Planview Business Continuity Plan

Contents

Section 1 – Overview

OVERVIEW

This Business Continuity Plan consists of the information and procedures required for rapid recovery from an incident that prevents Planview from effectively delivering essential business services to its customers. The coordinated effort provided through use of this plan allows for the recovery process to be implemented immediately upon confirmation that such an incident has occurred and provides for a concentrated effort to re-establish operations under emergency conditions within 72 hours. This premise is based upon the plan being in a constant 'ready' or updated state and all necessary contracts with vendors being in place.

Successful recovery operations depend on:

- Training selected personnel on various aspects of the Business Continuity Plan
- Storing and securing adequate backup materials off-site
- Performing comprehensive plan exercises
- Modifying the plan as a result of the exercises
- Performing adequate cross-training to reduce reliance on key personnel
- Safeguarding vital records
- Preparing a system configuration that is viable in a disaster

PURPOSE

The purpose of the Business Continuity Plan is to coordinate recovery functions that are critical to managing and supporting the business recovery in the event of a facilities (office building) disruption or disaster. This can include short or long-term disasters or other disruptions, such as fires, floods, earthquakes, explosions, terrorism, tornadoes, extended power interruptions, hazardous chemical spills, and other natural or man-made disasters.

A disaster is defined as any event that renders a business facility inoperable or unusable to the extent that it interferes with the organization's ability to deliver essential business services.

This plan includes procedures that, if followed, assist in recovering critical operations and in maintaining the Business Continuity Plan during an emergency. It aids in ensuring organizational stability through an orderly recovery process. **This plan is not intended to be a procedure manual that covers all departmental tasks and functions; it includes only those high priority tasks required to ensure recovery of essential operations after a disaster.**

SCOPE

The Business Continuity Plan is limited in scope to recovery and business continuance from a serious disruption in activities due to non-availability of Planview's facilities. The scope of this plan is focused on localized disasters such as fires, floods, and other localized natural or man-made disasters although it could provide guidance for larger scale disasters such a war or nuclear holocaust. The Business Continuity Plan includes procedures for all phases of recovery as defined in the Business Continuity Strategy section of this document. Unless

otherwise modified, this plan does not address temporary interruptions of duration less than the time frames determined to be critical to business operations.

The major resources to be recovered using the Business Continuity Plan are:

- Customer Service and Support
- Systems and data storage
- Production applications
- Telecom, including LAN, WAN
- Business-critical functions

This Business Continuity Plan encompasses planning for most contingencies, ranging from minor disruptions to total destruction, which would require recovery at a designated recovery location or remote work.

Further, security and control considerations must become an integral part of the life cycle of each business function. As new systems are developed or existing systems are modified, security and recovery capabilities should be included in the basic design criteria, from functional description, through testing and integration, to a production environment. At each step in the developmental process, the system is evaluated in terms of the degree to which it meets requirements for security, recoverability, control, and reliability.

GOALS

The goals of this plan are:

- To minimize interruptions to the normal operations of Planview.
- To limit the extent of disruption to essential Operations
- To minimize the economic impact of the interruption to the business
- To establish alternative means of operation in advance
- To train personnel in emergency procedures
- To provide for smooth and rapid restoration of the essential Planview operations identified in this plan

ASSUMPTIONS

The Business Continuity Plan has been developed and is maintained based upon the following assumptions:

- Worst Case Interruption - The facilities are totally unusable; there is no salvageable equipment, data, documentation, etc., and the disaster occurred at the worst possible time.
- Minor Interruption - Although the plan is designed for the worst case, the ability to recover from less serious interruptions is inherent within the structure of the plan.
- Staff - Sufficient staff is available after the interrupting event to implement recovery. Staff is available to perform critical functions defined within the plans. Staff can be notified and can report to the backup site to perform critical processing, recovery, and reconstruction activities.

- Functions / Roles - The functions and roles referenced in this plan do not have to previously exist within an organization; they can be assigned to one or more individuals as new responsibilities or delegated to an external third party if funding for such services can be arranged and allocated.

Section 2 – Disaster Declaration

DECLARING A DISASTER

A disaster declaration is made when any business interruption results in a decision to mobilize either a portion of or the entire organization. The declaration is made to initiate a recovery of some or all of the interrupted business functions at a recovery site.

INITIAL NOTIFICATION

The plan has been designed to handle a worst-case processing interruption: i.e. total destruction of the Planview Headquarters facility located in Austin Texas or other Planview office location. Because problems may occur in varying degrees, each situation requires careful consideration before a decision can be made regarding disaster qualification.

Initial disaster notification can come from:

- Building security
- Police or fire departments
- Computer operations personnel
- Other employees
- Customers/clients

ESTIMATING DURATION OF OUTAGE

The Business Continuity Coordinator is expected to qualify the disaster and recommend the level of the disaster to be initiated. In order to make a realistic decision, the outage duration must be a realistic estimate and not an optimistic expectation. Certain factors and criteria affect the qualification process, and they must be weighed to decide whether to mobilize the Contingency Organization. Some considerations may include the following:

- Time period, day of the week or month, time of the year, accounting requirements, peak processing period, etc.
- Nature of interrupting event and confidence in estimated time to repair
- Nature of threat, i.e., bomb scare or actual event
- Non-data center-related event, i.e., caused by widespread communications failure, earthquake, toxic gas envelopment, etc.

Reliance is placed upon the Disaster Management Team to ascertain the degree of disaster and to offer the most reliable estimate for its resolution.

Once the Disaster Management Team determines the best estimate of recovery time, they immediately recommend mobilizing the Contingency Organization and invoking the recommended level of disaster.

Section 3 – Disaster Levels

DISASTER LEVELS

Disaster levels are used to quantify the length of a processing interruption and the time frame in which a disaster declaration decision must be made to the user community. These plans are designed around the critical time frames established for the recovery of critical application systems.

LEVEL 1 (PROBLEM) – Interruption for up to 8 hours

A resolution takes up to 8 hours. It involves minor equipment breakdown, partial loss of network, major program error, contaminated databases, etc.

LEVEL 2 (EMERGENCY)– Interruption for 8-48 hours

A resolution takes up to 8-48 hours. Moderate damage to facility and/or the computer equipment is observed.

LEVEL 3 (DISASTER)– Interruption for over 48 hours

A resolution takes over 48 hours and involves major facility and/or computer equipment damage. All functions and personnel are moved to a recovery site(s).

Section 4 – Planview Disaster Recovery Team Structure

DISASTER MANAGEMENT TEAM

The following teams are in place to manage disaster recovery:

- Disaster Management Team
- IT Recovery Team
- Corporate Function Team
- Crisis Management Team
- Recovery Logistics Team
- Remote Site Management Teams for Stockholm, Bangalore, and Karlshue

Contact information for team members is available to Planview employees via Office 365 (Exchange). As this is a cloud service, it would be expected to be available in the event of an incident.

Remote Site Disaster Recovery

In the event of a disaster involving one of the remote office locations for Planview, the Onsite Team Leader will manage all efforts locally while coordinating with the remainder of the Disaster Management Team.

The Onsite Team Leader will have the following local responsibilities:

- Initiate disaster recovery procedures (Section 5) and notify the Business Continuity Coordinator
- Coordinate with local emergency services and authorities
- Coordinate and communicate recovery activities with local employees
- Communicate regular updates to Disaster Management Team

In the event of a remote site disaster, the Business Continuity Coordinator is responsible for coordinating communication channels between the Onsite Team Leader and the rest of the Disaster Management Team.

DISASTER MANAGEMENT TEAM

Upon notification of a disaster, the Disaster Management Team determines the extent of the damage. The Disaster Management Team reviews the disaster's impact on various operations within the department and the feasibility of performing normal business operations at the main facility.

It is up to the Disaster Management Team to monitor all aspects of the recovery process and to receive reports from each team leader confirming recovery. Information collected during the recovery process is used for post-recovery evaluation and training.

Business Continuity Coordinator Responsibilities

The Business Continuity Coordinator has the ultimate responsibility to declare a disaster, activate the plan, and begin recovery. The Business Continuity Coordinator receives first notification of a disaster and activates the recovery process. Within one hour, the Business Continuity Coordinator notifies Executive Management.

During a disaster, the duties of the Business Continuity Coordinator include the following:

- Initiate Business Continuity proceedings and disaster declarations
- Coordinate management decisions
- Coordinate recovery activities
- Ensure the safety and well-being of on-site employees
- Document and monitor the recovery process
- Make final decisions
- Establish methods for evaluating the Business Continuity Plan
- Monitor and control all disaster-related expenses

IT RECOVERY TEAM

The IT Recovery Team is responsible for managing the day to day operations for Planview IT infrastructure and computers, which includes the following:

- Coordinate all recovery activities to re-establish processing to acceptable levels within the shortest timeframe.
- Address concerns related to technical issues of the processing site and the associated computers.
- Restore the equipment that is required to communicate with other departments within the organization and install servers, software and workstations as required.
- Restore the network, providing access to SAN, installing PCs and components, modems and printers for mission critical people and to recover critical computer infrastructure and functionality.
- Maintain the workstations, desktop computers, servers, databases, networking, and communications to employees and customers regarding outages or degradations to these systems.

Team Leader Responsibilities

- Coordinate and communicate recovery activities that are to be performed by IT Recovery Sub-Teams.
- Provide direction and support to all contingency team members of each specific functional Team within the vertical IT Recovery Team.
- Maintain morale of each functional team as the recovery process progresses.
- Account for the performance of the sub-teams
- Provide regular status and progress updates to effected parties
- Coordinate activities between the sub-teams and stakeholders
- Manage interactions with vendors

Team Leader Tasks (First 72 Hours)

- Coordinate, facilitate, and partner with Sub-Team leads to establish and maintain Business Continuity plans for all business units.
- Lead others in understanding the importance of Business Continuity Planning.
- Participate in periodic status update reviews to monitor program goals, progress, and metrics.
- Partner with key stakeholders and plan owners to resource the IT Recovery vertical team to fully maintain Business Continuity plan and exercise success.
- Collaborate with all other team leaders to maintain a consistent flow of accurate information and to provide assistance in critical areas of support.

Team Leader Tasks (After 72 Hours)

- Continue emergency recovery processes until the IT Recovery Team can achieve the recovery time objectives necessary to start up normal operations.
- Start evaluating how many employees need to be recalled for the second phase recovery efforts.

CORPORATE FUNCTION TEAM

Lead the Business Unit vertical team by providing communication and coordination to all sub-team leaders in the event of a disaster.

Team Leader Responsibilities

- Coordinate and communicate recovery activities for Corporate Functions sub-teams.
- Provide direction and support to all contingency team members of each specific functional team within the vertical Corporate Functions team.
- Maintain morale of each functional team as the recovery process progresses

Team Leader Tasks (First 72 Hours)

- Coordinate, facilitate, and partner with sub-team leads to establish and maintain Business Continuity plans for all business units.
- Lead others in understanding the importance of Business Continuity Planning.
- Participate in periodic status update reviews to monitor program goals, progress, and metrics.
- Partner with key stakeholders and plan owners to ensure that the Corporate Functions vertical team has the resources it needs to fully maintain the Business Continuity plan and exercise success.
- Collaborate with all other team leaders to maintain a consistent flow of accurate information and to provide assistance in critical areas of support.

Team Leader Tasks (After 72 Hours)

- Continue emergency recovery processes until the Corporate Functions Team can achieve the recovery time objectives necessary to start up normal operations.
- Start evaluating how many employees need to be recalled for the second phase recovery efforts.

CRISIS MANAGEMENT TEAM

Each day of the interruption, the Crisis Management Recovery Team function must be prepared to manage the dissemination of information, provide for continuation of payroll, manage individuals with special needs resulting from the crisis, handle legal issues related to the crisis, and maintain the safety and security of our property and personnel.

Team Responsibilities

- Account for all employees.
- Determine causalities, injuries, etc.
- Determine the welfare of non-hospitalized employees.
- Notify employees when they can return to work and where they will be located.
- Provide benefit assistance to employees and employees' families.
- Coordinate counseling services/EAP for employees and employees' families.
- Monitor employee well-being and needs
- Determine if legal counsel is required
- Develop company's public response to disaster
- Secure disaster site and recovery site
- Ensure all employees receive their pay on schedule
- Communicate to employees when to return to work
- Review any contracts or legal questions that may arise
- Assist Crisis Mgmt Team and/or other Units (e.g. HR) to determine any impacts on legal obligations to vendors, customers, regulatory units, and employees. Also, determine action needed to mitigate damages.

Team Tasks (First 72 Hours)

- Review and approve external communications to the media/government officials
- Review insurance coverage and coordinate with the insurance brokers and/or insurance carriers to implement 'stop loss' and recovery activities
- Coordinate purchasing exception policies and expedited contract approvals for vendors involved in restoration activities
- Ensure continued communications with governmental rules/regulations

Team Tasks (After 72 Hours)

- Review and approve external communications to the media/government officials
- Review insurance coverage and coordinate with the insurance brokers and/or insurance carriers to implement 'stop loss' and recovery activities
- Coordinate purchasing exception policies and expedited contract approvals for vendors involved in restoration activities
- Ensure continued communications with governmental rules/regulate

RECOVERY LOGISTICS TEAM

The Recovery Logistics Support Team is charged with providing logistical support for all other teams throughout the duration of the crisis.

Team Responsibilities

- Address immediate logistics issues, such as helping to establish the Disaster Command Center. Facilitate the ordering and delivery of office furniture, supplies, and equipment.
- Arrange for transportation of staff, equipment, supplies, and other necessary items between sites
- Arrange for delivery of food to staff at Command Center, Recovery Site, and any other location where personnel may be working
- Provide clerical and administrative support for all other teams.
- Advise Command Center of status and progress.
- Coordinate and communicate recovery activities for Recovery Logistics Sub-Teams.
- Provide direction and support to all contingency team members of each specific functional team within the vertical team.
- Maintain the morale of each functional team as the recovery process progresses.

Team Tasks (First 72 Hours)

- Contact appropriate maintenance/repair contractors and approved suppliers in the event of extensive facility damage. A vendor phone list is available for this task.
- Contact vendors to procure necessary equipment, software, and supplies
- Coordinate, facilitate, and partner with sub-team leads to establish and maintain Business Continuity plans for all business units.
- Lead others in understanding the importance of Continuity of Operations Planning.
- Participate in periodic status update reviews to monitor program goals, progress, and metrics.
- Partner with key stakeholders and plan owners to ensure the business unit vertical team consists of enough resources to fully maintain Continuity of Operations plan and exercise success.
- Collaborate with all other team leaders.

Team Tasks (After 72 Hours)

- Arrange for continued service and delivery of material and freight services at alternate site, if necessary
- Arrange for transportation of staff, equipment, supplies, and other necessary items between sites
- Continue emergency recovery processes until the Disaster Recovery IT Systems Team can achieve the recovery time objectives necessary to start up normal operations.

Section 5 – Disaster Recovery Plans

Disaster Recovery Plans

Given the complexity and unique nature of Planview's products, a separate, documented disaster recovery plan will be maintained for each product in the event of a disaster affecting services/causing downtime for customers.

- DR Plan – LeanKit
- DR Plan – Planview Enterprise One
- DR Plan – PPM Pro
- DR Plan – Projectplace
- DR Plan - Spigit

The following plans will be utilized for the recovery of a Planview office in order to maintain continuity of business operations in the event of a disaster:

Level 3 Plan

Level 3 - Disaster Recovery Steps		
Step	Responsibility	Description
1	Employee	Notifies supervisor immediately of issue / problem
2	Supervisor	Identifies that a level 3 disaster has occurred and immediately notifies the Business Continuity Coordinator.
3	Business Continuity Coordinator	Confirms level of disaster, determines appropriate level of action. Contacts the Disaster Management Team members, thus activating the Business Continuity Plan. If necessary, the Business Continuity Coordinator provides the time and place to set up a command center and provides additional instructions regarding other employees and the use of the recovery site.
4	Team Leaders	Upon notification that the Business Continuity Plan has been activated, place calls to all their team members and provide instructions on meeting location, and any other information from the Business Continuity Coordinator.
5	Team Leaders	Provides clear instructions to their team members. These instructions include: • Obtaining damage estimates • Estimating salvage probabilities • Performing salvage operations Estimating recovery time. • Setting up operations at the recovery site • Resuming operations under emergency conditions.
6	Team Members	Reports their findings and estimates only to their team leaders, who are their points of contact. This prevents multiple versions of loss estimates or inconsistent recovery information from reaching the Business Continuity Coordinator.
7	Team Leaders	Updates the Business Continuity Coordinator at regular intervals.
8	Business Continuity Coordinator	Oversees all sub teams and recovery efforts.
9	Business Continuity Coordinator	Determines that operations can safely and productively return to the main facility or some other permanent location. Until determination is made, operations continue under the temporary emergency conditions.
10	Business Continuity Coordinator	Notifies managers that normal operations may resume and all teams may be disbanded.

Level 2 Plan

Level 2 - Disaster Recovery Steps		
Step	Responsibility	Description
1	Employee	Notifies supervisor immediately of issue / problem
2	Supervisor	Identifies a level 2 disaster. Notify the Business Continuity Coordinator.
3	Business Continuity Coordinator	Confirms level of disaster, determines appropriate level of action. Contacts the Disaster Management Team members, thus activating the Business Continuity Plan.
4	Team Leaders	Places calls to all their team members and provide instructions on dress, meeting location, and any other information from the Business Continuity Coordinator, upon notification that the Business Continuity Plan has been activated. It is not necessary for any employee to confirm the disaster or level of disaster after initial notification.
5	Team Members	Reports their findings and estimates only to their team leaders, who are their points of contact. This prevents multiple versions of loss estimates or inconsistent recovery information from reaching the Business Continuity Coordinator.
6	Business Continuity Coordinator	Determines that operations can safely and productively return to the main facility or some other permanent location. Until determination is made, operations continue under the temporary emergency conditions.
7	Business Continuity Coordinator	Notifies managers that normal operations may resume and all teams may be disbanded.

Level 1 Plan

Level 1 - Disaster Recovery Steps		
Step	Responsibility	Description
1	Employee	Notifies supervisor immediately of issue / problem
2	Supervisor	Confirms the issue / problem. Determine appropriate action.
3	Supervisor	Communicates issue and estimated length of time to resolve.
4	Employee	Implements actions to resolve the issue / problem.
5	Supervisor	Confirms that the issue / problem is resolved.
6	Supervisor	Communicates that the issue / problem is resolved.

Section 6 – Version History / Approvals

Version History

Version	Date	Author	Description
1.0	7/1/19	Lance Wright	Initial draft

Approvals

Version	Date	Approved by
1.0	7/1/19	Lance Wright
1.0	7/15/19	Security Steering Committee

Section 7 – Glossary

Definitions

This Glossary of Terms is a partial yet ever-expanding list of industry terms. It covers key terms used in Emergency Management and Business Recovery.

Activation. The implementation of recovery procedures, activities, and plans in response to an emergency or disaster declaration.

Alternate Site. An alternate operating location to be used by business functions when the primary facilities are inaccessible.

Cold-Site. One or more data center or office space facilities equipped with sufficient pre-qualified environmental conditioning, electrical connectivity, communications access, configurable space and access to accommodate the installation and operation of equipment by critical staff required to resume business operations.

Damage Assessment. The post-incident appraisal or determination of actual effects on human, physical, economic, and natural resources.

Data Security. The securing of safeguarding of electronic information owned by an organization using technology such as security software packages and data encryption devices.

Financial Impact. An operating expense that continues following an interruption or disaster, which as a result of the event cannot be offset by income and directly affects the financial position of the organization.

Hazard Identification. The process of identifying situations or conditions that have the potential of causing injury to people, damage to property, or damage to the environment.

Hot-site. A data center facility with sufficient hardware, communications interfaces and environmentally controlled space capable of providing relatively immediate backup data processing support.

Impact Analysis. A pre-incident study to estimate the effect that specific incidents can have on an entity's operations or activities.

Incident Command System (ICS). The combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure with responsibility for the management of assigned resources to effectively accomplish stated objectives pertaining to incident as described in the document, Incident Command System.

Mass Care. The temporary housing, feeding, and care of populations displaced by a disaster.

Mitigation. Activities taken to eliminate or reduce the degree of risk to life and property from hazards, either prior to or following a disaster.

Mobilization. The activation of the recovery organization in response to an emergency or disaster declaration.

Mutual Aid Agreement. A pre-arranged agreement developed between two or more entities to render assistance to the parties of the agreement.

Needs Assessment. The identification of resources needed to restore vital functions.

Operational Impact. An impact which is not quantifiable in financial terms but its effects may be among the most severe in determining the survival of an organization following disaster.

Outage. The interruption of automated processing systems, support services or essential business operations which may result in the company's inability to provide services for some period of time.

Personal Accountability. Constant awareness of the location and function of all personnel who are within controlled access areas.

Preparedness. Activities, programs, and systems developed prior to a disaster that are used to support and enhance mitigation of, response to, and recovery from disasters.

Pre-positioned Resource. Material (i.e. equipment, forms and supplies) stored at an off-site location(s) to be used in business resumption and recovery operations.

Prevention. The process of planning for and/or implementing controls to prevent incidents and manage risks by decreasing the potential for incidents or the affects thereof which may threaten the assets of the organization.

Recovery Window. A period of time in which time sensitive business operations must be resumed.

Recovery. The process of planning for and/or implementing recovery of less time sensitive business operations and processes after critical business functions have resumed.

Response. The reaction to an incident or emergency in order to assess the level of containment and control activity required.

Restoration. The process of planning for and implementing full-scale business operations which allow the organization to return to a normal service level.

Resumption. The process of planning for and/or implementing the recovery of critical business operations immediately following an interruption or disaster.

Warm-site. A data center or office facility which is partially equipped with hardware, communications interfaces, electricity and environmental conditioning capable of providing backup operating support.

