Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Business Continuity Planning Concept of Operations

BCP Command Structure Business Continuity Planning (BCP) is a program that assesses the existing operations, risks, and customer relationships of an organization for the development of organizational preparedness. BCP develops an integrated approach to ensuring that critical processes continue to function during and after a disaster or incident that interrupts the operation of the organization.

Copyright SANS Institute
Author Retains Full Rights

AD

Beating the IPS?

STONESOFT
Can't be Beat

Learn
More

BCP Command Structure

Business Continuity Planning (BCP) is a program that assesses the existing operations, risks, and customer relationships of an organization for the development of organizational preparedness. BCP develops an integrated approach to ensuring that critical processes continue to function during and after a disaster or incident that interrupts the operation of the organization. The Homeland Security national incident management system (NIMS) incident command system (ICS) provides the basis for this BCP command structure.

The BCP command structure is designed to benefit the operational environment with coordinated emergency management (EM), IT disaster recovery (ITDR), and continuity of operations planning (COOP) BCP elements. Roles have been assigned as they pertain to executive management and decision makers. Note that the infrastructure support function has been identified as a specific section because of the core services provided to keep the organization in operation. Similarly, finance and administration and line operations functional areas have been added because of critical importance at a program level. BCP / COOP, IT support and EM program offices are also included to illustrate the ongoing effort needed to sustain BCP program viability. The BCP command structure is illustrated in figure 1.

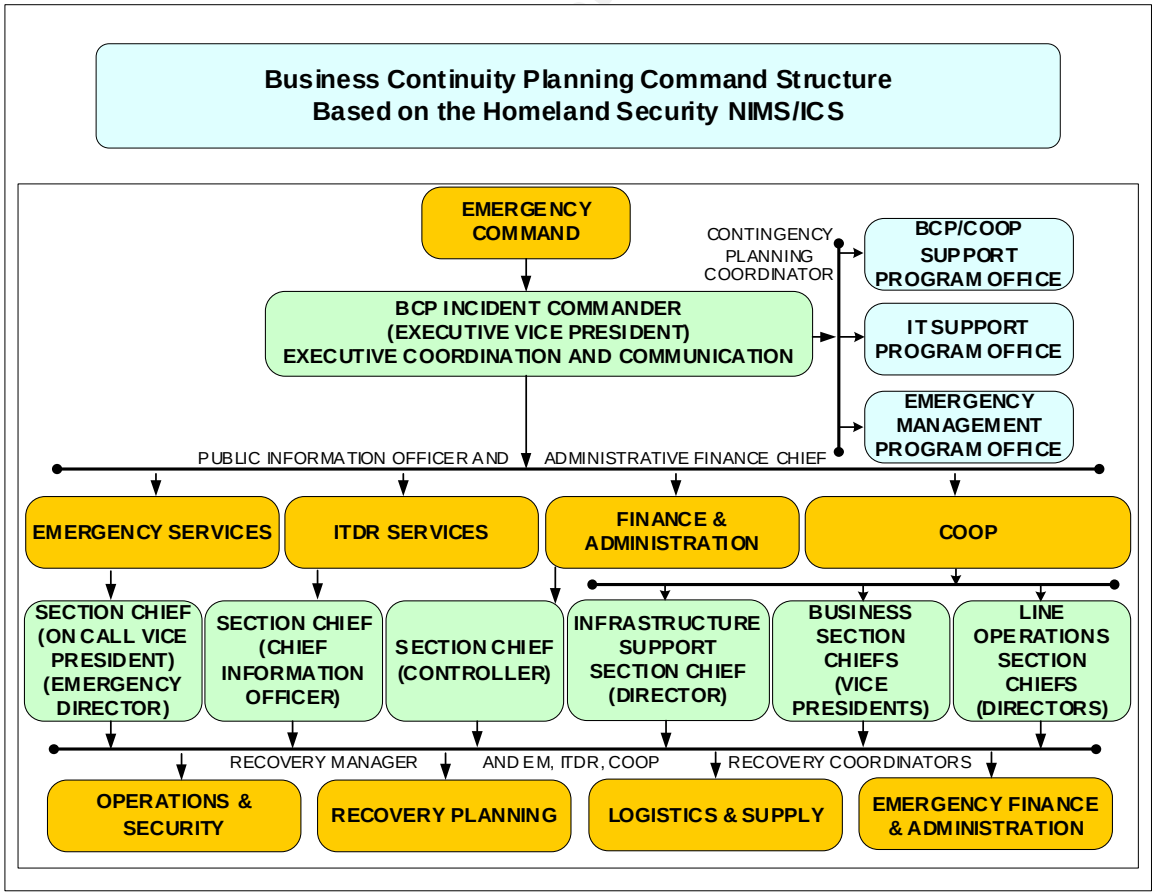

Figure 1: BCP Command Structure

© SANS Institute 2006, As part of the Information Security Reading Room Author retains full rights.

BCP Roles

- Emergency Incident Commander (EIC) - The EIC is responsible for on-site field emergency operations until threats and hazards to people, facilities and the environment are terminated.
- Public Information Officer (PIO) – The PIO is responsible for public relations communication.
- Administrative Finance Chief (AFC) – The AFC is responsible for overall coordination of emergency funding and cost collection.
- Emergency Director (ED) – The ED is responsible for all emergency operations coordination and communications and doubles as the emergency management section chief. The ED calls for BCP activation and declares that normal operations may resume upon BCP termination.
- BCP Incident Commander (BCP IC) - The BCP IC is responsible for overall BCP coordination and communications. The BCP IC declares BCP termination.
- Section Chief (SC) – An SC is responsible for coordination of area activities and reporting to the ED and BCP IC any issues that require higher level attention
- Recovery Manager (RM) – The RM is responsible for all mission recovery coordination, which includes the restoration of support services needed to perform mission during BCP operations and full recovery to normal operations
- Recovery Coordinator (RC) An RC is responsible for supporting the RM by facilitating the resumption and recovery of EM, ITDR and COOP BCP elements
- Contingency Planning Coordinator (CPC) – The CPC is responsible for overall coordination of COOP planning to ensure consistency in development and provide resources to support implementation across the organization.

This functional model for BCP is considered to be a distributed solution that provides responsiveness in any situation and allows individuals to solve the problems at hand. The majority of recovery work will be done by operations teams under the direction of the section chiefs. The BCP command structure is intended to facilitate consistency in approach and communications. Each incident is unique and requires evaluation of vulnerabilities and threats to determine appropriate action. Such a distributed solution will maximize value and provide dynamic response in the worst of times.

Figure 2 illustrates the coordination and overlap of EM and BCP facilitated through consistent command, public and internal communications where vulnerabilities for each incident are examined and BCP activation is called for by the emergency director when organizational operation is threatened. Note that appropriate levels of physical and cyber security must be maintained throughout the BCP life cycle.

© SANS Institute 2006, As part of the Information Security Reading Room Author retains full rights.

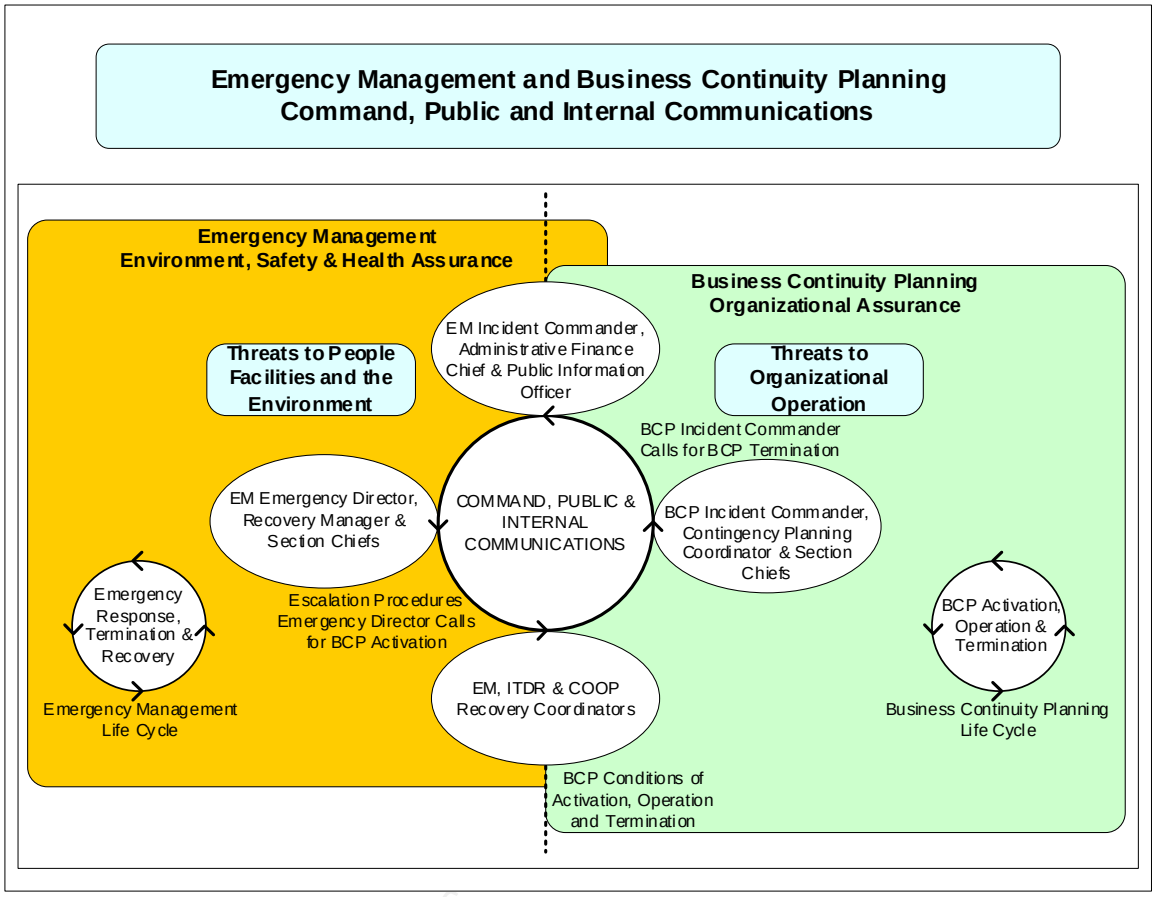

Figure 2: EM and BCP Command, Public and Internal Communications

BCP Conditions of Activation, Operation and Termination

Emergency operations have established methodologies for emergency response rooted in the NIMS / ICS. 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 in-kind with EM, meaning that the emergency director will have authority of control for the BCP activation and operation phases for all operations of the organization. The emergency incident commander will work with the emergency director and section chiefs to manage initial response through to the termination of the emergency situation. The emergency situation is terminated when threats and hazards to people, facilities and the environment are controlled and a safe environment is restored. Upon emergency director declaration of BCP activation, the BCP incident commander coordinates BCP operation with the section chiefs and the EM recovery team (recovery manager and recovery coordinators).

<u>BCP Conditions of Activation</u>
BCP activation is triggered when an incident is determined to threaten mission operations. Threats to mission operations include: threats to people, facilities and the environment requiring emergency response; threats to critical infrastructure that are

© SANS Institute 2006, As part of the Information Security Reading Room Author retains full rights.

essential to the operation of the organization (facilities, energy and water utilities, information and communication networks); threats to the operability of critical processes, supply and critical partnerships.

The emergency director declares BCP activation to initiate resumption and recovery services and communication. BCP activation puts into action mission operation contingency plans in order to sustain critical processes and services.

BCP Conditions of Operation

BCP operations initiate upon BCP activation as contingency plans and recovery operations begin. Contingency operations run in conjunction with EM 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. The BCP incident commander declares that BCP operations are completed upon consensus from the emergency director, section chiefs, recovery manager and recovery coordinators.

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 incident commander, section chiefs, recovery manager and recovery coordinators.

Critical Issues

BCP operations are dependent on planning, communication, coordination and security. Critical issues include:

1. Personnel Safety
2. Environmental Safety
3. Physical Security
4. Cyber Security
5. Identification of Critical personnel
6. Identification of Critical assets
7. Identification of Critical processes
8. Identification of Vital Records
9. Established Command Structure
10. Managed Command Communications
11. Managed Public Information and Safety Communications
12. Managed EM and BCP Internal Communications
13. Prioritization of Activities
14. Training, Testing and Continual Improvement
15. Timely Implementation

© SANS Institute 2006, As part of the Information Security Reading Room Author retains full rights.

Last Updated: August 28th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

FOR578 Cyber Threat Intelligence	**Tysons Corner, VAUS**	**Aug 31, 2015 - Sep 04, 2015**	**Live Event**
SANS Milan 2015	**Milan, IT**	**Sep 07, 2015 - Sep 12, 2015**	**Live Event**
SANS Crystal City 2015	**Crystal City, VAUS**	**Sep 08, 2015 - Sep 13, 2015**	**Live Event**
SANS Network Security 2015	**Las Vegas, NVUS**	**Sep 12, 2015 - Sep 21, 2015**	**Live Event**
SANS Seoul 2015	**Seoul, KR**	**Sep 14, 2015 - Sep 19, 2015**	**Live Event**
SANS Baltimore 2015	**Baltimore, MDUS**	**Sep 21, 2015 - Sep 26, 2015**	**Live Event**
Data Breach Investigation Summit & Training	**Dallas, TXUS**	**Sep 21, 2015 - Sep 26, 2015**	**Live Event**
SANS Perth 2015	**Perth, AU**	**Sep 21, 2015 - Sep 26, 2015**	**Live Event**
SANS Tallinn 2015	**Tallinn, EE**	**Sep 21, 2015 - Sep 26, 2015**	**Live Event**
SANS ICS Amsterdam 2015	**Amsterdam, NL**	**Sep 22, 2015 - Sep 28, 2015**	**Live Event**
SANS Bangalore 2015	**Bangalore, IN**	**Sep 28, 2015 - Oct 17, 2015**	**Live Event**
SANS DFIR Prague 2015	**Prague, CZ**	**Oct 05, 2015 - Oct 17, 2015**	**Live Event**
SANS Seattle 2015	**Seattle, WAUS**	**Oct 05, 2015 - Oct 10, 2015**	**Live Event**
SOS: SANS October Singapore 2015	**Singapore, SG**	**Oct 12, 2015 - Oct 24, 2015**	**Live Event**
SANS Tysons Corner 2015	**Tysons Corner, VAUS**	**Oct 12, 2015 - Oct 17, 2015**	**Live Event**
GridSecCon 2015	**Philadelphia, PAUS**	**Oct 13, 2015 - Oct 13, 2015**	**Live Event**
SANS Gulf Region 2015	**Dubai, AE**	**Oct 17, 2015 - Oct 29, 2015**	**Live Event**
SANS Cyber Defense San Diego 2015	**San Diego, CAUS**	**Oct 19, 2015 - Oct 24, 2015**	**Live Event**
SANS Tokyo Autumn 2015	**Tokyo, JP**	**Oct 19, 2015 - Oct 31, 2015**	**Live Event**
SANS Sydney 2015	**Sydney, AU**	**Nov 09, 2015 - Nov 21, 2015**	**Live Event**
SANS South Florida 2015	**Fort Lauderdale, FLUS**	**Nov 09, 2015 - Nov 14, 2015**	**Live Event**
SANS London 2015	**London, GB**	**Nov 14, 2015 - Nov 23, 2015**	**Live Event**
Pen Test Hackfest Summit & Training	**Alexandria, VAUS**	**Nov 16, 2015 - Nov 23, 2015**	**Live Event**
SANS Hyderabad 2015	**Hyderabad, IN**	**Nov 24, 2015 - Dec 04, 2015**	**Live Event**
SANS Chicago 2015	**OnlineILUS**	**Aug 30, 2015 - Sep 04, 2015**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**