

Tests and Exercises: Standards, Practices, Results

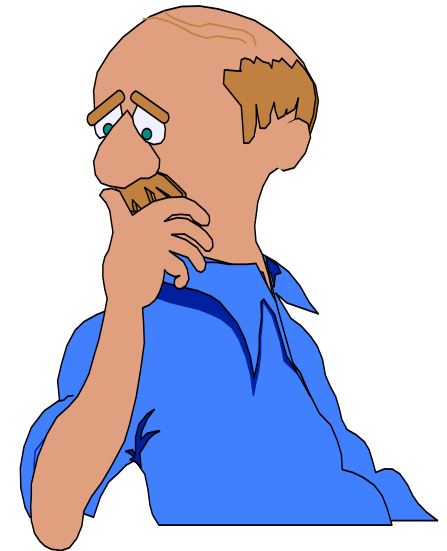
Lee Milligan, Sr. Project Manager



Today's Discussion

KEEPING PEOPLE AND INFORMATION CONNECTED®

- **To understand the impact of regulatory and standards on test requirements**
- **Testing, exercises, simulations: what do you want at the end?**
- **A quick review of types of tests and test methods**
- **Defining a standard testing process**
- **Answering your questions about testing**



“We endorse the ANSI recommended standard for private preparedness (NFPA 1600)....We also encourage the insurance and credit rating industries to look closely at a companies compliance in assessing it’s insurability and creditworthiness. We believe that compliance with the standard should define the standard of care owed by a company to it’s employees and the public for legal purposes”

Omnibus BCP Law

KEEPING PEOPLE AND INFORMATION CONNECTED®

- On 8/3/07, Congress passed and the President signed the Omnibus BCP law (Voluntary Private Sector Preparedness Accreditation and Certification Program) with provisions for public and private organizations to:
 - **Establish and maintain comprehensive BCP programs for any corporate areas where a major BCP event could significantly affect the organization's earnings or shareholder value, or directly affect the ability to provide vital community services**
 - To build, maintain, test, and support the internal BCP program
 - To **conduct an annual review of their BCP program**, including risk and impacts, **reporting their findings in the organization's annual report to the organization's stakeholders**
 - Reports and findings from within the organization concerning BCP **must be reviewed and approved jointly by the CEO and CFO, and accepted by the company's auditors.**

Setting the Standards for Auditable Testing - NFPA1600

KEEPING PEOPLE AND INFORMATION CONNECTED®

- The entity shall evaluate program plans, procedures, and capabilities through periodic reviews, testing, and exercises
- Additional reviews shall be based on post-incident analyses and reports, lessons learned, and performance evaluations
- Exercises should be designed to test individual essential elements, interrelated elements, or the entire plan(s)
- Procedures shall be established to take corrective action on any deficiency identified

Purpose: BCP audit standards applicable to financial institutions

Focus: Definition of baseline BCP requirements

Enacted by: Federal Financial Institutions Examination Council

Applicability: Applies to Financial organizations

Basis for: Many other regulations relating to financial structure

Risk monitoring and testing is the final step in the cyclical business continuity planning process. ensures that the institution's business continuity planning process remains viable through the:

- Incorporation of the BIA and risk assessment into the BCP and testing program;
- Development of an enterprise-wide testing program;
- Assignment of roles/responsibilities for implementation of the testing program;
- Completion of annual, or more frequent, tests of the BCP;
- Evaluation of the testing program and test results by senior management/BoD
- Assessment of the testing program and test results by an independent party;
- Revision of the BCP and testing program based upon changes in business operations, audit and examination recommendations, and test results.

- An emerging standard that defines a Business Continuity Management System (BCMS) providing a guideline for establishing and running a business continuity program
- Currently under review by the International Standards Organization (ISO) for adoption as an international standard
- At the present time, unclear on any US regulatory acceptance

At the same time, this standard is the first to address the discipline of a continuity program from inception through to maturation

BS25999 – The Value Proposition

KEEPING PEOPLE AND INFORMATION CONNECTED®

- Provides a **common framework**, based on internationally accepted best practices for implementing and managing business continuity
- Provides a framework **for organizations of any type, size and location**
- Improves operational **effectiveness** of a BCM organization
- Allows for the **proactive management of business risks**
- Helps demonstrate that applicable laws, regulations and contractual requirements are being observed
- Brings a **common understanding to all stakeholders**

- **The organization shall:**
 - **Develop exercises that are consistent with the scope of the BCMS**
 - **Have a program approved by top management to ensure exercises are carried out at planned intervals and when significant changes occur**
 - **Carry out a range of different exercises that, taken together, validate the whole of it's business continuity arrangements (program)**
 - **Plan exercises so that the risk of an incident occurring as a direct result of the exercise is minimized**
 - **Define the aims and objectives of every exercise**
 - **Carry out a post-exercise review of each exercise that will assess the achievement of the aims and objectives of the exercise**
 - **Produce a written report of the exercise, outcome, and feedback, including required actions**

A Process for Managing Tests

Achieving Auditability



Why Test? Why a Testing Process?

KEEPING PEOPLE AND INFORMATION CONNECTED®

- **Why Test?**
 - We want to know that our plans are accurate, and that our BCP resources are adequate
 - We want to identify and address logistical, technical, and managerial issues
 - Through testing, we want to raise BCP awareness, and strengthen support for our BCP program
- **Why a process?**
 - We want to be clear about what we're testing
 - We want our approach to testing to be consistent
 - We want the test to be auditable
 - We want records and reports to show the auditors what was tested, and what results were achieved
 - We want to establish a history of test results to illustrate and track improvement of our BC program over time

- Traceable information about the test – good books and records
 - What was tested, with what expectations, when, where, and by whom
- Verifiable information about test issue and problem follow up activities and their successful closure
- Verification of executive management knowledge of tests and test results; executive acknowledgement of test results



Specificity: What is Regulation Asking For?

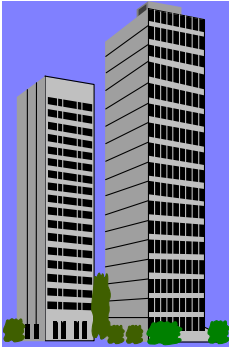
KEEPING PEOPLE AND INFORMATION CONNECTED®

- Development of a testing strategy, to show that the BCP program's recovery objectives can be achieved during an event or interruption
- Strategy should include test objectives, scripts, and schedules, and provide for review and reporting of test results
- Test scope and objectives should define what functions, systems, or processes being tested, and what constitutes a successful test

- **Orientation or walkthru** - to ensure that critical personnel are familiar with the BCP
- **Tabletop or mini-drill** - A more sophisticated walkthru, centered on an event scenario
- **Function test** - Actual mobilization at other sites in an attempt to establish communications and coordination, as set forth in the BCP
- **Full scale test** - implementation of all or portions of the BCP by processing data and transactions at a recovery site

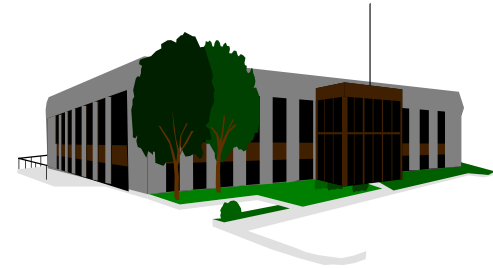


- **Here are some types of tests that you may choose to perform:**
 - **Event management/crisis management/EOC - Test or exercise focusing on how the event team(s) and their plans will perform in an actual event**
 - **Notification or call tree test - Assessment of how effective the communications/escalation processes are and how accurate the contact information is**
 - **Systems/application recovery test - Emphasis on our ability to recover critical and essential systems used by the IT customer**
 - **Business recovery test - Tests our ability to recover business departments as a result of losing our business locations**
 - **End to end - complete exercise involving event management, call tree, system and business recovery, including data recapture, data synchronization and validation, for a specific location**



Business recovery tests focus on loss of business operating location and required local technology

- Recovery of critical processes
- Recovery of supporting technology
- Validity of offsite storage programs
- Ability to reconcile or recover to data sync point



Systems recovery (DR) tests focus on loss of technical capabilities within the computer complex, and may involve business departments

- Loss of major applications and computing capability
- Validation of data integrity
- Loss of IT infrastructure
- Major IT changes/upgrades to operations systems, internal IT processes

Tactics for Testing

KEEPING PEOPLE AND INFORMATION CONNECTED®

All elements of the testing process are designed to be highly visible; plans, schedules, results are published to all involved departments, execs, BCP Steering Committee and/or Crisis teams

Decisions on what to test are based on:

Critical/essential processes documented in BCP plans

Impact of change to the process or underlying application since the previous BCP test

The length of time that has passed since the last recovery test

Business departments are responsible for testing the accuracy and functional usability of any computer applications needed to operate the business

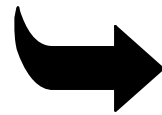
IT is responsible for supporting technology used by business, regardless of where it's placed



Test Planning Cycle - Business Recovery Test

(Example for Test Date of September 1)

KEEPING PEOPLE AND INFORMATION CONNECTED®

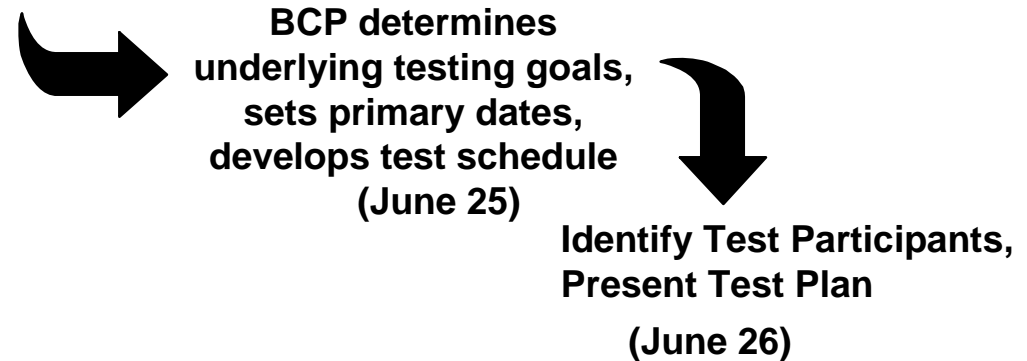


**BCP determines
underlying testing goals,
sets primary dates,
develops test schedule
(June 25)**

Test Planning Cycle - Business Recovery Test

(Example for Test Date of September 1)

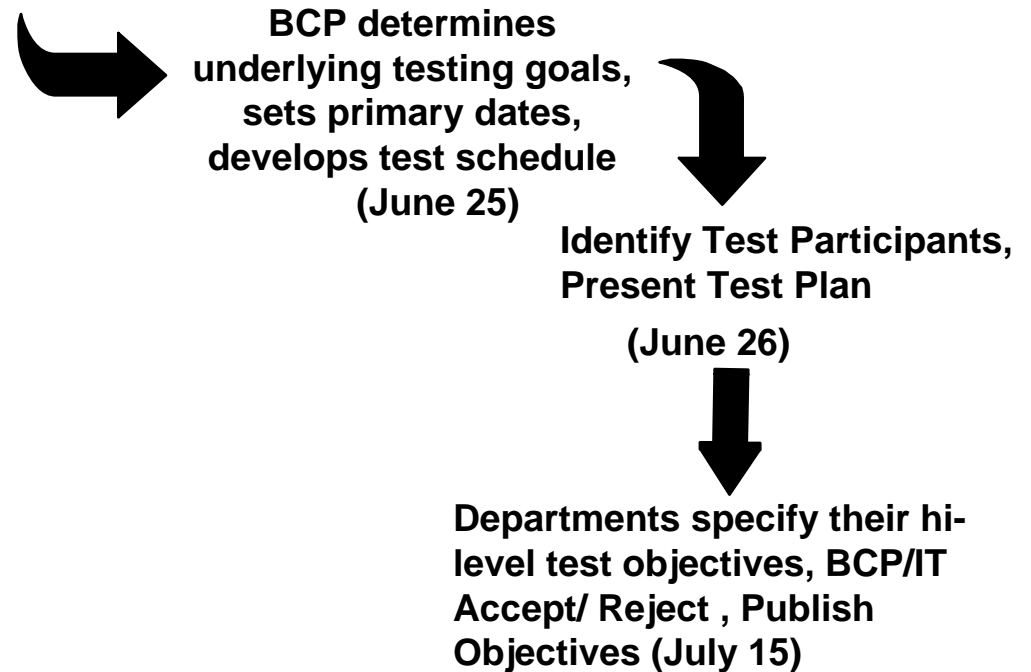
KEEPING PEOPLE AND INFORMATION CONNECTED®



Test Planning Cycle - Business Recovery Test

(Example for Test Date of September 1)

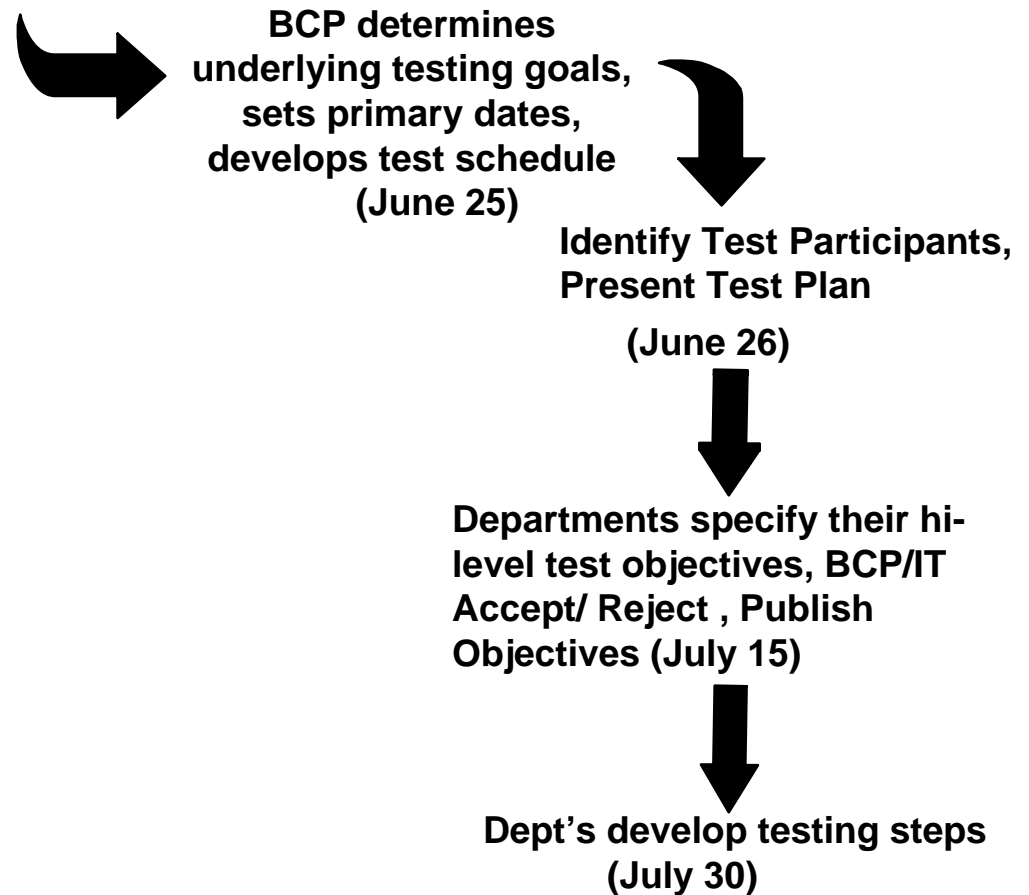
KEEPING PEOPLE AND INFORMATION CONNECTED®



Test Planning Cycle - Business Recovery Test

(Example for Test Date of September 1)

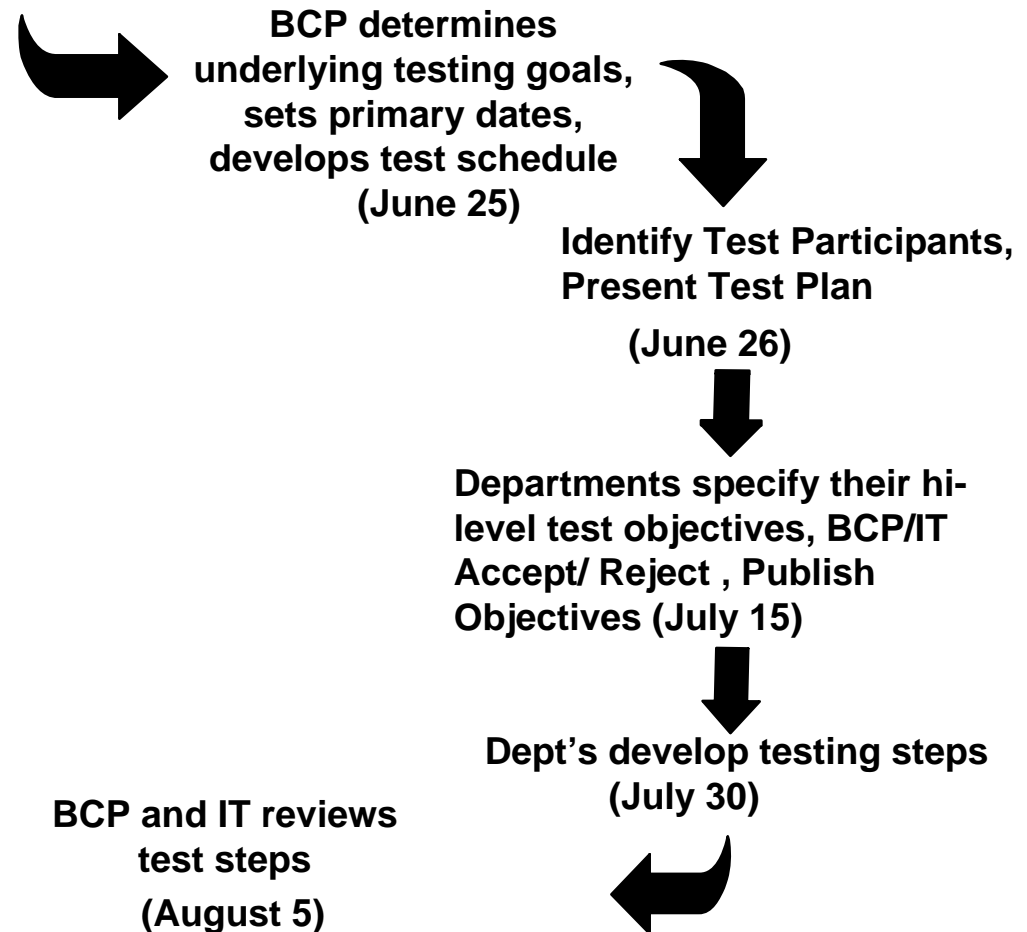
KEEPING PEOPLE AND INFORMATION CONNECTED®



Test Planning Cycle - Business Recovery Test

(Example for Test Date of September 1)

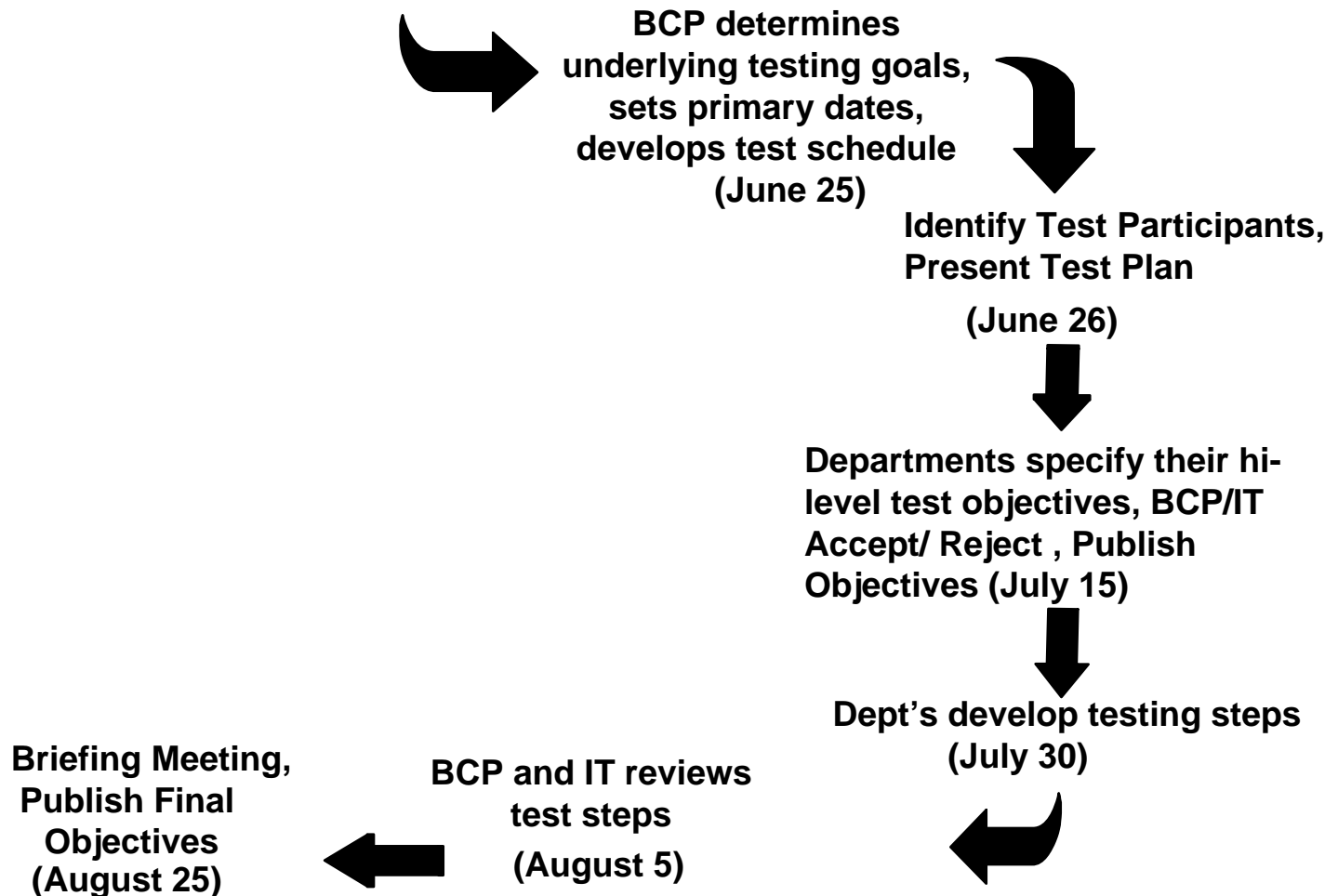
KEEPING PEOPLE AND INFORMATION CONNECTED®



Test Planning Cycle - Business Recovery Test

(Example for Test Date of September 1)

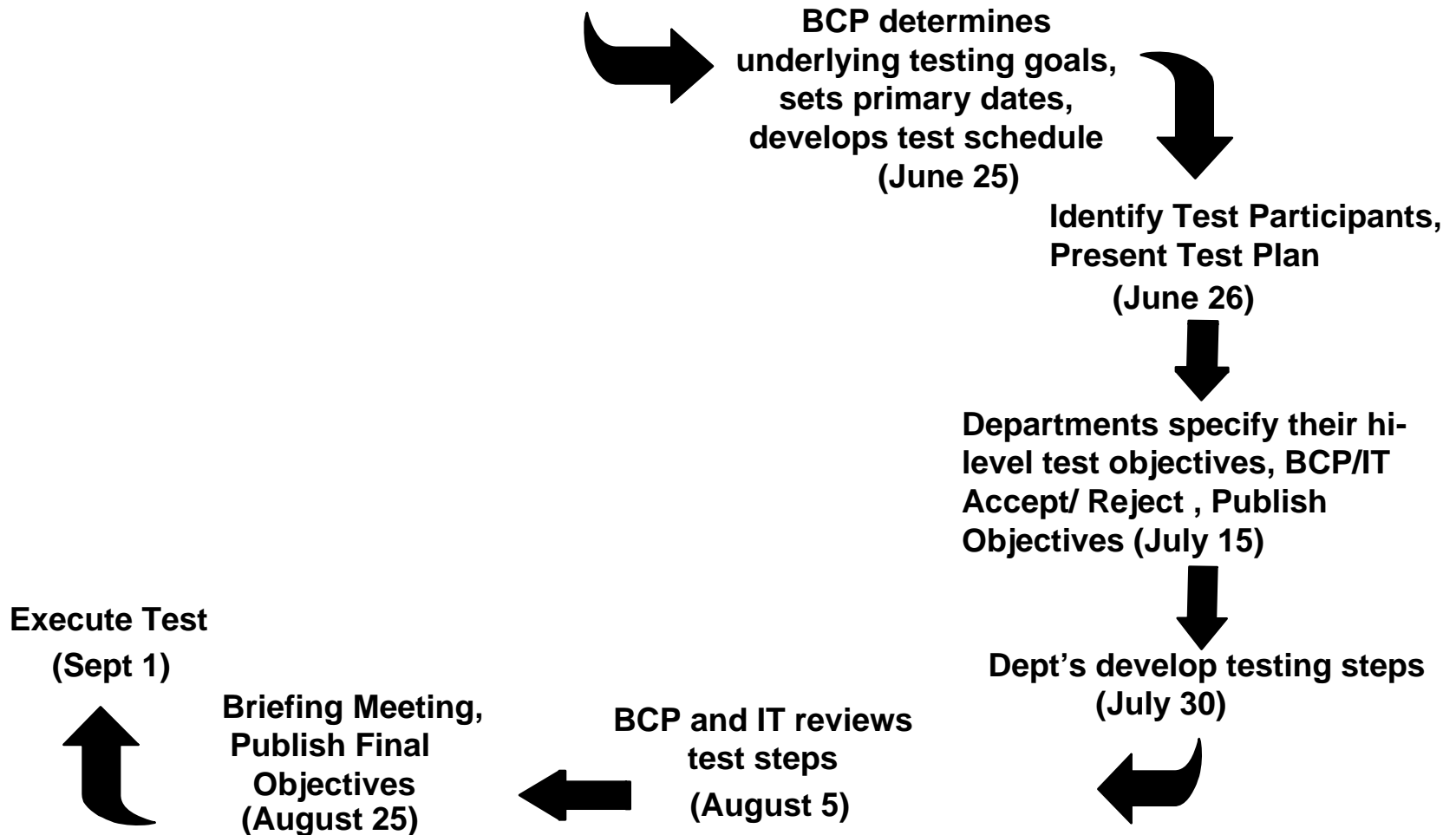
KEEPING PEOPLE AND INFORMATION CONNECTED®



Test Planning Cycle - Business Recovery Test

(Example for Test Date of September 1)

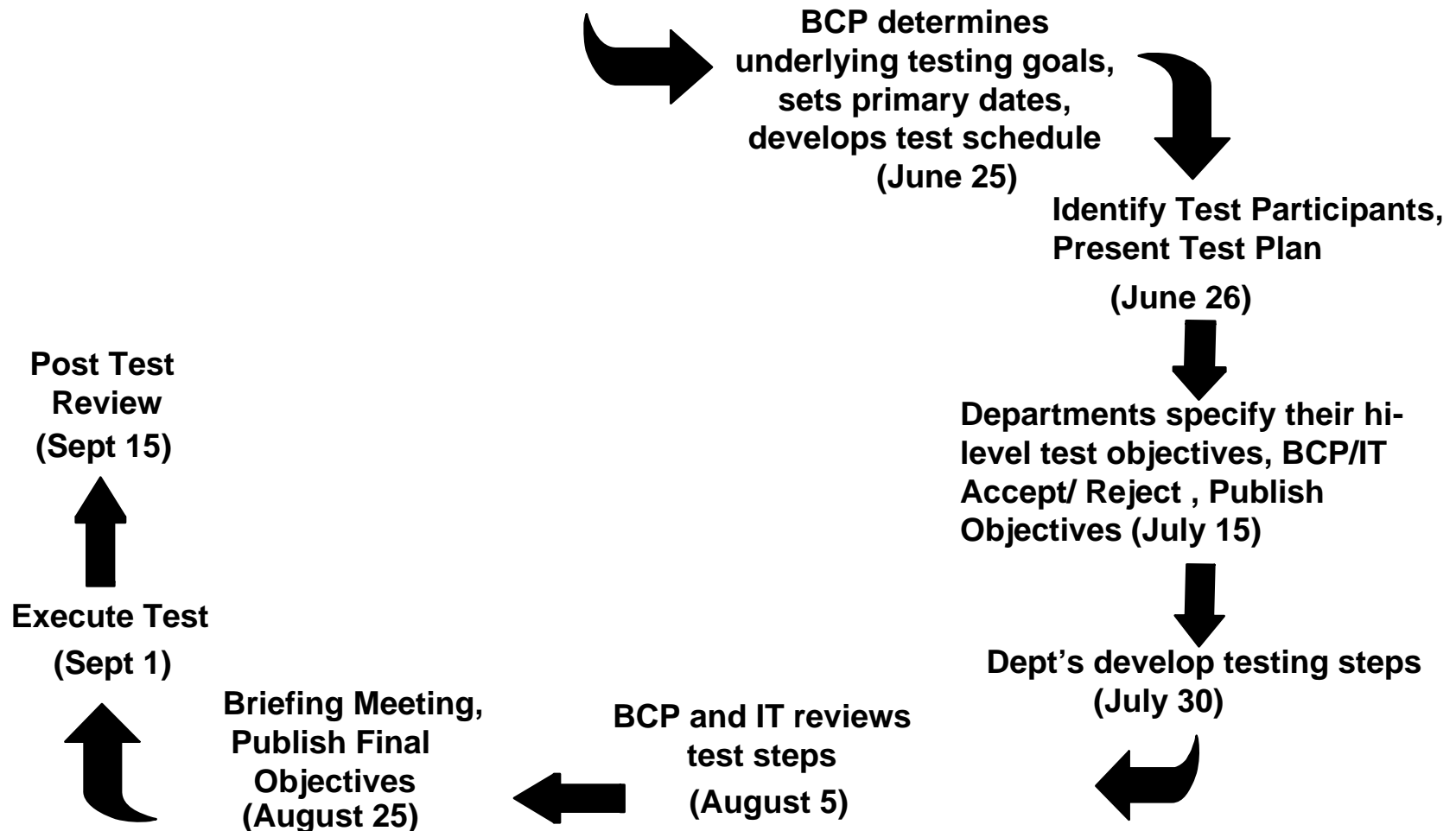
KEEPING PEOPLE AND INFORMATION CONNECTED®



Test Planning Cycle - Business Recovery Test

(Example for Test Date of September 1)

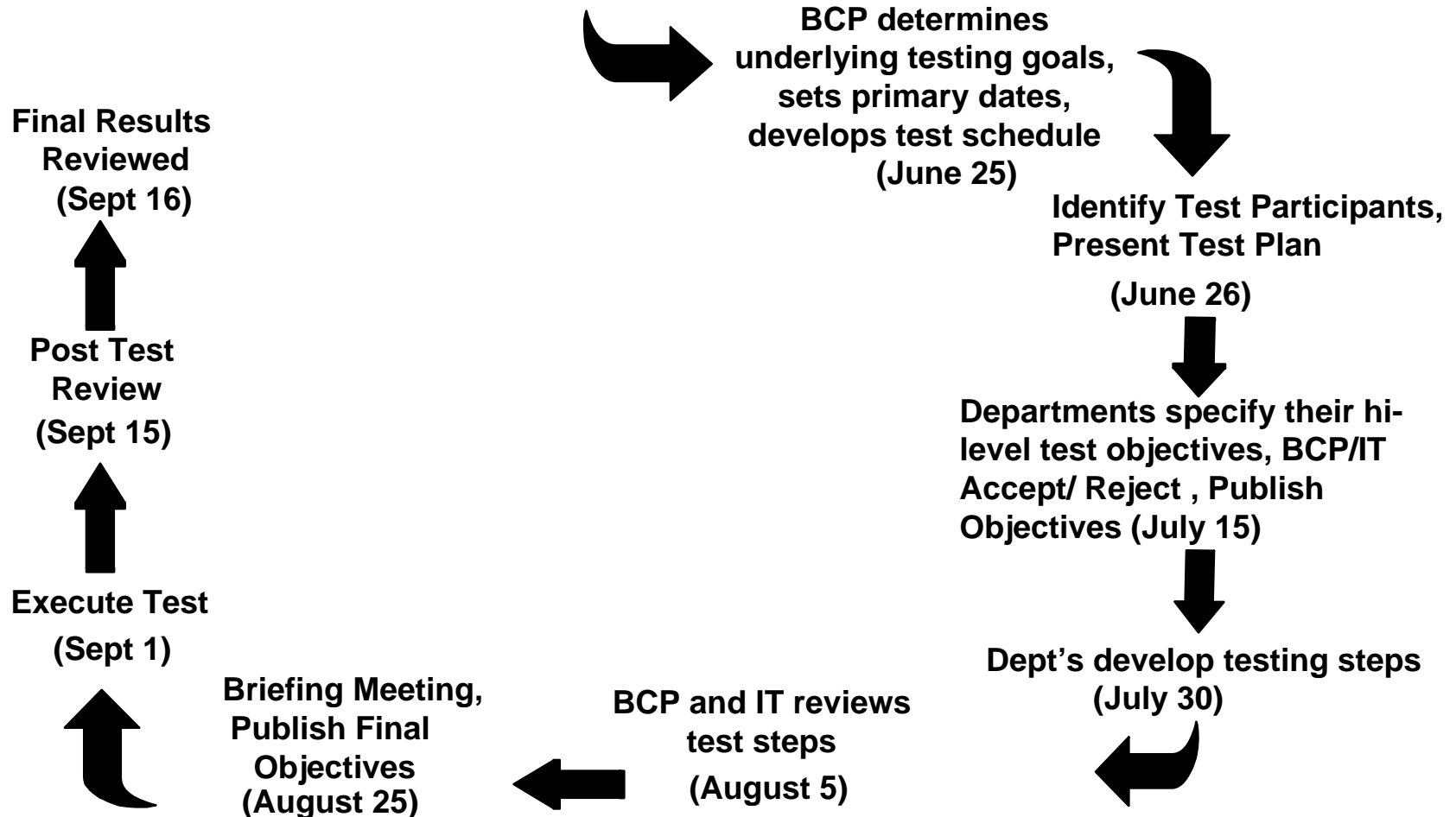
KEEPING PEOPLE AND INFORMATION CONNECTED®



Test Planning Cycle - Business Recovery Test

(Example for Test Date of September 1)

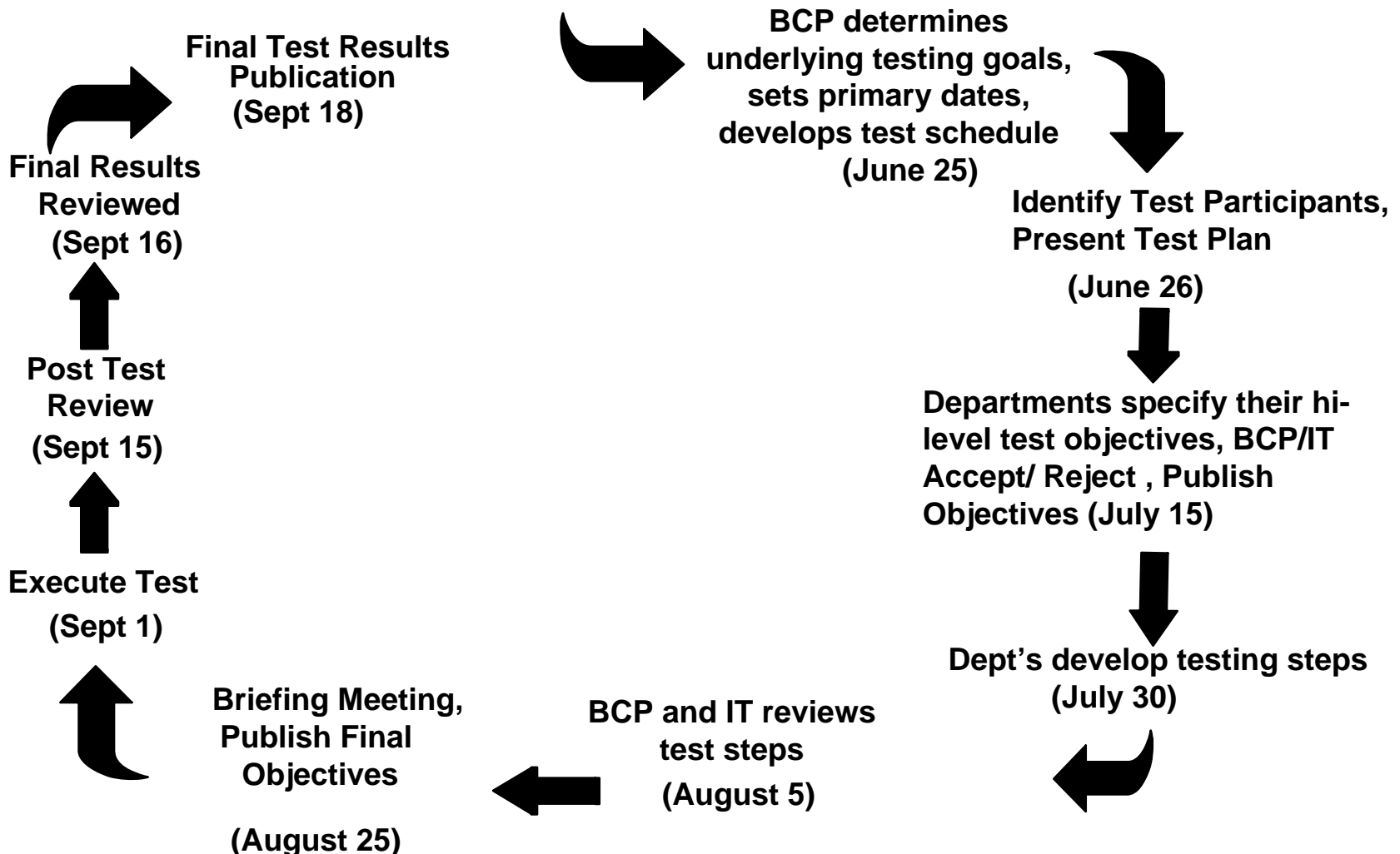
KEEPING PEOPLE AND INFORMATION CONNECTED®



Test Planning Cycle - Business Recovery Test

(Example for Test Date of September 1)

KEEPING PEOPLE AND INFORMATION CONNECTED®



Departments document test plans in a prescribed format

Detailed Objectives Report

Dept: Finance

Objective: Recover Payroll

Business Purpose: Payroll function is critical to operating the company

Departments document test plans in a prescribed format

Detailed Objectives Report

Dept: Finance

Objective: Recover Payroll

Business Purpose: Payroll function is critical to operating the company

Testing Step	Expected Result	Acceptable Variance	Actual Result
Launch Paychex	Program starts correctly	No acceptable variance	
Enter payroll data	Data is accepted into the program in correct areas	Slow response, up to 20 secs.	

Departments document test plans in a prescribed format

Detailed Objectives Report

Dept: Finance

Objective: Recover Payroll

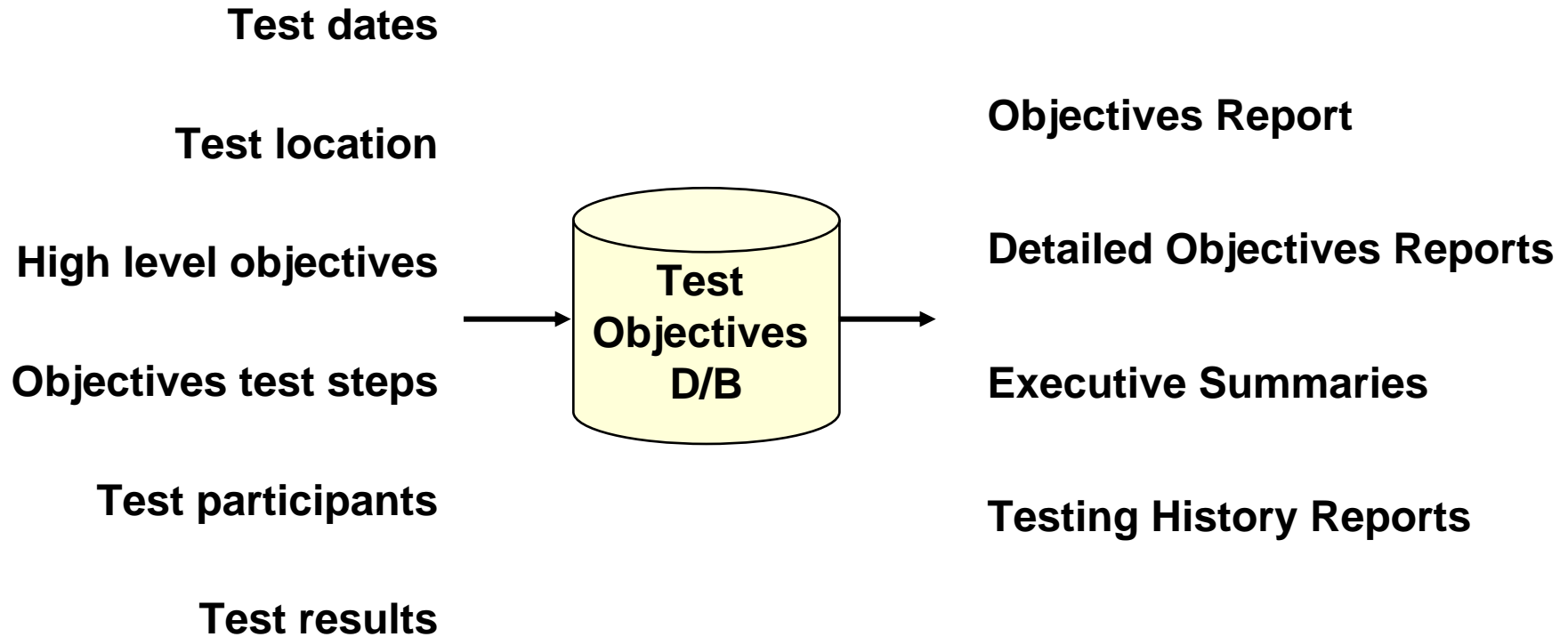
Business Purpose: Payroll function is critical to operating the company

Testing Step	Expected Result	Acceptable Variance	Actual Result
Launch Paychex	Program starts correctly	No acceptable variance	Program started successfully
Enter payroll data	Data is accepted into the program in correct areas	Slow response, up to 20 secs.	Response is timed at 35 secs.

 - Indicates area of form to be completed during test

Gathering and Tracking Testing Information

KEEPING PEOPLE AND INFORMATION CONNECTED®



Communicating About the Test

KEEPING PEOPLE AND INFORMATION CONNECTED®

- Objectives and detailed results will be communicated via a memo to all stakeholders
- Following test, post test review is held to review test results, problems encountered, issues with Recovery Site vendor or facilities.
 - List of follow up action items and assigned due dates and responsibilities is created and published.
 - BCP will track and report on progress on action list through the Steering Committee/Crisis Management Team



- **Set up a schedule for test progress updates**
- **Establish a voicemail distribution scheme for publishing updates**
 - **Can create separate lists for execs and all else**
 - **Communicate progress, problems, and other issues**
- **Provide a small gift to everyone**
- **Use a tool for communicating test activities, status**





To: CEO, CAO, CFO, CIO, Business Departments

Fr: Lee

A test was held on September 29, 2008. The results of the test were not satisfactory.

The following problems were encountered:

- **The Accounts Payable application was not accessible at the Recovery Center. During an actual BCP event, the result of this failure would prevent us from being able to pay our critical vendors, which could slow availability of raw materials.**
- **HR data, processed within the HR Benefits application could not be reconciled. In an actual BCP event, this failure would delay our ability to prove employee coverage for insurance purposes.**
- **The Customer Services customer line (800-555-1234) could not be transferred to the Recovery Center. Our customers would not be able to obtain product support if this failure took place during an actual emergency.**

These issues will be resolved within 30 days, and will be re-tested at our next BCP test, scheduled for January, 2009.

- It's critically important that problems be recorded during the test, to ensure that:
 - Problems that can be resolved successfully within the testing time frames are documented
 - Remaining problems can be discussed and addressed after the test
 - That situations that caused problems are retested to ensure they are resolved
 - Problems are not repeated from test to test
 - Management understands the impacts of the problems on the overall ability to recover the process/application/department





- In 2008, it is necessary that we be able to show, not just what is critical to recover, but that we can prove the BCP will work by conducting tests and documenting the test and the results
- Establishing and using standard testing terminology helps everyone understand the testing processes with less confusion and missed information, and provides an auditable record of what was tested, and the results achieved
- Defining and implementing a standard testing process that ensures consistency from test to test
- Defined, specific standard documents and reports to provide the needed audit trail for proving that your BCP program is accomplishing it's objectives, and is effectively viable

- **Getting the business departments to set test objectives and test steps increases their understanding of BCP and their involvement in tests**
- **Tracking test objectives and results over time helps to show progress**
- **An effective testing process, makes a significant contribution to BCP preparedness.**
- **Making test results public increases attention to BCP and ensures prompt correction of any problems encountered**





Questions?