Business Continuity/Disaster Recovery (BC/DR) Program
ITS Division Operation Center (DOC)

Town Hall Overview

February 11, 2009
Marian Sherrin
Today’s Objective:

• Prepare you for the launch of the ITS Division Operation Center (aka ITS DOC)
  – Week of Feb 9-13, 2009
  – DOC Member ToGo Packets Released
  – Rooms Ready to go

• Answer some anticipated questions - and any others
  – Why is it designed THIS way??
  – When will it be activated? Who decides??
  – What happens when it is activated?
  – How will I know it has been activated?
  – What is expected of me when it is activated?
  – How do I get more information?
  – How do I volunteer?
Definitions

Emergency Management
Process and procedures for identifying threats and hazards, putting mitigation plans in place, developing emergency response action plans, and initiating Alerts and Emergency Operation Plans

Business Continuity
(private sector term)
Processes and procedures an organization puts in place to ensure that essential functions can continue during and after a disaster. Business continuity planning seeks to prevent interruption of mission-critical services, and to reestablish full functioning as swiftly and smoothly as possible.

Disaster Recover
(private sector term)
Processes and procedures required for a timely and orderly resumption of regular business

Gov’t Standards & Regulations
Standardized Emergency Management System (SEMS)/National Incident Management System (NIMS) – Incident Command System (ICS) VTV Act 2008 if approved

UCOP Policies & Directives

Campus Directives
UCSC Hazard Plans (EM)
UCSC EOP (EM)
UCSC EOC (EM)
CruzAlert (EM)

Campus Safety & Emergency Response Gaps

UC Ready

“UC Ready”

UCOP BFB IS-12

Communications & Infrastructure Improvement Projects

Enterprise System BU/DR Assessment

UC Santa Cruz
Mary Doyle is on Policy Group

Chancellor & Policy Group

UCOP

Doug Hartline Sits on EOC

EOC Director

Management Section

Planning Section

Operations Section

Logistics Section

Finance/Admin Section

We fit here

Incident Commander

Fire Dept.

Police Dept.

EH&S

Physical Plant DOC

Student Affairs DOC

ITS DOC

We fit here

Division/Department Operations Centers
Why Division Operations Centers?

• Essential response organizations have Department or Division Operations Centers (DOCs) and DOC Plans
  – Coordinate the actions of their personnel
  – Facilitate communication with (EOC)

• The DOCs will automatically work to restore their critical business functions

• The EOC will provide interdepartmental coordination and prioritization of activities

• DOCs may activate independently
  – In response to localized events that require extraordinary attention
ITS DOC Project Scope

• Out of Scope
  – Campus wide Emergency Alerts
  – Decisions on campus closures – EOC/Policy Group
  – Life/Safety/First aid/CPR – CALL 911
  – Communication with the media – PIO Scope

• In Scope of DOC Project
  – Activation Criteria and Authority
  – ITS Roles & Responsibilities and Contact Lists
  – Physical DOC Rooms
  – Prioritization of critical ITS services and applications
  – Process of accounting for employees
  – Training, Drills, & Continuous Improvement
Why Use Incident Command System (ICS)?

- Developed in 1970’s response to catastrophic fires in California, then directed as national standard in 2003.  
  - Designed to address the "inadequate management" problem
- Designed to be effective and efficient
- Used by all levels of government, Private Sector, & Higher Ed
  - UC Berkeley’s IT group has had an ICS DOC for >6 years
- Common Language & Structure with Fire, Police
- Modular and Scalable
  - Fill only the functions or positions necessary for a particular incident
Incident Command System (ICS)

- Structured to facilitate five major functions:
  - Command
    - Overall incident management & communications
  - Operations
    - Manages direct response and recovery
  - Planning
    - Status of the Situation
    - Planning for future needs
  - Logistics
    - Filling immediate needs of the DOC
  - Finance & Administration
    - Tracking resources used (hours worked, purchases)
Deputies may be assigned to tasks as needed

Goal: Three levels deep in all roles
ITS DOC Activation

- ITS DOC may be activated by
  - EOC
  - VC IT
  - ITS Director or Acting Director
- Using their best judgment
  - Operational incident transcends or exceeds the ability of the operational team to manage

**Flow of Director Activation of the DOC**

1. Director consults with VC IT
2. Director decides to activate DOC
3. Director calls ITS DOC Manager and Communications Officer
4. Communications Officer’s calls or sends CruzAlert to ITS DOC Members with specific roles to be filled
5. ITS DOC Activated
6. ITS DOC Roles are filled
7. ITS DOC Communications Officer’s sends All ITS Message of Activation and Role Assignment
   - All ITS Message depends on email capability, could use phone broadcast as backup.

Activation by **VC IT** or the **EOC** follow similar flows
## DOC ACTIVATION

<table>
<thead>
<tr>
<th>Scenario</th>
<th>ITS DOC Activation</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SERVICE INTERRUPTION:</strong> A service interruption is defined as an enterprise wide system (CruzMail, FIS, AIS, etc.), component, or peripheral that is down or unavailable for <strong>less than 48 HOURS</strong>. Service interruptions are not the result of facility or systems damage and such outages are normally addressed by day-to-day emergency procedures.</td>
<td><strong>No</strong></td>
<td>Operations are fairly confident they can resolve on their own. Use Major Incident Process for communication.</td>
</tr>
<tr>
<td><strong>MINOR DISASTER:</strong> A minor disaster is defined as an enterprise wide system outage(CruzMail, FIS, AIS, etc.) that is expected to last for <strong>more than 48 hours but can be resolved within FIVE days</strong>. Minor disasters, typically, are not the result of extensive damage to facilities or physical hardware or systems. An outage of a system that prevents instruction when classes are in session or impacts research for &gt;24 hrs. of time would be considered a “Major Disaster”.</td>
<td><strong>Maybe</strong></td>
<td>May be activated if risk increases towards a Major Disaster, or operations require additional help to manage – inside or outside of ITS (physical plant, police, fire, etc).</td>
</tr>
<tr>
<td><strong>MAJOR DISASTER:</strong> A major disaster is defined as an enterprise wide systems outage that is expected to last for <strong>more than FIVE days</strong>, especially when the service outage is due to fire or flood, a small earthquake, or civil disorder, or other calamity resulting in extensive damage requiring new facilities or replacement of major computer components or entire systems. An outage of a system that <strong>prevents instruction (when classes are in session) or impacts research for &gt;24 hrs.</strong> would be considered a “Major Disaster”.</td>
<td><strong>Yes</strong></td>
<td>High likelihood. Activation will still depend on need for increased management beyond operations.</td>
</tr>
<tr>
<td><strong>CATASTROPHIC DISASTER:</strong> A catastrophic disaster is defined as a calamitous event that disrupts operation throughout the entire campus to such a degree that the need for technology support is obviated until rebuilding takes place and normal campus operations begin again.</td>
<td><strong>Maybe</strong></td>
<td>The DOC may be activated for initial assessment and communication. Most likely these incidents will start as Major and evolve to Catastrophic</td>
</tr>
</tbody>
</table>
DOC Role Requirements

Guiding principle

– Not critical for field deployment
– One of 3 members living on Westside

Commitment

– 3 hours of official ICS 100 Training
– 4 + hours of ITS DOC Training
– Quarterly drills throughout 2009
– On call and likely active during emergencies
What should you expect?

1. Expect an email that alerts you when the ITS DOC is activated.

2. You may be instructed to help by someone other than your normal supervisor – please cooperate.

3. Expect a new process to make sure you are accounted for after an evacuation/emergency.

4. Expect to be able to get more information on our ITS DOC website:
   
   http://its.ucsc.edu/its_doc/index.php
Back-up
**Criteria:** Causes a severe interruption of university programs/services.
<table>
<thead>
<tr>
<th>Application</th>
<th>Initial Priority</th>
<th>Justification Info</th>
<th>IS-12 Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>800MHz &amp; VHF Radio</td>
<td>1A= 800MHz</td>
<td>800MHz used by Police, ITS, Media Services, Shuttle Drivers</td>
<td>Essential</td>
</tr>
<tr>
<td></td>
<td>1B = VHF</td>
<td>VHF used by Fire (Police may move from 800MHz if they can solve the coverage issues)</td>
<td></td>
</tr>
<tr>
<td>Phone Service</td>
<td>2A=Wired</td>
<td>Required for life/safety</td>
<td>Essential</td>
</tr>
<tr>
<td></td>
<td>2B = Cell Service</td>
<td>In the future Phone Service (1A) will be dependent on network service</td>
<td></td>
</tr>
<tr>
<td>Network, Firewalls, &amp; Gateways</td>
<td>3A = Ethernet</td>
<td>Includes Central DNS (vs. departmental), DHCP</td>
<td>Essential</td>
</tr>
<tr>
<td></td>
<td>3B = Wireless</td>
<td>Geographic Priorities: UCSC ERC, EOC, CommD1, Mt. Hamilton (they have no cell phone service and no satellite phones as of 8/27/08), Delaware, rest of campus.</td>
<td></td>
</tr>
<tr>
<td>Authentication</td>
<td>4A = Kerberos</td>
<td>Many other systems are dependent on these servers.</td>
<td>Essential</td>
</tr>
<tr>
<td></td>
<td>4B = Active Directory (AD)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage</td>
<td>5A = NetApps</td>
<td>Many other systems are dependent on these servers.</td>
<td>Essential</td>
</tr>
<tr>
<td></td>
<td>5B = SunNAS</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>5C = APS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>eMail</td>
<td>6A = CruzMail</td>
<td>PB Sci and SOE dropped. Will come up after other priorities within division applications.</td>
<td>Necessary</td>
</tr>
<tr>
<td>WWW</td>
<td>7A=WWW</td>
<td>Action: May want 1) off campus replication/hosting 2) Cross Hosting with WWW2 for Emergency.ucsc.edu (Jeff/Leslie/Joe)</td>
<td>Necessary</td>
</tr>
<tr>
<td></td>
<td>7B=WWW2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WebCT/LMS/Instructional Computing Systems</td>
<td>8A = WebCT/ LMS</td>
<td>A: WebCT/LMS dependent IC Infrastructure systems</td>
<td>Essential for classroom instruction in many cases (mission of campus)</td>
</tr>
<tr>
<td></td>
<td>8B = Unix Timeshares</td>
<td>B: Instruction</td>
<td></td>
</tr>
<tr>
<td>IT Request</td>
<td>9</td>
<td>Need to track issues and problems</td>
<td>Necessary</td>
</tr>
<tr>
<td>AIS</td>
<td>10</td>
<td></td>
<td>Necessary</td>
</tr>
<tr>
<td>IDM/CruzID</td>
<td>11</td>
<td>moira/potmos, others. Fields that are not in the table.</td>
<td>Necessary</td>
</tr>
<tr>
<td>PIS</td>
<td>12</td>
<td>Need in order to produce paper checks to student employees. May get higher priority near student pay dates</td>
<td>Essential (IS-12 controllers)</td>
</tr>
<tr>
<td>Ticket Office/A. View</td>
<td>13</td>
<td>As long as we put forth best effort to restore services we are within the boundaries of the contract with the City of Santa Cruz</td>
<td>Necessary</td>
</tr>
<tr>
<td>Door Lock Support</td>
<td>14</td>
<td>The doors will continue to run without power - all have battery backup. Higher risk after 8 hours if power is not restored and wireless ports are not up, doors will roll more frequently, draining batteries sooner.</td>
<td>Necessary</td>
</tr>
<tr>
<td>WebGiving</td>
<td>15</td>
<td>Actual online giving site is hosted offsite at a third party. The links to get there, however, are through our WWW sites. Action: If major disaster strikes we need to have alternative to a site that will get donors to the actual offsite hosting giving site. Key learning from Hurricane Katrina. Work with University Relations to revise hosting strategy (Marlan/Brian Duesenberg/Bomi Patel)</td>
<td>Essential if a major campus disaster occurred that would prompt the need for extraordinary giving from supporters. Otherwise, deferrable.</td>
</tr>
<tr>
<td>PPS</td>
<td>NA</td>
<td>Hosted at UCOP/UCSD</td>
<td>Essential (IS-12 controllers)</td>
</tr>
<tr>
<td>CruzTime</td>
<td>Necessary</td>
<td></td>
<td>Necessary</td>
</tr>
<tr>
<td>Health Center Prescription</td>
<td>Necessary</td>
<td>In a major campus emergency the health center would close and students would be referred off-campus.</td>
<td>Necessary</td>
</tr>
<tr>
<td>Other Division Apps</td>
<td>A= Exchange Mail</td>
<td></td>
<td>Deferrable</td>
</tr>
<tr>
<td></td>
<td>B= PB Sci Mail</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>C= SOE Mail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Student Housing Online</td>
<td>Deferrable</td>
<td>At one point we thought that SHO might be needed for Life/safety. In speaking with Adam Shook, the community safety officers have printed rousers that they utilize on a day to day basis and would use in an emergency situation. We thus moved SHO to the bottom and as deferrable. This may move to the top if during emergency.</td>
<td>Deferrable</td>
</tr>
<tr>
<td>Data Warehouse</td>
<td>Deferrable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial Managers Workbook</td>
<td>Deferrable</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Teleconferencing

• Digital Phone
  – Using line 1 make first call
  – Using line 2, make second call
  – Hold down the “3” to connect these two on line 1
  – Using line 2, make third call
  – Hold down the “3” to connect to line 1 call
  – Repeat up to 6 lines

• Polycom
  – Dial the first number
  – Hit the “Flash” button to get a second dial tone
  – Dial the second number (talk and hang up or…)
  – Hit the “Flash” button to connect the first two calls
  – Repeat

• Using ReadyTalk
  – Get a free account from ReadyTalk to enable you to host a web meeting
    • Web meetings are free, the only additional costs are for using their teleconferencing services
      ($0.035/line/minute)
    • Link: http://its.ucsc.edu/services/telephone/faculty_and_staff/services_and_features/readytalk_conference_call.php
  – To log in to a ReadyTalk web meeting:
    • Go to www.readytalk.com
    • Use the hosts office phone number. Example: if I was hosting the access code would be 5027365
ITS DOC Activation by VC IT

• VC IT may activate the ITS DOC
  – IT sustains a site specific disaster
  – Interruption to essential computer and communications functions
  – Rest of campus is relatively unaffected

Flow of VC IT Activation of the DOC

VC IT decides to activate DOC

VC IT Calls ITS DOC Manager and Communications Officer

Communications Officer’s calls or sends CruzAlert to ITS DOC Members with specific roles to be filled

ITS DOC Communications Officer’s sends All ITS Message of Activation and Role Assignment

VC IT also notifies Campus Emergency Planner of DOC Activation

ITS DOC Manager with VC IT Determine DOC roles to be filled

ITS DOC Activated

ITS DOC Roles are filled

All ITS Message depends on email capability, could use phone broadcast as backup.
ITS DOC Activation by EOC

- EOC may activate ITS DOC
- EOC Operations ITS Rep connects to ITS DOC
  - The EOC Operations ITS Rep will oversee our response and give us priorities as set by the EOC for the specific Incident

Flow of EOC Activation of the DOC

1. EOC decides to activate DOC
2. EOC ITS Rep consults with VC IT
3. EOC ITS Rep calls ITS DOC Manager and Communications Officer
4. Communications Officer’s calls or sends CruzAlert to ITS DOC Members with specific roles to be filled
5. ITS DOC Activated
6. ITS DOC Roles are filled
7. ITS DOC Communications Officer’s sends All ITS Message of Activation and Role Assignment
8. EOC Directs Communications/Actions
9. CruzAlert or other methods used as determined by Campus Incident Command (IC) & EOC
10. EOC ITS Rep consults with VC IT
11. DOC Manager consults with EOC ITS Rep to determine what roles to fill on the ITS DOC
12. All ITS Message depends on email capability, could use phone broadcast as backup.
ITS DOC Project Scope

• In Scope of DOC Project
  – Activation Criteria and Authority
    • All ITS Supported UCSC Sites are within scope (on campus, off campus, & remote)
  – Incident Command Organization
    • Roles & Responsibilities and Contact Lists
  – Physical Division Operation Center (DOC) Rooms
    • Comms 143, Kerr 61, Delaware A138
  – Training and Drills
  – Prioritization of critical ITS services and applications
  – Process of accounting for employees
  – Process for Continuous Improvement of DOC
ITS Risk Matrix

Unprepared: No procedures, no back-up method

Somewhat Prepared: Some procedures, some experience, maybe a back-up method

Prepared: Documented printed procedures, several layers of experience, solid or capable back-up method

High

- Wireless Radio Outage
- AT&T Outage
- Network Outage
- Internal Phone Outage
- Local Fire/ Flood
- Internal Cyber Sabotage
- Cell Phone Tower Outage
- Tape Media Degradation

Low

- Human Error causing data or access loss
- Vandalism to IT Equipment
- Staff Reduction (access/illness)
- Computers Hacked
- Email Outage
- Forest Fire/ Large Scale Flood
- Data Center Environmental (partial shutdown)
- Unauthorized User on network
- Hardware Failure Server Disk Error
- Stolen PC
- External Virus

LIKELIHOOD

Low

High
ITS DOC Manager

ITS’ “Incident Commander (IC)”

• The DOC Manager has overall responsibility for the management of all emergency activities
  – Manages the incident
    • For small incidents, only DOC manager and Communications Officer may be activated.
  – Completes Incident Briefing (ICS 201)
  – Develops Incident Objectives (ICS 202) with Operations Section Chief
  – Ensures safety related instructions are followed, people are accounted for
  – Key interface to Campus EOC, if applicable.
    • The DOC manager may also call EOC for external assistance.
  – Makes decision to expand or contract the DOC roles required.
  – Maintains an Activity Log (ICS 214)
  – Manages post event assessment.
Communication Officer

• Primary responsibility is to establish and maintain communications of the ITS DOC
  – Support ITS DOC Manager with coordinating communications within ITS and with ITS clients
  – Report communications to the ITS DOC Manager
  – Record incoming communications
    • Example: Physical Plant, EOC, CruzAlert, Radio/TV, email to ITS DOC account.
Safety Officer/Runner

• Primary role is to ensure the working safety of those on site or around campus
  – Monitors incident operations and advises the DOC manager on all matters relating to operational safety, including the health and safety of responders

• Be available to physically 'run' messages if necessary due to communication issues.
Operations Section Chief

• This section is responsible for all operational activities focused on:
  – Assessment of operational areas
  – Overseeing expert staff & response in order to:
    • Reduce the immediate hazard
    • Restore division services to normal operations

• Should have direct involvement in the preparation of the
  – Incident Objectives (ICS 202)
  – Incident Action Plan (IAP)

• Maintains an Activity Log (ICS 214)
Operations Section

- Operations Section Chief
  - Radio/Cell Network Supervisor
  - Wired Voice Network Supervisor
  - Data Network Group Supervisor
  - Cyber Security Group Supervisor
  - Servers Group Supervisor
  - Divisional Server Group Supervisor
  - Labs/Classroom Group Supervisor
Plans Section Chief

• The Planning Section Chief:
  – Collects and evaluates incident situation information
  – Develops and documents the Incident Action Plan (IAP) (ICS-202) with the DOC Manager
  – Prepares status reports (ICS 209)
  – Displays situation information
  – Maintains status of resources assigned to the incident
  – Collects information from building and unit coordinators who are accounting for all ITS employees during any necessary evacuations.
    • Includees full time, part time, and student employees

View checklist
Plan Section Deputy

• Plan Section Chief may delegate some tasks to a Plans Section Deputy
  – Keeping up with the Situation Status and maintaining the Status Boards and reports
  – Coordinating the staffing of future shifts
  – Coordinating detailed information on asset damage assessment and ability to salvage equipment
  – Collecting information from building and unit coordinators who are accounting for all ITS employees during any necessary evacuations.
Logistics Section Chief

• The Logistics Section is responsible for:
  – Supporting the direct resource needs of Operations and the ITS DOC including:
    • Staffing necessary positions
    • Obtaining supplies, equipment, and nourishment (if required)
    • Facilities
    • Transportation
    • Communication services for DOC
    • Information technology support for DOC
Logistics Section Deputy

• Logistics Section Chief may delegate some tasks to a Logistics Section Deputy
  – Preparing the ITS DOC room
    • Supplies and Equipment
    • Sign-in/Sign-out and distribution of role packets
  – Contacting ITS employees required for tasks and assignments
  – Obtaining any necessary Equipment/Supplies
  – Understanding/finding applicable contracts for services. These could be located in different groups.
    • Business Services, Purchasing, Core Tech, Legal, ITSM Software
Finance Section Chief

• Finance Section has responsibility for:
  – Cost accounting
  – Financial risk assessment
  – Documenting expenditures, purchase authorizations, damage to property, equipment usage, and vendor contracting
    • May be used for reimbursement from FEMA
  – Tracking labor hours, locations worked, mileage and other costs
    • May be used for reimbursement from FEMA
  – Provide summary reports to the DOC Manager
  – In the recovery period, this position may be asked to assist with damage reports and records for the University’s FEMA application
Finance Section Deputy

• Finance Section Chief may delegate some tasks to a Finance Section Deputy
  – Tracking labor hours, locations worked, mileage and other costs
    • May be used for reimbursement from FEMA
  – Documenting expenditures, purchase authorizations, damage to property, equipment usage, and vendor contracting
    • May be used for reimbursement from FEMA
  – Generation of summary reports for the DOC Manager