U.S. Department of Education Sector Specific Plan** states "That all schools and universities are prepared to mitigate/prevent, respond to, and recover from all hazards, natural or man-made by having a comprehensive, all-hazards plan based on the key principles of emergency management to enhance school safety, to minimize disruption, and to ensure continuity of the learning environment."

REMS TA Center: Under the administration of the U.S. Department of Education's Office of Safe and Healthy Students, the Readiness and Emergency Management for Schools (REMS) Technical Assistance (TA) Center provides free technical assistance and training services to the K-12 and higher education populations (along with their community partners) on a variety of safety, security, and emergency management topics. Cyber threats are just one of many emergency threats and hazards that they address through resource development, virtual trainings (webinars and online courses), live trainings by request, a community of practice, and their comprehensive website. Do you have questions specific to higher ed safety, security, or emergency management? Contact the REMS TA Center Monday through Friday from 9 AM to 5 PM ET at info@remstacenter.org or 1-855-781-REMS [7367]. You can also download the REMS TA Center's 2017 Cybersecurity Considerations for Higher Education Fact Sheet.

The **Minnesota State Colleges and Universities System Board** addresses **Long-Term Emergency Management** by requiring that "Each college, and university and the Office of the Chancellor shall develop and maintain an All Hazards Plan that provides guidelines in the event of long term emergency. The plan shall be developed in accordance with guidelines developed and administered by the Office of the Chancellor in accordance with state and federal directions. The All Hazards Plan will include sections that address crisis intervention, continuity of operations, and emergency preparedness."

- Business Continuity After Hurricane Ike: A Tale of Two Schools
- Fire at OLLU! Business Continuity from an IT Perspective
- A Report on the Business Continuity Summit
- How Ready Are IT Managers for a Crisis?
- ISO 27002 Toolkit - Business Continuity
- Business Continuity diagram and description

Top of page

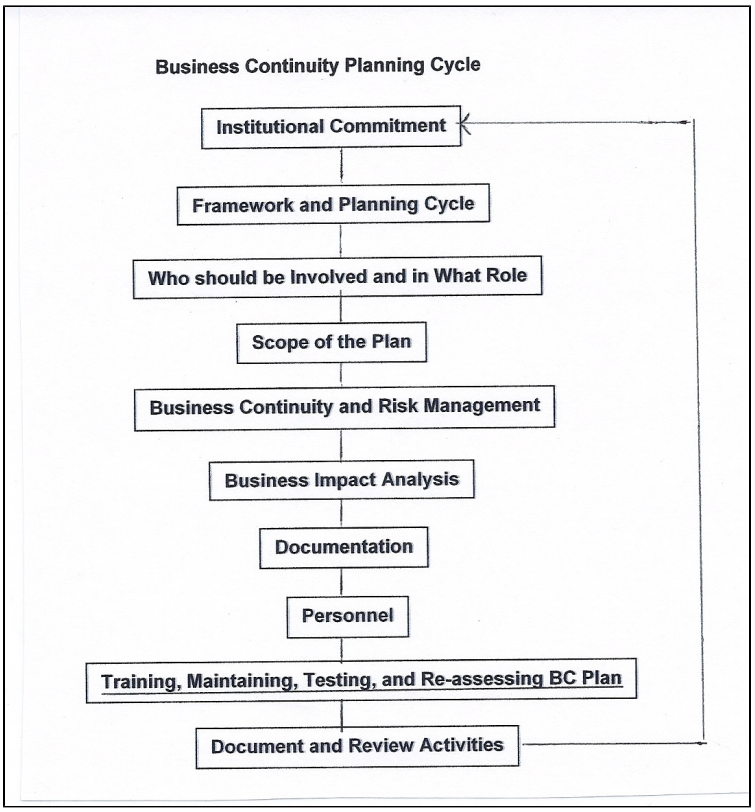
Planning Information Security Continuity

Information security must be an integral part of all institutional policies, procedures, and practices. Information security should also be an integral element of business continuity management systems.

Implementing Information Security Continuity

Business continuity plans must recognize the need to strictly adhere to institutional security and privacy policies and regulations, even while the institution is functioning during extraordinary conditions. Good business continuity plans should be built in accordance with strong institutional security and privacy policies as well as state and federal regulations. This will allow important security and privacy practices to continue to be practiced, even during and after a disruptive event. Such practices should be elements of all planning, implementation, testing, and evaluation efforts.

Business Continuity Planning Cycle



Institutional Commitment: Obtain commitment and authority from institutional leadership

A plan begins with a university-wide commitment to develop, staff, and support efforts that will be activated when circumstances clearly indicate that business has been or will be disrupted for more than a brief or acceptable time. A plan is not intended to address routine disruptions such as planned or routine maintenance. On the contrary, well-developed and tested plans are essential during and after catastrophic events that preclude resumption of normal business functioning within well defined time frames.

Begin the planning process by obtaining the buy-in from the executive level of the institution. This high level mandate establishes the ability, authority, and support to build the cross functional teams needed for the preparation and the deployment of the plan, facilities and resources, necessary redundancy of services and resources, and commitment from units for ongoing participation. Institutional support for business continuity should include funding for plan development, staffing, training, testing, updating, deployment, and transitioning to normal operations.

Note that a business continuity plan is not just a technology plan. It is not just what to do about unavailable IT resources. It is a much broader view of the functions and information resources of the institutions. IT resources are a necessary part, but not a sufficient part. People are the most important element. Commitment, leadership, preparation and practice are key factors of a business continuity plan.

Business continuity can be viewed as an added expense at a time when funding is limited. It is important to realize that having a business continuity plan is a critical function that needs continuous funding. However, even if your institution determines that it cannot afford to support a full plan for everything that is needed, it is important to develop and have a plan in place. Developing a plan forces priorities to be identified and implemented and identifies which risks are acceptable and which must be addressed. And when possible, additional components of a plan should be implemented. Some plan is better than no plan at all.

Many Campuses Have No Strategic Plans for Disaster Recovery

Data from the Campus Computing Project reveal that a large number of campuses do not have strategic plans for disaster recovery. Just under two-thirds (63.7 percent) of the institutions participating in the fall 2010 survey report a strategic plan for IT disaster recovery, up slightly from 2009 (62.2 percent) and reflecting only modest gains since 2004 (55.5 percent) or even 2002 (53.0 percent). Some sectors have shown only small increases in the percentage of institutions reporting a strategic plan for IT disaster planning between 2008 and 2010. Moreover, the survey data do not reflect the age of campus DR plans -- when the plans were last updated. (A DR document dated 2005 or 2007 might be a plan, but not necessarily a good one!)

Strategic Plans for IT Disaster Recovery (percentages by sector for selected years, 2002-2010) *Source:* The Campus Computing Project

- Presidents and Campus Cybersecurity
- Presidential Leadership for Information Technology
- Gaining the President's Support for IT Initiatives at Small Colleges

Top of page

Framework and Planning Cycle

Having a framework assures a defined structure for the planning process, the development of a plan, priorities and dependencies within a plan, testing of a plan, procedures for maintaining and updating the plan, and responsibilities of individuals and units before, during, and after the activation of a business continuity plan. Choose a framework to be used as the basis for the plan.

- Create the plan
- Train the participants
- Perform drills
- Do post mortems on the drills
- Review the plan
- Revise the plan

University of California, Davis: Creating an Institutional Framework for Business Continuity (ECAR case study)
Building ISO 27001 Certified Information Security Programs - University of Tampa, 2017

- Seizing the Moment: A New Model for Disaster Recovery at Florida State University
- ISO 27002 Toolkit - Business Continuity
- Business Continuity Planning Process from READY.GOV (US Government)

Top of page

Who Should be Involved and in What Role - Establish a planning team for each business unit

At its core, business continuity management is a well-coordinated, well-tested, cross-functional effort.

Representatives from each functional area or business unit are responsible for the identification, prioritization, documentation, and updating of their aspects of the plans, covered services, and facilities. Remember to include academic and their support areas in the list of units to be included.

Members of a business continuity team are responsible for the compilation and integration of all input from each functional area into the overall plan.

Team coordinators are responsible for the overall coordination of the plan, its deployment, and its refinement. They must be good, dependable managers with strong leadership and problem solving skills, capable of keeping the effort organized according to procedures, yet able to be creative when things don't go as planned.

Disaster Recovery: A Multi-Institutional Collaboration at the University of California System (ECAR case study)

- A Business Continuity Planning Toolkit (2008 presentation + resources)

Top of page

Scope of the Plan

A Business Continuity Plan cannot be unlimited in scope, so it's important to define the comprehensiveness of the plan: whether it covers contingencies for all major potential threats (severe weather events, terrorist threats, fire, shooter, cyber-attacks, pandemic) or a subset of these disruptions. Define whether the plan covers the entire campus, parts of the campus or multiple campuses. Define what critical functions are covered as part of the plan and what activities are not essential. Define the time scope of the plan - does it plan for a disruption that lasts hours, days or weeks? The Business Impact Analysis should heavily inform the plan's scope.

Defining the scope does not negate the concept that BCP should broadly account for any business disruption. It's a practical measure acknowledging that the continuity planning process is impacted by budgetary restraints.

- Business Continuity Planning (EDUCAUSE Library page)
- Disaster Recovery Planning (EDUCAUSE Library page)
- IT Disaster Recovery Plan, Adams State College
- Creation of Disaster Recovery and IT Continuity Plan
- Seizing the Moment: A New Model for Disaster Recovery at Florida State University
- Business Continuity Planning: Process, Impact, and Implications
- Business Continuity Plan from READY.GOV

Top of page

Business Continuity and Risk Management - Perform a risk assessment in each unit

It is important to determine the impact of risks on the functioning of the institution under normal operating conditions as well as under the extraordinary conditions during which a business continuity plan will be activated.

Risk Management is an activity directed towards the assessing, mitigating, and monitoring of risks to an organization. In Business Continuity Management, it is important to determine what activities are vulnerable under what conditions, what measures should be taken to reduce risk and at what cost, what risks are acceptable, and what measures should be taken to facilitate functioning during and immediately after incidents that disrupt normal operations of the institution. Refer to the Risk Management section of this guide for a full discussion of this topic.

Post-9/11 Emergency Response and Business Continuity Changes at Pace University and New York University (ECAR case study)

Top of page

Business Impact Analysis - Identify Critical Resources

A Business Impact Analysis (BIA) identifies the institution's critical services and resources and the maximum tolerable downtime (MTD) for these critical services. The BIA must identify vulnerabilities, threats and risks and prioritize the order of events for restoration of key business processes. The BIA is distinguished from Risk Assessment in that it defines the window of time available to restore services.

First determine the institution's key functions and resources that must be continuously available, during and immediately after major disruptive events. Business units must identify their key resources, prioritize them, and assess the risks to determine how long these key resources can be unavailable and factors that impact that duration. Each unit must perform a risk assessment to identify measures to be taken to reduce risks as well as identify acceptable risks where the cost of mitigation is higher than the cost of the consequence. Each unit must also assess the priority of resources and services. This prioritization should be identified by the unit itself.

Alternate resources may be identified for use should the primary resources become unavailable or inaccessible. The results of the business impact analysis are input to the development of the business continuity plan.

- Business Continuity Planning: Process, Impact, and Implications
- A Business Continuity Planning Toolkit (2008 presentation + resources)
- Risk Management

💡 Shared Responsibility for Business Continuity: The Team Approach at UCLA (ECAR case study)

Top of page

Documentation

All required information pertaining to the plan, key resources, facilities, management structure, priorities/dependencies, documentation, and personnel should be kept in secure locations which can be physical, virtual, or cloud-based. This information should also be made available to key personnel who will be responsible for coordinating continuity efforts during and after the incident or event.

Operational information will assist those directly working to keep/restore functions. Individuals most familiar with applications may not be able to respond. Documentation will assist others in performing required tasks.

Emergency templates for all functions included in the plan should include a summary of business impact analysis data, required resources (hardware, software, data) for the application to run, dependencies on other applications and resources, vendor contacts, people who should be kept apprised of status of the recovery, and the list of key individuals and how to reach them.

Contact Information

The inability to contact key team members can hamper the most well designed plan. Contact information must include all means for reaching people at all times. This list must include alternate people should a key individual be unavailable or unreachable. Contact information must be kept current at all times and include alternative means such as home and cell phone numbers, alternate email addresses, and social networking, text, and twitter contact information.

Checklists

Checklists should be created to document the inventory of everything kept in designated physical, remote, virtual, and/or cloud locations for coordinating efforts - contact information, documentation, resources/systems, backup power, communications equipment, food, water, vendor contacts, etc.

Keep Track of Activities

While testing a plan or during an actual deployment, remember to keep track of who is doing what. This can be done via conference calls, texting, alternative web sites, and actual staff reporting in to track all activities as well as make sure that people are safe and getting sufficient food, water, and rest. Communication may be difficult, but it is essential. Not everything will work as scripted, and communicating with other team members may help solve the unexpected or undocumented.

Top of page

Personnel

People are the key element of the plan. Being able to communicate during a crisis may not be easy due to loss or overloading of infrastructure. Continuity plan leaders or coordinators should be good leaders and managers, capable of keeping the effort organized according to procedures, yet able to be creative when things don't go as planned.

Have at least two people scheduled at all times as team coordinators for the continuity effort. Never have a single point of failure! Someone may not be available at the critical time.

Team coordinators should be involved in monthly assessment of the resources and facilities. Establish a substitution procedure for team coordinators should one be unavailable due to schedule conflicts, illness, or vacations. Substitution should be communicated carefully to avoid confusion.

Because people are key, it is important to care for their needs as the institution is heavily dependent on their skills and ability to perform. Be cognizant of their needs for food, water, and rest as well as their ability to communicate with their families. Support them as they help the institution get through the crisis.

Top of page

Communication

Being able to communicate during a crisis is essential. Students, faculty, and staff on campus need to know what is happening as well as what they can/cannot do. Relatives want to know about the safety of individuals on campus. Employees involved in continuity need to know how, when, and where they should report. Continuity plan personnel need to communicate with campus executives on the status of services and resources. Everyone needs to know what they should/should not do and when circumstances are expected to change.

Determine alternative means for communication. "Normal" communication means and data feeds for supplying such information such as phone numbers may not be available. Plans should include alternative technologies for communicating and availability of key data. Social networking sites should be considered as an alternative means of communication, but not necessarily as a primary method.

Power losses (regardless of cause) may result in disruption of services - cell towers, Internet access, and the campus network. Other failures have equally disruptive consequences. During 9/11 in New York City, dial tone was lost, cell service was spotty and overloaded, and most internet access was disrupted due to loss of the carriers. No services were maintained during Hurricane Katrina. Super Storm Sandy presented major disruptions to infrastructure (electricity, natural gas, communications, roads), routine and emergency services, life/safety services, housing, deliveries (food/water/fuel) and facilities. Many of its impacts are still being experienced today.

Identify alternative means (cell phone, text, email, etc.) for contacting individuals needed to manage the process and to provide continuity services. Consider digital signage, landlines or speakers in locations where cell signals are weak/unavailable, CATV, text messaging, social media, and new technologies as they proliferate in classroom, residential, administrative, and service buildings. People need to know what the emergency is, how to react, and what to expect in order to prevent a bad situation from becoming worse. No information, or worse, bad information can transition a bad situation into a crisis. Emergency responders must be contacted, know if/when they are needed, what roles they will play, and where you want them to perform tasks. Remember, people are the key component to business continuity and communication with and among them is absolutely necessary.

Communication is also a life/safety concern for the community, not just for first responders. Timely consistent communications are essential before, during, or after natural disasters, weather/natural disasters, lockdowns, and any event that impacts the life/safety of individuals and the availability of services and facilities. It is also important to be able to determine who is ok after an incident. A preset, known means for communication is essential.

The **Common Alerting Protocol** provides a means for dissemination of consistent information via a multitude of technologies. From the FEMA.gov link listed,

> *"As more systems are built or upgraded to CAP, a single alert can trigger a wide variety of public warning systems, increasing the likelihood that intended recipients receive the alert by one or more communication pathways. CAP provides the capability to include rich content, such as photographs, maps, streaming video and more as well as the ability to geographically-target alerts to a defined warning area, limited only by the capacity of the delivery system used. Because CAP provides the capability to incorporate both text and equivalent audio, CAP alerts can better serve the needs of hearing or visually impaired persons. Although IPAWS does not provide translation services, CAP does provide the capability to issue alerts in multiple languages."*

Details about CAP, its implementation, terminology, elements, messaging, standards, and implementations can be seen at the above web address. Its intent is to support a means for disseminating consistent, timely messages via multiple technologies to reach as many people as possible.

In summary, communications should involve a suite of products/technologies, be activated for life/safety reasons, and must quickly reach as many people as possible.

Examples of the use of emergency communications include the Virginia Tech shooting, Hurricane Katrina/Super Storm Sandy preparations and aftermath, New York City area on and after 9/11, tornadoes/blizzards/earthquakes/massive fires/floods, the major northeast power disruption, and more.

- FEMA Common Alerting Protocol
- Emergency Notification

Top of page

Training, Maintaining, and Re-assessing Business Continuity Plans

Objective: Business continuity plans must include managed, organized procedures for the development of procedures to assure the continuity of operations under extraordinary circumstances including the maintenance of measures to assure the privacy and security of its information resources. It includes training individuals with responsibilities for the plan's implementation, having regular reviews and updates to keep the plan correct, and for testing the plan to evaluate its feasibility, thoroughness, and effectiveness even under the most unusual of circumstances while maintaining the privacy and security of its information resources.

Training of all plan coordinators and key personnel should take place at least once a year. Training should include:

The process, expectations of individuals, applications and resources, priorities, contact information and methods, procedures, documentation, facilities, and schedules. At least once a year a drill should be conducted. This can be a table-top exercise or a "live" test. At the conclusion of the drill, a review of responses and actions should be completed to determine next steps such as modifications to the plan, additional training, and further testing. Brandeis University developed a disaster recovery tabletop exercise plan in 2015 that can be used or modified by other institutions.

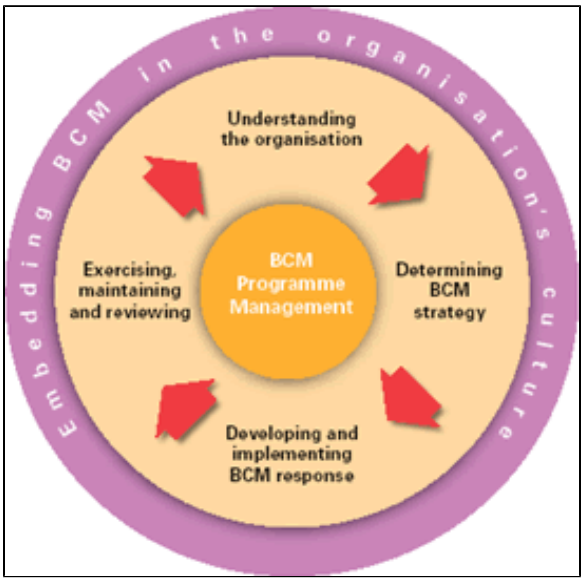
In addition to drills to test the plan, its components/procedures, and its people, it is critical to test all methods of emergency communication with members of the institution. Institutions should have multiple methods for contacting members of the University community in the event of an emergency or urgent change in regular functions. Everyone (faculty, staff, student, contractors, and suppliers) should be enrolled in an emergency communication alert list, including all cell phones which would likely be used for texting messages. Data collected should not be limited to campus supplied phones and email addresses. All information collected will only be used in the event of an emergency and should not be shared outside the institution. Everyone should be prompted at least semi-annually to review/update their data. Drills should be scheduled at least quarterly to test this emergency alert system. Events at several universities in the last year have demonstrated the necessity for such emergency alert systems using personal communication devices as well as other technologies.

Document and Review Activities - Review the business continuity plan annually

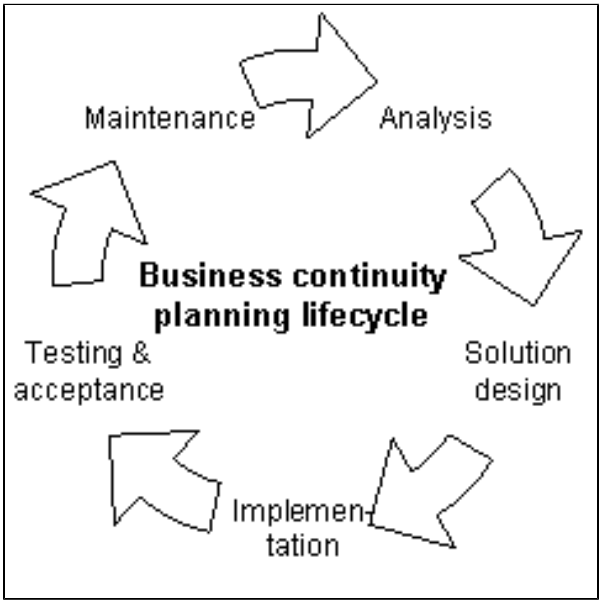
Business Continuity plans are living documents that must change and evolve to reflect institutional changes. To be effective, plans must be continually revised and improved to be in alignment with the current environment. A review should be conducted annually (or more frequently) to document all institutional changes that will impact the plan including:

- Information gleaned from recent incidents.
- Information gleaned from plan training and testing.

- Changes in the Business Impact Analysis.
- Implementation of new equipment and technology.
- Organizational restructuring.
- Major additions or changes to facilities.



With permission from BCM lifecycle, BSI Group



Courtesy of Wikipedia Commons

Redundancies

Objective: As a critical element of maintaining continuity of services, there needs to be adequate redundancy of facilities, people, communications, documentation, training, and services.

Business Continuity Plans must anticipate a multitude of failures, causes, loss of data or facilities, unavailability of trained personnel, communications losses, powers losses, and more. Plans must assess the risks associated with each critical component and identify redundant/alternative means for providing for continuity of services under all conditions.

Due to the nature of business continuity management, it is essential that all elements of a plan have adequate redundancies available, knowing that some elements may be compromised by the nature of the disruption. Redundancies include cross training of personnel, alternate facilities at locations that do not share vulnerabilities, redundant communications methods and providers, power sources, physical access, and more.

Top of page

BC PLAN - AVOID POTENTIAL SINGLE POINTS OF FAILURE

LOCATION /GEOGRAPHY	Campuses, metro area, flood plain/river bank, avalanche, hurricane or tornado prone, unreliable power source, poor transportation /communication systems, etc.
FACILITIES and INFRASTRUCTURE	Power, generators/fuel supplies/suppliers, air conditioning, communications lines-data, voice, multiple high speed network connects, network topology, environmental conditions/hazards, central organization, schools, or admin units
SYSTEMS	Lost, damaged, can't be "touched" or "reached"
DATA	Lost, not accessible
PEOPLE	Not 24x7 staffing; off hours not on campus, no/limited transportation, not reachable via communications-voice, Internet, cell, text, etc., facilities disabled, unsafe conditions, evacuated, can't leave campus – government enforced, not cross trained, insufficient backup of skills
DOCUMENTATION	must document critical/emergency procedures and recovery procedures, must assume that "usual" trained people are unavailable, need for depth of cross training, docs must be available to all potential users – not just on one, local system or in one place, vendor contacts – office, cell, text, social networking, IM, etc.

Top of page

Key Considerations

Data is Essential and Must Be Replicated

Data is more important than hardware. Data should be replicated by a variety of means and should be retrievable as needed. Hardware can always be replaced. Be aware of dependencies between software and data. Cloud services may provide viable options for replication as long as security and privacy are maintained.

Lecture Capture and Delivery for Use During a Pandemic or Biological Emergency

Consider the impact of a pandemic or biological emergency on the delivery of instruction when neither the instructor nor the students are able to be present in the same physical location. There are several alternative means for instructional delivery ranging from videoconferencing to providing previously captured lectures available on demand. Lectures can be streamed to or from campus and alternate locations. Technology can be leveraged to produce audio, video, and screen captures that enable both time and location shifts.

Alternate Sites for Web Hosting

Consider the impact of a hurricane on physical facilities (which become uninhabitable), life-safety issues (evacuations, flooding, disease, lack of potable water and food, etc.), electrical power/network infrastructures, and an extended prognosis for the restoration of "normal operating conditions." A business continuity plan should identify alternative means to be used to provide essential services under such unthinkable circumstance. Services should include means for communicating information on the status and safety of the institution and its people to the rest of the world. Consider contracting for an alternate service for communicating key information with on and off campus people while normal institutional web services cannot be provided.

Availability of Information Processing Facilities

Despite the emergency or disruptive circumstances, information processing facilities must continue to function, be accessible for critical processing, and maintaining the security, integrity, and privacy of information. In creating plans, many variables need to be considered when choosing alternative sites, services, personnel, vendors, power/communication means, and accessibility.

Choosing the Right Locations for Locating Emergency Equipment and Locations to Serve as Continuity Centers

First and foremost, consider all types of factors when evaluating locations to house emergency equipment such as electricity generators. As learned from Super Storm Sandy, never locate generators in basements, locations below 100 year flood lines, or locations likely to be inaccessible for fuel deliveries. NYU Medical Center lost the use of all of its power generators when the East River overflowed its banks. Patients had to be evacuated to other hospitals because all power sources were down and all its generators were underwater. Restoration of power took weeks. Physical damage and lost revenues were beyond any expectations as no one expected the water level to rise to the extent it did. Only now are plans being made that consider rising water levels that are likely to recur more frequently.

A plan should include the identification of physical locations that will be used to coordinate during and immediately after an incident. Ideally, several locations should be chosen at increasingly distant locations from the institution. This allows for a disruption in a key building or campus, a metropolitan area, and a significant geographic designation while minimizing the impact on a continuity effort.

Be cautious and exercise due diligence when considering locations and technologies for potential sites to serve as continuity centers. While some locations and facilities may seen to have some very positive attributes that would seems to make them cost effective choices, there are many critical issues that should be explored. Categories of considerations include:

- Physical locations on or off campus.
- Virtual locations (address security and privacy concerns).
- Cloud resources (address security and privacy concerns).
- Availability of sufficient communications excellent/redundant/multi-vendor cell capacity, land lines, internet bandwidth from more than one vendor and physical supply (not all coming through the same conduit, following the same path), and satellite access.
- Availability of alternative power sources - generators with adequate fuel supply and delivery. (Natural gas is ideal, if available, as long as the location is not prone to flooding, hurricanes, tornadoes, or earthquakes. It minimizes delivery issues.) Multiple suppliers should be contracted for other types of fuel supply. Remember that generators need routine maintenance and testing.

- Sufficient physical access during emergency situations (not located along a major evacuation route, yet highly accessible).
- Proximity to locations that contain hazardous material, or are near river banks/flood plains, avalanche zones, mud slide zones, frequent forest fires, or earthquake prone locations.
- Security and support for personnel staffing the continuity effort.

It is not critical that hot sites (physical, virtual, or cloud) be as extensive or as fast as normal resources. They are for emergency use, not daily operations.

Communications facilities and contact information must be as accurate and complete as those used for daily operations. They provide the lifeline for all coordination of communication.

Top of page

Good Vendor Relationships are Important

Establishing good, working relationship with key vendors can help in times of crisis. Resources may need to be replaced. Good relationships may help move your needs to the head of the queue of waiting orders. While there may be many others facing similar problems related to the same or other crises, vendors are sensitive to the problems and will try to assist however and whenever possible when there is an existing relationship.

- Business Continuity After Hurricane Ike: A Tale of Two Schools
- At Least It Wasn't a Football Weekend: The Notre Dame Tunnel Fire
- Hazards and Hurricanes: Hallmarks of IT Readiness, Response, and Recovery
- Fire at OLLU! Business Continuity from an IT Perspective
- Irene/Katrina Business Continuity and Disaster Recovery

Top of page

After the Resumption of Normalcy

While everyone may be tired and anxious to get back to business as usual, bringing all the key individuals to a session to discuss how the plan worked or failed is important. This is a unique opportunity to get direct feedback on the usefulness of the plan. Scheduling a "postmortem" is invaluable in getting constructive feedback as well as complaints that need addressing. Drills are helpful, but a postmortem shares real experiences and feedback.

Terminology and Definitions

- **All Hazards** - An integrated planning approach to all domestic terrorist attacks, major disasters, and other emergencies.
- **Business Continuity** (also referred to as Continuity of Operations Planning and Service Continuation Planning) - A process for determining an institution's ability to maintain or restore its business and academic services when some circumstance disrupts normal operations.
- **Business Impact Analysis** - A management level analysis which identifies the impacts of losing resources. This analysis measures the effect of resource loss and escalating losses over time, in order to provide senior management with reliable data upon which to base decisions on risk mitigation and continuity planning.
- **Disaster Recovery** - A plan for the recovery of information technology resources in the event of a disaster or emergency that generally contains details to ensure systems and communications are restored within a predetermined time frame. The disaster recovery plan is a critical component of the business continuity plan.
- **Emergency Response Plan** - This includes details for responding to sudden states of danger that require immediate action.
- **Pandemic Planning** - Preparation in the event that a highly infectious virus, such as the H1N1 or Avian flu reaches pandemic stage.

Top of page

Resources

Campus Case Studies On This Page
Building ISO 27001 Certified Information Security Programs (University of Tampa, 2017)

EDUCAUSE Resources

- Brandeis University 2015 Disaster Recover Tabletop Exercise Plan
- Disaster Recovery Planning (EDUCAUSE Library page)
- Emergency Notification (EDUCAUSE Library page)
- Business Continuity Planning (EDUCAUSE Library page)
- Risk Management (Information Security Guide chapter)
- 7 Things You Should Know About Emergency Notification Systems
- Irene/Katrina Business Continuity and Disaster Recovery
- Post-9/11 Emergency Response and Business Continuity Changes at Pace University and New York University
- Disaster Recovery: A Multi-Institutional Collaboration at the University of California System
- Shared Responsibility for Business Continuity: The Team Approach at UCLA
- Cloud Computing and the Power to Choose
- At Least It Wasn't a Football Weekend: The Notre Dame Tunnel Fire
- Changing Ideas of Campus Disaster Recovery: Designing Resiliency into Systems
- IT Disaster Recovery Plan
- The Myth about Business Continuity and Disaster Recovery
- Hazards and Hurricanes: Hallmarks of IT Readiness, Response, and Recovery
- Seizing the Moment: A New Model for Disaster Recovery at Florida State University
- Business Continuity Planning: Process, Impact, and Implications
- What if it happens here? Cornell upgrades its emergency plans to meet challenges of health and safety
- Shelter from the Storm: IT and Business Continuity in Higher Education - Key Findings
- University of California, Davis: Creating an Institutional Framework for Business Continuity
- Learning the Hard Way
- Lemons to Lemonade: Disaster Preparation and Recovery
- IT Readiness for Business Continuity
- A Report on the Business Continuity Summit
- A Business Continuity Planning Toolkit (2008 presentation + resources)
- Fire at OLLU! Business Continuity from an IT Perspective
- IT Disaster Recovery Within the Framework of Business Continuity Planning
- Business Continuity After Hurricane Ike: A Tale of Two Schools
- Transforming Continuity
- Academic Continuity-Emergency Management Workshop Report
- Weathering the Storm Panel - Preparing for, Responding to, and Recovering from Emergencies
- Stories from Superstorm Sandy
- Preparing for the Future with Disruption-Resistant Online Programs
- Disaster Recovery Preplanning: Decision Making for RTO and RPO
- Pandemic Flu and Computer and Network Disaster Recovery Planning: Some Starting Thoughts
- Disaster Recovery Planning: How to Build It, How to Test It
- The New Normal: When Disaster Recovery Efforts Become Very Real
- University of Wisconsin-Stout Emergency Management Information
- Strategies for Success in Disaster Recovery
- Protecting Cyber Assets

Initiatives, Collaborations, & Other Resources

- Business Continuity diagram and description (from Crisisleaders.com)
- Business Continuity Plan from READY.GOV (US Government)
- Disaster Recovery Institute International
- Disaster Recovery Journal
- ISO 22301:2012: Societal Security – Business Continuity Management Systems – Requirements
- ISO 22313:2012: Societal Security – Business Continuity Management Systems – Guidance
- Microsoft Word Document Template for Disaster Recovery Planning (Microsoft TechNet)
- Readiness and Emergency Management for Schools (REMS) Technical Assistance (TA) Center website
- REMS TA Center's 2017 Cybersecurity Considerations for Higher Education Fact Sheet

Top of page

Standards

ISO	NIST	COBIT	PCI DSS	2014 Cybersecurity Framework	HIPAA Security

27002:2013 Information Security Management **Chapter 17**: Information Security Aspects of Business Continuity Management **ISO 22301:2012**	**800-100**: Information Security Handbook: A Guide for Managers **800-53**: Recommended Security Controls for Federal Information Systems and Organizations **800-12**: An Introduction to Computer Security - The NIST Handbook **800-14**: Generally Accepted Principles and Practices for Securing Information Technology Systems **800-34**: Contingency Planning Guide for Information Technology System, Revision 1	**DSS04.02** **DSS04.03**	**Req 12.9.1**	**ID.BE-4** **PR.IP-4** **PR.IP-9** **PR.IP-10**	**45 CFR 164.308(a)(7)** **45 CFR 164.310(a)(2)(i)**

The ISO 27002 Toolkit provides assistance in the development of a business continuity plan. It addresses much of the essential preparation including identification and analysis of priorities, dependencies, contingencies, risk analysis, auditability, and impact analysis. The toolkit includes a framework and checklists to aid in the development, on-going support, and testing of a plan.

Top of page
