



San José State UNIVERSITY

BUSINESS CONTINUITY PLANNING (BCP)

MASTER PLAN

This BCP Master Plan is a management document explaining the methodology for assembling the BCP logistical manual, its maintenance, and how BCP is executed to restore University operations after a disaster. It is continuously revised and updated to reflect the changes in University management, organization, and business. New materials will also be constantly added as the need arises.

BCP Overview

BCP Guiding Principles

SECTION1 : SJSU BCP FRAMEWORK

AUTHORITY

CONCEPT OF OPERATIONS

BCP COMMUNICATION AND MANAGEMENT

CREATION OF LOGISTICAL MANUALS

PHASED APPROACH TO DEVELOPING THE SJSU BCP:

- Phase 1
- Phase 2
- Phase 3

SCHEDULE OF CURRENT BCP INCEPTION CYCLE (2009 - 2011)

OVERVIEW OF METHODOLOGY TO DEVELOP THE BCP LOGISTICAL MANUAL

- 4 main steps
- Other considerations

OVERVIEW OF MAIN TYPES OF RISK ANALYSIS

- Business Impact Analysis
- Risk (Vulnerabilities) Assessment
- Threat Analysis

SECTION2 : BCP ANALYSES

BUSINESS IMPACT ANALYSIS

- Methodology:

RISK (VULNERABILITIES) ASSESSMENT - SCENARIOS OF THREAT

- Methodology:

ANALYSIS OF RECOVERY REQUIREMENTS AND SOLUTION DESIGN

- Prediction of impact scenarios of specific threats
- Solution design in response to recovery requirements

SECTION 3 : CAMPUS IMPLEMENTATION OF BCP MANUAL

DESCRIPTION OF METHODOLOGY FOR IMPLEMENTATION

SECTION 4 : TESTING AND VALIDATION OF BCP MANUAL

DESCRIPTION OF METHODOLOGY FOR TESTING

TREATMENT OF TEST FAILURES

SECTION 5 : ON-GOING MAINTENANCE & TESTING

COMPONENTS OF A MAINTENANCE CYCLE

METHODOLOGY FOR MAINTENANCE

ONGOING MAINTENANCE TESTING - OVERSIGHT & REMEDIAL - ICQ 16

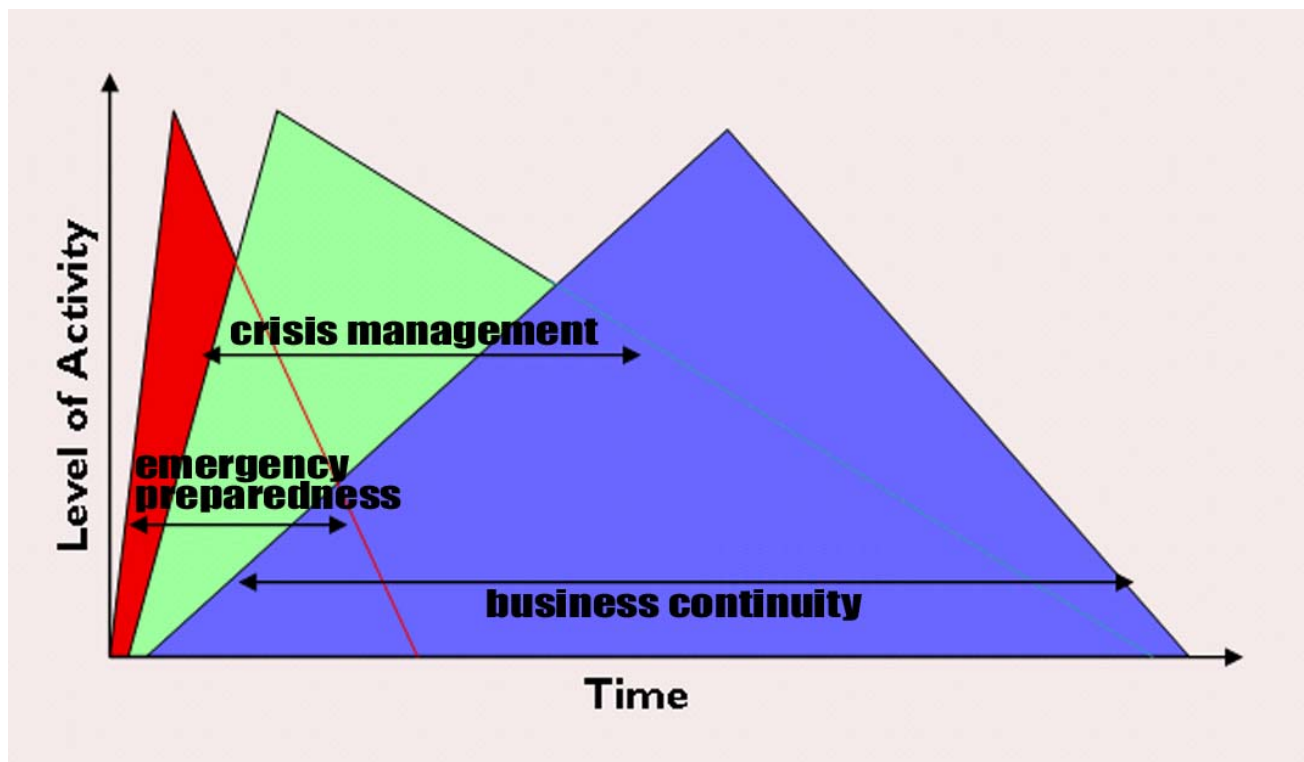
- Information update and testing
- Testing and validation of technical solutions
- Testing and verification of organization recovery procedures

RECORDS RETENTION - ICQ 20

SECTION 6 : BUSINESS CONTINUITY TRAINING

BCP Overview

- **Emergency Preparedness:** This phase involves undertaking activities to reduce and prevent death, injury, and loss of property/assets during a disaster by applying consistent and ongoing prevention and mitigation measures.
- **Crisis Management:** This phase involves the emergency response of appropriate personnel to a disaster. The SJSU Emergency Operations Plan describes the various activities, roles and responsibilities of the emergency personnel.
- **Business Continuity:** This phase involves restarting mission-critical (essential) business operations after a major disruption occurs.



SJSU Business Continuity Planning (BCP) is the creation of a logistical plan for how the University will partially or completely restore certain interrupted **essential/critical** departments (functions) within a predetermined time after a disaster or disruption.

The intended purpose of BCP is to ensure business continuity, i.e. to provide a detailed methodology governing how business is restored after a disaster, including *local* incidents like building fires, *regional* incidents like earthquakes, or *national* incidents like pandemic illnesses.

BCP Guiding Principles

San Jose State University has adopted the following Principles for the guidance of the responsible authorities for the development, and management of deployment of the Business Continuity Plan.

Continuity of student learning- Ensure access to and consistent delivery of, academic education and related support services to students (existing and prospective) within the current and projected capacity of the University.

Health and well-being of employees – Ensure the health, safety, and well-being of University employees through policy, work-place practices, and employee benefits programs.

Protection and preservation of University assets – Ensure that measures are in place and readily implemented for the protection and preservation of physical, financial, intellectual, and intangible properties and assets of the University – including its reputation, public relations, and accumulated good-will.

Strategies and procedures enable the effective and efficient deployment of institutional assets and resources in support of a business continuity response to a risk occurrence.

Critical functions – Maintain to the extent of available resources those functions of the University that, when not delivered or not performed within a specified period of time would result in the unmanageable curtailment, suspension, or termination of University operations or parts thereof that would place at risk:

- the health and safety of persons, other living things, or entities; or
- a University Academic/Administrative/Research unit on which students, employees, other University units, or the community-at-large are dependent.

Communication and information – The University will distribute timely, comprehensive, and accurate information about the status of University operations, the current risk incident, and related risk mitigation information and resources available to employees, students, and, as appropriate, the community at large.

SECTION 1: FRAMEWORK

AUTHORITY

The campus BCP Project is mandated by the CSU Chancellor's Office Executive Order #1014. The VP of Administration and Finance has the delegated authority by the SJSU President to be in charge of campus-wide BCP.

CONCEPT OF OPERATIONS

BCP Conditions of Activation, Operation and Termination

Emergency operations have established methodologies for emergency response. These include roles and activities that define initial emergency response (activation phase), resolution of the emergency situation (termination phase) and return to normal operations (recovery phase). BCP activation will work with emergency management, meaning that the Emergency Director will have authority of control for the BCP activation and operation phases for all operations of the organization. Upon the Emergency Director's declaration of BCP activation, the BCP Coordinator coordinates BCP operation with the EOC Section Chiefs and the Emergency Management Recovery Team (Recovery Manager and Recovery Coordinators).

BCP Conditions of Activation

The Emergency Director declares BCP activation to initiate resumption and recovery services and communication. BCP activation puts into action plans to sustain critical processes and services. Mission recovery includes the recovery of facilities, infrastructure and services required for the return to normal operations.

BCP Conditions of Operation

BCP operations initiate upon BCP activation as contingency plans and recovery operations begin. Contingency operations run in conjunction with emergency management recovery operations through to completion of the BCP operations phase. Mission recovery includes the recovery of facilities, infrastructure and services required for the return to normal operations.

BCP Conditions of Termination

BCP operations can be terminated when facilities, infrastructure and services are sustainable and reliable. The Emergency Director declares that normal operations may resume upon consensus from the BCP Coordinator, Section Chiefs, Recovery Manager and Recovery Coordinators.

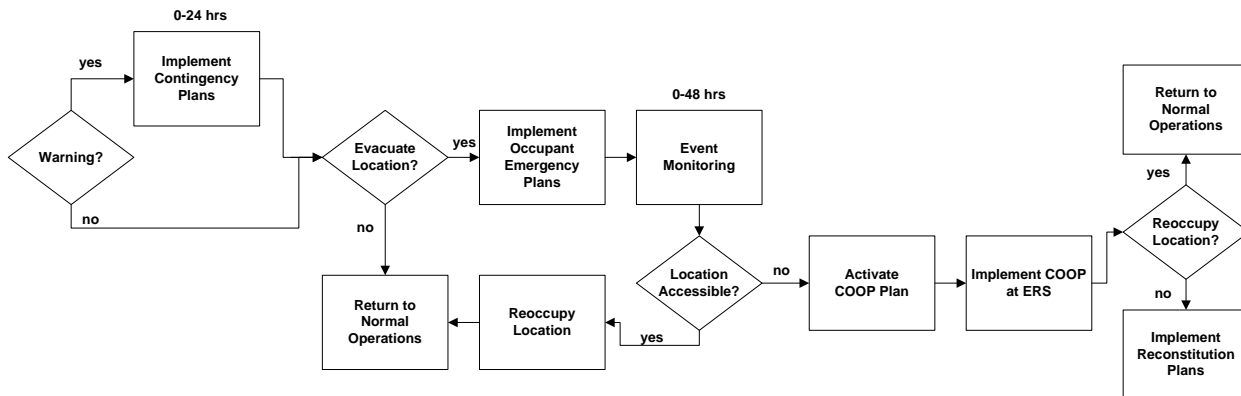
Critical Issues

BCP operations are dependent on planning, communication, coordination and security. Critical issues include: personnel safety, environmental safety, physical security, cyber security, identification of critical personnel, identification of critical assets, identification of critical processes, identification of vital records, established command structure, managed command communications, managed public information and safety communications, managed emergency management and BCP internal communications, prioritization of activities, training, testing and continual improvement, and timely implementation.

The SJSU BCP Toolkit includes a section describing in detail the SJSU methodology for activating BCP - below is an excerpt.

Orderly alert and notification depends upon the amount of warning received, whether employees are on duty at university locations and the extent of risk for university employees or locations.

Any disaster that adversely affects the university's ability to perform essential functions requires activation of the BCP.



University employees will be contacted with alert and notification information using variety of communication resources/contact lists (e.g., Alert-SJSU, Emergency Personnel Roster; Response/Recovery Team Personnel form, etc.).

In the event of a vacancy in the position of President, succession lines have been established. Presidential Directive # 2009-03 serves as the official delegation of both authority and responsibility to the following administrators to make decisions on behalf of the President in a disaster or an emergency in which the President is absent or disabled. The "Chain of Command" is as follows:

1. President
2. Provost and Vice President for Academic Affairs
3. Vice President for Administration and Finance/CFO
4. Vice President for Student Affairs
5. Vice President for University Advancement
6. President's Chief of Staff

The following should be added to the "Chain of Command" for major disaster or emergency situations:

7. Vice Provost for Academic Planning and Budgets
8. Chief of Police
9. Vice President for Information Technology and Chief Information Officer

University employees with select knowledge, skills and abilities are required to perform the tasks associated with the university's essential functions. The following personnel are identified as critical members of the Emergency Response Group (ERG).

BCP COMMUNICATION AND MANAGEMENT

- SJSU BCP is sponsored by the President's Cabinet; is under the delegated authority of the VP of Administration and Finance; is planned and coordinated by the campus BCP Coordinator; is executed at the divisional level by the divisional managers under the oversight of the Division Vice Presidents.
- The campus BC Coordinator serves as the Chair of the Campus Business Continuity Committee (BCSC)
- Each campus Division has a representative as permanent member on the BCSC.
- BCSC is scheduled to meet once a month. These meetings are designed to be work sessions
 - to review and approve the BCP Master Plan
 - to plan and prioritize the execution of BCP tasks
 - to assign BCP tasks to the Divisions
 - to review divisional BCP status reports
 - to review and approve the completion of BCP tasks
 - to make decisions on BCP functions and issues, such as training, resources planning, change management, etc.
- The BCSC Chair is responsible for preparing the summary report for each meeting, which then will be emailed to all BCSC members and also posted to the SJSU BCP website.
- The Office of the VP of Administration & Finance is responsible for maintaining the SJSU BCP website.
- On an ongoing basis, the BCSC Chair will update the VP of Administration & Finance on campus BCP issues and progress. The VP of Administration & Finance will be responsible for briefing the President's Cabinet.
- The BCSC members are responsible for disseminating BCP information discussed during the BCSC meetings back to all levels of management within their respective Divisions.
- The BCSC members are responsible for identifying managers within their respective Divisions who will execute the BCP tasks as assigned; and for tracking the work-in-progress and giving status reports to BCSC in the monthly meetings.
- The Division Vice Presidents and their BCSC representatives have total control over the management of their staff to implement and execute the assigned BCP tasks.
- Bi-annually the campus BC Coordinator will prepare a status report on BCP for the President's Cabinet.
- The VP of Administration & Finance is responsible for solving budget issues related to BCP implementation for the campus.
- The campus BC Coordinator is responsible for keeping BCP records for the campus. Divisional BCSC representatives are responsible for keeping BCP records for their respective Divisions, or they may delegate the record keeping function to another manager in their Divisions.

CREATION OF BCP LOGISTICAL MANUALS

A product of the BCP Project is a formal manual available for reference before, during, and after disruptions. Its purpose is to reduce adverse impacts determined by both the disruption's scope (who and what it affects and to what extent) and duration (e.g., hours, days, months).

In other words, the end product will be one “campus-wide BCP manual” for the entire campus, in which the “departmental BCPs” of each campus department will be basic building blocks.

A BCP manual for an operation at a minimum would be a printed manual, stored safely away from the primary work location, containing:

- names, addresses, and phone numbers of emergency management staff, general staff members, clients, and vendors.
- location of the offsite data backup storage media
- copies of insurance contracts, and other critical materials necessary for organizational survival.

At its most complex, a BCP manual for a large Division may include

- a secondary work site
- technical requirements and readiness
- regulatory reporting requirements
- work recovery measures
- the means to reestablish physical records
- the means to establish a new supply chain
- or the means to establish new operation centers

A BCP manual must be realistic and easy to use during a crisis. As such, BCP sits alongside crisis management and disaster recovery planning and is a part of an organization's overall risk management.

PHASED APPROACH TO DEVELOPING THE SJSU BCP:

The BCP function at SJSU is an ongoing project with no termination, and it will go through successive *cycles*. The first cycle is the inception cycle, i.e. the creation of the Business Continuity Plan for the first time. Subsequent cycles will be for BCP maintenance, in which the Plan is revised, updated, and re-validated.

The current SJSU BCP Project's Inception Cycle will have 3 main Phases:

Phase 1: Office of VP of Admin to create the campus-wide BCP as a top-down framework

1. Create a Business Continuity Steering Committee (BCSC) composed of senior management.
2. Business Impact Analysis: Identify essential campus departments that have top priority to be restored after a disaster.
3. Create tools to support the BCP Project, e.g. analysis templates, communication tools, instructions documents, etc.
4. Identify key managers from all campus departments that will work on BCP.
5. Design methodologies for testing.
6. Design BCP maintenance cycle.

Phase 2: Campus community to add details to the campus-wide BCP

1. BCSC to validate and finalize the draft of the campus-wide BCP
2. BCP tools and templates are deployed to all campus departments
3. Each campus department to create their "individual BCP" by filling out BCP templates
4. "Individual BCPs" are reviewed and finalized at Divisional level, and submitted to BCSC

Phase 3: Consolidation of individual BCPs into campus-wide BCP

1. BCSC to review and approve the submitted "individual BCPs"
2. BCSC to deploy the schedule for testing to all campus departments
3. BCSC to monitor the testing, assess results, and recommend remedial actions.
4. BCSC to start a new BCP cycle for ongoing maintenance (revising, updating, testing)
 - a. Strengthen Threat Analysis with more specific scenario projections
 - b. Strengthen Recovery Solutions and Planned Redundancies - if budget permits

SCHEDULE OF CURRENT BCP INCEPTION CYCLE (2009 - 2011)

	by Office of VP of Admin	by BCSC	by individual campus departments
Create BCP framework, project management, steering committee, templates, communication tools, etc.	in Phase 1		
Threats Analysis	in Phase 1, not differentiating the specific causes/threats, but assuming a major and state-level disaster	in Phase 3, will refine BCP with specific scenario projections	
Business Impact Analysis	in Phase 1, a detailed top down assessment is made	in Phase 2, review and validate	in Phase 2, give feedback to BCSC
Concept of Operations - Chain of command in BCP execution to restore campus business	in Phase 1, a detailed top down assessment is made	in Phase 2, review and validate	
Risk Assessment / Recovery Requirements			in Phase 2, fill out templates to create "individual BCPs"
Solution design			in Phase 2, fill out templates to create "individual BCPs"
Validation and consolidation into campus-wide BCP	in Phase 3		
Organizational acceptance	in Phase 3: finalization and approval		
Implementation at departmental level	in Phase 3: monitoring and oversight		in Phase 3: execution
Testing	in Phase 3: monitoring and oversight		in Phase 3: execution
Maintenance (new BCP cycle) Information update and testing Testing and verification of technical solutions Testing and verification of recovery procedures Treatment of test failures	next BCP cycle		

OVERVIEW OF METHODOLOGY TO DEVELOP THE BCP LOGISTICAL MANUAL

The development of a BCP manual has 4 main steps:

1. Analysis:
 - Business Impact Analysis and Risk Assessment
 - Recovery Requirement and Solution Design
2. Implementation
3. Testing and organization validation
4. Maintenance

There are a number of other considerations that could be included:

- Risk Identification Matrix
- Roles and Responsibilities (ensuring names are left out but titles are included, e.g. HR Manager).
- Identification of top risks and mitigating strategies.
- Considerations for resource reallocation e.g. skills matrix for larger organizations.

OVERVIEW OF MAIN TYPES OF RISK ANALYSIS

- Business Impact Analysis is for identifying critical and essential departments/functions that are needed to restore the teaching function to SJSU.
- Risk (Vulnerabilities) Assessment is to identify the main vulnerabilities of each essential department; and to design mitigating solutions.
- Threat Analysis is for projecting disaster scenarios and identifying the corresponding vulnerabilities of each essential department/function; and to design mitigating solutions. In other words, Threat Analysis is basically risk assessment for specific scenarios.

SECTION2 : BCP ANALYSES

BUSINESS IMPACT ANALYSIS (BIA)

An impact analysis results in the differentiation between critical (urgent) and non-critical (non-urgent) organization functions/ activities. A function may be considered critical if the implications for stakeholders of damage to the organization resulting are regarded as unacceptable.

Perceptions of the acceptability of disruption may be modified by the cost of establishing and maintaining appropriate business or technical recovery solutions. A function may also be considered critical if dictated by law.

METHODOLOGY:

For the purpose of restoring the University to basic functionality, the following impacts are considered as top priorities:

- A. Disruption of teaching
- B. Disruption of research
- C. Loss of faculty
- D. Loss of staff
- E. Loss of students
- F. Well-being of faculty members or staff affected
- G. Well-being of students affected
- H. Payment deadlines unmet by campus
- I. Loss of revenue to campus
- J. Legal or regulatory obligations unmet by campus
- K. Legal harm to the University
- L. Loss of reputation
- M. Impact on other campus unit(s)
- N. Impact on important business partner(s) or academic collaborations
- O. Data collected prior to the event is unrecoverable
- P. Data available or collected after the event is unavailable
- Q. Additional costs incurred to recover unprocessed data or transactions

In BCP Phase 1, this analysis is done for all campus departments by the Office of the VP of Administration. In Phase 2, the analysis is reviewed and strengthened by the BCSC. In Phase 3, it will incorporate feedback from the campus departments, and then it will be validated and approved by the BCSC.

The SJSU BCP Toolkit includes a section to guide campus managers to do BIA in detail.

RISK (VULNERABILITIES) ASSESSMENT - SCENARIOS OF THREAT

After the impact analysis is done, departments that are critical to business restoration are identified. The next step is to assess if these departments can be reliably restarted after a disaster.

METHODOLOGY:

Risk/Vulnerabilities Assessment involves identifying, analyzing, and weighing all the potential risk scenarios, i.e. threats and hazards to the University's internal and external environment. It discovers if a campus department or business unit is vulnerable to risk scenarios such as weather related events, HVAC failure, Internal/External Security vulnerabilities and local area hazards. It allows a manager to document what mitigating actions have been taken to manage these exposures.

By identifying the threats that currently are being mitigated verses threats that are not, a business unit can compile a list of recommendations for improvement. Such a list is the foundation of the Solution Design step.

The process of identifying risks/threats, probability of occurrence, the vulnerability to each risk/threat and the potential impact that could be caused, is necessary to prepare preventative measures and create recovery strategies.

Risk identification also provides a number of other advantages including:

- Exposes previously overlooked vulnerabilities that need to be addressed by plans and procedures
- Identifies where preventative measures are lacking or need reevaluated
- Can point out the importance of contingency planning to get staff and management on board
- Will assist in documenting interdependencies between departments and increase communication between internal groups. Can also point out single points of failures between critical departments

For the ease of this process, categories of risk have been created to focus the thought process. In the attached Risk Assessment Survey, the categories include, Natural Risks, Man-Made (Human) Risks, and Environmental Risks. These are certainly not requirements, and should not be considered to be constraining. If a risk is not listed, you may add it to your analysis.

Categorizing Risks / Threats

The nature of a risk/threat should be determined, regardless of the type. Factors to consider should include (but not limited to):

- Geographic Location
- Weather Patterns for the Area and Surrounding Areas
- Internal Hazards (HVAC, Facility Security, Access, etc)
- Proximity to Local Response/Support Units
- External Hazards (neighboring Highways, Plants, etc)

Potential exposures may be classified as:

- Facility Related: Bomb Threat, Chemical Spills, Civil Disturbance, Electrical Failure, Fire, HVAC Failure, Water Leaks, Work Stoppage / Strike
- Technology Related: Human Error, Loss of Telecommunications, Data Center Outage, Lost / Corrupted Data, Loss of Local Network Services, Power Failure, Prolonged Technology Outage, UPS / Generator Loss of service.
- Weather Related: Earthquake, Flood / Flash Flood, Hurricanes / Tropical Storms, Severe Thunderstorms, Tornado, Winter Storms

Listing of Threats

Part of the risk analysis process is to review the types of disruptive events that can affect the normal running of the organization.

There are many potential disruptive events and the impact and probability level must be assessed to give a sound basis for progress. To assist with this process the following list of potential events has been produced:

Environmental Disasters

- Tornado
- Hurricane
- Flood
- Drought
- Earthquake
- Electrical storms
- Fire
- Subsidence and Landslides
- Freezing Conditions
- Contamination and Environmental Hazards
- Epidemic

Organized and/or Deliberate Disruption

- Act of terrorism
- Act of Sabotage
- Act of war
- Theft
- Arson
- Labor Disputes / Industrial Action

Loss of Utilities and Services

- Electrical power failure
- Loss of gas supply
- Loss of water supply
- Petroleum and oil shortage
- Communications services breakdown
- Loss of drainage/waste removal

Equipment or System Failure

- Internal power failure
- Air conditioning failure
- Cooling plant failure
- Equipment failure (excluding IT hardware)
- IT system failure

Other Emergency Situations

- Workplace violence
- Neighborhood hazard

Although not a complete list, it does give a good idea of the wide variety of potential threats.

The SJSU BCP Toolkit includes a section to guide campus managers to do Risk/Vulnerabilities Assessment in detail.

ANALYSIS OF RECOVERY REQUIREMENTS AND SOLUTION DESIGN

After the completion of the risk assessment phase, the business and technical plan requirements are documented in order to commence the implementation phase.

Recovery requirements consist of the following information:

- The business requirements for recovery of the critical function, and/or
- The technical requirements for recovery of the critical function

For an office-based, IT intensive business, the plan requirements may cover the following elements which may be classed as ICE (In Case of Emergency) Data:

- The individuals involved in the recovery effort along with their contact and technical details
- The applications and application data required for the alternative location to resume critical business functions
- The manual workaround solutions
- The maximum outage allowed for the applications
- The peripheral requirements like printers, copier, fax machine, calculators, paper, pens etc.
- The numbers and types of desks, whether dedicated or shared, required outside of the primary business location in the alternative location

Other business environments, such as distribution, warehousing, etc. will need to cover these elements, but are likely to have additional issues to manage following a disruptive event.

METHODOLOGY:

Prediction of impact scenarios of specific threats

After defining potential threats, documenting the impact scenarios that form the basis of the business recovery plan is recommended. In general, planning for the most wide-reaching disaster or disturbance is preferable to planning for a smaller scale problem, as almost all smaller scale problems are partial elements of larger disasters.

A typical impact scenario like 'Building Loss' will most likely encompass all critical business functions, and the worst potential outcome from any potential threat. A business continuity plan may also document additional impact scenarios if an organization has more than one building.

Solution design in response to recovery requirements

The goal of the solution design phase is to identify the most cost effective disaster recovery solution that meets two main requirements from the impact analysis stage.

For IT applications, this is commonly expressed as:

1. The minimum application and application data requirements
2. The time frame in which the minimum application and application data must be available

Disaster recovery plans are also required outside of the IT applications domain. For example, information in hard copy format, identification of trained backup staff, etc.

This BCP phase mainly draws on the Disaster Recovery planning methodology, which is already fully covered by the SJSU Emergency Operations Plan. The Emergency Operations Plan includes:

- the crisis management command structure
- the location of a alternative work site (when necessary)
- telecommunication architecture between primary and alternative work site
- data replication methodology between primary and alternative work site
- the application and software required at the alternative work site, and
- the type of physical data requirements at the alternative work site.

The SJSU BCP Toolkit includes a section to guide campus managers to do Analysis of Recovery Requirements and Solution Design in detail.

SECTION 3 : IMPLEMENTATION OF BCP MANUAL

The implementation phase is the execution of the design elements identified in the solution design phase. "Work package" testing is the testing of individual functions. It may take place during the implementation of the solution. However, work package testing does not take the place of organizational testing.

METHODOLOGY:

There are 8 major steps associated with BCP implementation. Note that these planning/preparedness activities need to be completed ahead of time.

1. **Prepare the departmental BCP infrastructure resources.** This involves manpower, and the resources required in the BCP Solution Designs. It is important that the characteristics of the environment. i.e., the production infrastructure needs to be in place. This step is under the oversight of BCSC.
2. **Coordinate with the departments involved in implementation.** At a minimum, there needs to be clear communication between: the campus BC Coordinator, BCSC, and the essential campus department or business unit where BCP is going into deployment. The communication should include (1) start and end date of implementation, (2) status reporting requirement, (3) listing of objectives, (4) designation of implementer - usually the department manager/director or the BCSC representative of that division.
3. **Training on Implementation.** This training may be necessary, depending on the complexity of the tasks, the business functions, and the campus department. This type of training could be completed in advance, but the further out the training is held, the less information will be retained when implementation rolls around. Training that takes place close to the time of implementation should be made part of the actual implementation plan. The manager of the campus department or business unit is responsible for training his/her staff, and the campus BC Coordinator is responsible for providing support and answering how-to questions.
4. **Implementing the solution.** Make sure that all objectives identified in Step 2 above are implemented successfully.
5. **Status report.** As the implementation may span several months, status reports should be given to the Divisional BCSC representative, who will discuss it in the monthly BCSC meetings.
6. **Perform final verification of implementation.** All check list items should be checked. The Divisional BCSC representative confirms completion in the final report to BCSC for BCSC approval. Campus BC Coordinator will report to the President's Cabinet that implementation is done for that Division.
7. **Ongoing maintenance.** After completion of implementation, BCP maintenance will start. The campus BC Coordinator and the BCSC are responsible for planning and scheduling the new BC maintenance cycle.
8. **Ongoing monitoring.** The campus BC Coordinator is responsible for monitoring campus-wide BCP compliance and reporting back to the President's cabinet.

SECTION 4: TESTING AND VALIDATION OF BCP MANUAL

The purpose of testing is to achieve organizational acceptance that the business continuity solution satisfies the organization's recovery requirements. Plans may fail to meet expectations due to insufficient or inaccurate recovery requirements, solution design flaws, or solution implementation errors.

Testing may include:

- Crisis command team call-out testing
- Application test
- Business process test
- Technical swing test from primary to alternative work locations
- Technical swing test from alternative to primary work locations

At minimum, testing is generally conducted on an annual schedule. Problems identified in the initial testing phase may be rolled up into the maintenance phase and retested during the next test cycle.

METHODOLOGY:

Testing is to make sure that the business continuity plans deal effectively with potential disruptions or disasters. It is to ascertain that all the essential business elements of SJSU can be restored using the business continuity plans, and that they will stand up to an audit. A comprehensive, multi-dimensional and ongoing BCP testing program is the only way to achieve such assurance.

Business Continuity Plans can be progressively tested to confirm that maximum benefit is derived. The Methodology consists of the following phases:

Plan Audit

The campus BCP Coordinator and the BCSC will comment on the overall effectiveness of the plans and may suggest that adjustment are made to the plans before any further test phases are commenced.

Passive Walk Through

This Phase will increase the awareness for all participants concerning their roles. Test Modules with checklists will be used to ensure a constant and structured approach.

Scenario Workshop

A Test Scenario will be compiled based upon realistic circumstances to SJSU and potential threats. The participants will be asked to invoke the plans and to perform their individual roles in order to recover from the scenario.

Physical Test

As a result of the Scenario Workshop, the Physical Test will involve the actual attendees at the recovery site, and that the Recovery Requirements are met according to the Solution Designs.

Live Simulation Test

As a result of the preceding phases, a live Simulation Test is the ultimate proof of the effectiveness of the plans. The Live Simulation Test will only be attempted when a high degree of confidence has been generated by the successful completion of the previous phases. To minimize disruption to campus business, the Live Test will be rotated through essential campus departments, instead of deploying all at once.

For each essential campus department, a Recovery Test Status Report will be produced at the end of each phase of the test with recommendations for improvement in the short, medium and long term provided with an ongoing maintenance program. All departmental reports will be reviewed and signed-off by the campus BC Coordinator and the BCSC, with recommendation of remedial actions.

THE TESTING PROGRAMS ARE DESIGNED TO:

- Make the test experience measurable against BCP objectives
- Validate SJSU's recovery objectives
- Design a long range testing program with clear, usable management metrics
- Prepare meaningful test scenarios, learning objectives, and success criteria
- Manage the staging and execution of scheduled tests
- Use command center tools to capture auditable team actions, communication details, improvements and lessons learned during the test
- Develop pre- and post-test action plans to fill the gaps, prioritize organizational issues and plan improvements to business continuity program.
- Recommend training and awareness curricula for test participants
- Review/Analyze the integration of plan maintenance and testing
- Develop training programs for future BCP test managers.

TREATMENT OF TEST FAILURES

Issues found during the testing phase often must be reintroduced to the analysis phase. Remedial actions must be reported back to BCSC to review and approve.

FREQUENCY OF TESTING

Each essential unit will control their own BCP testing, under the oversight of the divisional VP and the divisional BCP representative. The selection of which tests to run, and the time frame in which to run it, will be recommended by BCSC and finalized by the Division's senior management. The campus will follow the industry standard of requiring each essential unit to have one complete BCP testing at least once every 7-years.

SECTION 5: ON-GOING MAINTENANCE TESTING AND NEW BCP CYCLES

A BCP is a dynamic document that will need to be reviewed and maintained on a periodic, scheduled basis. The adequacy of even the most well developed BCP remains unknown until it is tested. In many cases this only occurs when it is needed, at which time it may not have the desired outcomes and/or be out of date. The maintenance of a BCP is based on the key concepts of understanding, resourcing and assurance.

- Understanding - staff need to understand and implement business continuity policies and procedures.
- Resourcing - resources to perform critical business functions need to be adequate, or access is available to alternate adequate resources.
- Assurance - the performance of a BCP needs to be verified through regular monitoring, review, and testing.

A very effective way of maintaining a BCP is through testing scenarios with outcomes for improvement being incorporated into the BCP. Testing different scenarios is an effective method of training. It increases staff awareness of the BCP, can help identify gaps between the BCP and staff's interpretation of the BCP, and can improve staff confidence in implementing the BCP.

Testing different scenarios will also highlight resource and logistical gaps (for example, how to relocate essential staff). The overall adequacy of the BCP during the testing scenario may also be a good indicator of the adequacy of the testing cycle.

COMPONENTS OF A MAINTENANCE CYCLE

Maintenance of a BCP manual is broken down into three periodic activities.

1. The first activity is the confirmation of information in the Manual, roll out to ALL staff for awareness and specific training for individuals whose roles are identified as critical in response and recovery.
2. The second activity is the testing and verification of technical solutions established for recovery operations.
3. The third activity is the testing and verification of documented organization recovery procedures. An annual maintenance cycle is typical.

METHODOLOGY OF BCP REVISIONS, OVERSIGHT AND REMEDIAL ACTIONS

Review of the plan and plan components are conducted annually. In addition the SJSU Business Continuity Plan is re-evaluated when any of the following occur:

- Regulatory changes
- Resources or organizational structures change
- Funding or budget level changes
- When changes to the threat environment occur
- When substantive changes to the organization's IT infrastructure take place
- After an exercise, to incorporate findings.

1. Change Management

The responsible party for changes after the finalization of the current document is the Document Owner. Proposals for improvement of the management procedure are addressed to the document owner, who evaluates all the submitted proposals. Changes should be reported to the BCSC, and tracked by the campus BC Coordinator.

2. Business Continuity Preparedness

Refresher training is provided via instructional materials online. New staff who will have plan responsibilities will receive training shortly after they are hired. Campus personnel of essential departments and business units are trained to the point that they are comfortable to execute their respective business continuity responsibilities. It is the responsibility of the unit manager to make sure that designated personnel are properly trained on BCP. The Divisional BCSC Representative has oversight responsibility over their Division.

Training encompasses:

- Purpose of the Business Continuity Plan
- Business Continuity team co-ordination and communication
- Reporting procedures
- Security arrangements
- Team specific processes
- Individual responsibilities

3. BCP Validation

Validation of the ability to recover critical business functions as intended is an essential component of effective business continuity maintenance management. Such validation is conducted periodically, with the scope and frequency determined by the criticality of the business functions, under oversight of BCSC. In addition, such testing identifies the need to modify the SJSU Business Continuity Plan and other aspects of business continuity management in response to changes in business functions, responsibilities, systems, software, hardware, personnel, facilities or the external environment. The following items are incorporated when planning a validation:

Goal. The essential function of the BCP to be tested.

Objectives. The anticipated results. Objectives should be specific, measurable, achievable, realistic and timely.

Scope. Identifies the departments or organizations involved, the critical business function, the geographical area, the test conditions and presentation.

Artificial aspects and assumptions. Defines which exercise aspects are artificial or assumed, such as background information, procedures to be followed, and equipment availability.

Participant Instructions. Explains that the exercise provides an opportunity to test the BCP before an actual disaster.

Exercise Narrative. Gives participants the necessary background information, sets the environment and prepares participants for action. It is important to include factors such as time, location, method of discovery and sequence of events, whether events are finished or still in progress, initial damage reports and any external conditions.

Testing and Post-Exercise Evaluation. The exercise is monitored impartially to determine whether objectives were achieved. Participants' performance, including attitude, decisiveness, command, coordination, communication, and control are assessed. Debriefing is short, yet comprehensive; explaining what did and did not work, emphasizing successes and opportunities for improvement. Participant feedback will also be incorporated in the exercise evaluation. The campus Business Continuity Coordinator is responsible for records keeping for the exercise.

INFORMATION UPDATE AND TESTING

All organizations change over time, therefore a BCP manual must change to stay relevant to the organization. Once data accuracy is verified, normally a call tree test is conducted to evaluate the notification plan's efficiency as well as the accuracy of the contact data. Some types of changes that should be identified and updated in the manual include:

- Staffing changes
- Departmental changes like new, closed or fundamentally changed departments.
- Changes in organization's structure or mission statement
- Changes to important clients, emergency personnel and their contact details
- Changes to important vendors/suppliers and their contact details

TESTING AND VALIDATION OF TECHNICAL SOLUTIONS

As a part of ongoing maintenance, any specialized technical deployments must be checked for functionality. Some checks include:

- Virus definition distribution (IT)
- Application security and service patch distribution (IT)
- Hardware operability check
- Application operability check
- Data verification

TESTING AND VERIFICATION OF ORGANIZATION RECOVERY PROCEDURES

As work processes change over time, the previously documented organizational recovery procedures may no longer be suitable. Some checks include:

- Are all work processes for critical functions documented?
- Have the systems used in the execution of critical functions changed?
- Are the documented work checklists meaningful and accurate for staff?
- Do the documented work process recovery tasks and supporting disaster recovery infrastructure allow staff to recover within the predetermined recovery time objectives.

RECORDS RETENTION POLICY

The BCP Team is committed to effective records management to meet legal standards, ensure privacy, optimize the use of space, destroy outdated records in an appropriate manner, and comply with CSU policy and all applicable laws and regulations. The Records Retention Schedule provides for orderly and proper retention and destruction of all official records. Retention periods may increase by government regulation, judicial or administrative order, private or governmental contract, pending litigation or audit requirements.

Confidentiality Requirement:

Records containing confidential and personal data will be accessed only by authorized persons, maintained in secured and/or locked locations, and destroyed by appropriate methods.

Specific Responsibilities:

The University Business Continuity Coordinator is responsible for

- Implementing the records management practices consistent with this policy;
- Ensuring that access to confidential records and information is restricted;
- Ensuring destruction of inactive records that have no value upon passage of the applicable retention period;
- Ensuring that records are destroyed in a manner that is appropriate for the type of records and information involved.
- Computer records should be retained according to the retention periods as scheduled.

Disposal and Destruction of Records:

Upon determination that it is appropriate to dispose of certain records, they should be destroyed in one of the following ways:

- Recycle non-confidential paper records;
- Shred or otherwise render unreadable confidential paper records; or
- Erase or destroy electronically stored data.

Retention Period:

BCP records shall be retained for a period of 4 years, according to the CSU Guidelines for Records Retention. However, this rule shall not apply to old versions of documents that have been revised - for these documents, only the current version shall be retained.

SECTION 6: TRAINING

METHODOLOGY:

On-going training and education is imperative for those individuals in an organization, who will be involved not only in the development and implementation of the business continuity plan, but also in exercising, evaluating, maintaining, and executing the plan.

Business continuity teams need training at four distinct phases of the business continuity plan development process, namely: pre-planning, planning, post-plan development, and pre-exercise phases. These training requirements may need to be met on an on-going basis, rather than a one-time effort.

A Framework for Training Business Continuity Teams

The business continuity teams are developed based on the critical business functions identified during the business impact analysis. These teams include those which are held responsible for the continuity of critical business functions as well as recovery and resumption of critical support functions and vital records. These individuals will receive BCP training after their formal assignment as responsible for BCP of their campus department or business function.

The second concept to be clarified relates to the team membership. The team members typically develop, implement, exercise, evaluate, and maintain the plan, and execute it if necessary. However, it also may be deemed necessary to include other employees of an organization as either additional team personnel based on plans and procedures, or as alternates in case primary team members are unavailable for business continuity plan execution.

1. Pre-Planning Training and Awareness

Training for selected and potential BCP team members will begin at the start of Phase 2 of the SJSU BCP Inception Cycle, in the 4th Quarter of 2010. Where possible, our preferred method is to hire a training vendor to come and do in-classroom training on campus. Alternately, there may be online training that can be purchased and deployed over the campus network. The BCP Coordinator is currently reviewing various professional training vendors.

The training elements will include: a general overview of BCP and how it relates and augments university policies and procedures; objectives and assumptions in BCP; an overview of liabilities and regulations pertinent to the organization; business guidelines and an understanding of the core business processes; and a conceptual understanding of critical business functions, support technologies, and vital record requirements. These elements are essential foundations upon which all BCP teams may begin to build business continuity plans.

2. Planning Methodology Training

Upon completion of the pre-planning awareness training and gaining commitment from the selected and potential BCP team members, the training will focus on specific procedural aspects of developing and implementing the BCP. At this stage, the BCP team members should be trained, first and foremost, in the area of project management, which is essential for successful BCP development. This phase of training should then proceed to BCP development methodology

selected for the organization, a review of documentation standards, and necessary training in software, if selected for developing the BCP. The benefits from planning methodology training include:

- Adaptation of appropriate project management methodologies and tools, if any.
- Clear understanding of BCP terminology throughout the organization.
- Utilization of an accepted methodology throughout the organization.
- Enforcement of documentation standards throughout the organization, and
- Software training, if necessary.

This training will be delivered by the SJSU BC Coordinator, in classroom format and one-on-one, as well as online instructions. It will be mainly about how to use the BCP standard forms and templates to do departmental BIA, Risk/Vulnerabilities Assessment, Recovery Requirement, and Solution Design.

3. Plan Role and Responsibility Training

At this phase of training, the premise is that the BCP has been developed and implemented. This means that the necessary teams have been established and team members have been identified, with approvals from senior and functional area management. The teams typically include BCP teams for business functions, and BCP teams for support functions (such as facility team, data center team, telecommunications team, etc.). Alternate BCP team members and support personnel are also identified at this stage.

All of these individuals will be trained with regard to the provisions of deployment in the BCP. Although we recognize that these team members have developed and implemented the plan, training is essential in order to gain an understanding of the plan from several perspectives. These include:

- The team members specific role and responsibilities in the execution of the plan;
- Interdependencies of individual units plans;
- On-going evaluation and maintenance of units BCP; and
- A thorough understanding of the team checklists of procedures, including notification procedures.

The elements of this phase of training for the various BCP teams include: role of team leaders and team members, including alternates, business continuity plan provisions (who, what, when, where, and how), notification procedures, BCP event logging procedures, on-going BCP evaluation and maintenance procedures, and post-execution review procedures.

This training will be delivered by the SJSU BC Coordinator, in classroom format and one-on-one, as well as online instructions.

4. Training on Testing, Validation, and Remedial Actions

At this stage of training, all phases of BCP have been completed and BCP team members are well trained in their roles and responsibilities in the plan. The organization must recognize, however,

that exercising the plan is essential for verification and validation of the strategies and procedures in the BCP.

While exercising the plan, in its own merit, provides unique and valuable training for the BCP team members, training must be provided with regard to the “why” and “how” of exercising the plan. After all, most BCP team members may never have gone through an exercise of this type.

Furthermore, the value of such exercises, with little or no direct productivity gains, must be demonstrated through formal and relevant education, in order to gain support from team members as well as management.

The elements of pre-exercise training include: testing methodology and scheduling, developing objectives of exercises and scenarios, plan modification and update procedures subsequent to and based on the results of the exercises, and auditing and evaluating the business continuity plan.

This training will be delivered by the SJSU BC Coordinator, in classroom format and one-on-one, as well as online instructions.