Signs of the times: business continuity, disaster recovery, and IT audit

Win Shih
John Cashaw, University of Colorado at Boulder
Introduction

- Growing interdependence of technology
- 50% institutions experiencing IT disruption in last 5 years (ECAR)
- #6 of Top 10 projects in ’07 (Baseline)
- Top 5 critical issues facing Higher Ed CIO (EDUCAUSE)
- Business continuity, disaster recovery, risk assessment, business impact, and IT audit
Business Impact Analysis

- Identify unit’s functions and critical processes
- Examine likely threats to those processes
- Create mapping between functions and IT resources (campus + library)
- Determine impact and recovery time
- Identify the dependencies on IT resources
- Integrate with IT recovery plan

### Library IT Services Work Area

<table>
<thead>
<tr>
<th>Service #</th>
<th>Service Description</th>
<th>Critical</th>
<th>Vital</th>
<th>Sensitive</th>
<th>Non-Critical</th>
</tr>
</thead>
<tbody>
<tr>
<td>L101</td>
<td>Library Web server</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>L102</td>
<td>Library data server</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>L103</td>
<td>Library content server (tracking password, journal)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>L104</td>
<td>Library IT services (authentication)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>L105</td>
<td>Library IT services (networking, administration)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>L106</td>
<td>Library IT services (support)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>L107</td>
<td>Library IT services (training)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>L108</td>
<td>Library IT services (administration)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>L109</td>
<td>Library IT services (content management)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>L110</td>
<td>Library IT services (administration)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>L111</td>
<td>Library IT services (library management)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>L112</td>
<td>Library IT services (networking)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>L113</td>
<td>Library IT services (application)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Library IT Services Work Areas

- **Access Services**
  - Catalog materials in all formats (LIT5, LIT9, LIT10, LIT14), (TC1, TC2, TC3, TC4)
  - Inventory library resources in all formats (LIT5, LIT10, LIT14), (TC1, TC2, TC3, TC4)
  - Maintain library's ejournal holding information (TC1, TC2, TC3, TC4)

- **Technical Services**
  - Catalog materials in all formats (LIT5, LIT10, LIT14), (TC1, TC2)
  - Inventory library resources in all formats (LIT5, LIT10, LIT14), (TC1, TC2, TC3, TC4)
  - Maintain library's ejournal holding information (TC1, TC2, TC3, TC4)

### IT Requirement Workgroup Service Description

**Critical:** 0-12 hours; **Vital:** 13-24 hours; **Sensitive:** 1-3 days; **Non-critical:** 3+ days

**Recovery Time Objective:**
- Critical: 0-12 hours; Vital: 13-24 hours
- Sensitive: 1-3 days; Non-critical: 3+ days
**Risk Assessment**

Overall Risk = Probability * Severity (Magnitude – Mitigation)

<table>
<thead>
<tr>
<th>Threat</th>
<th>Probability 1-5 (high-low)</th>
<th>Magnitude 1-3 (high-low)</th>
<th>Overall Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Earthquake</td>
<td>9</td>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>Fire</td>
<td>2</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>Flood / Flash Flooding</td>
<td>2</td>
<td>2.5</td>
<td>5</td>
</tr>
<tr>
<td>Hurricane</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Ice Storm</td>
<td>5</td>
<td>3</td>
<td>15</td>
</tr>
<tr>
<td>Landslides</td>
<td>1</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Power Failure</td>
<td>2</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>Computer Crime</td>
<td>3</td>
<td>3</td>
<td>9</td>
</tr>
</tbody>
</table>

---

**Literature Review**

Signs of the Times
Business Continuity, Disaster Recovery, and IT Audit

John Culshaw
University of Colorado at Boulder
Win Shih
University of Albany, SUNY

University of Colorado at Boulder
• Flagship campus of CU System
• Nearly 29,000 students
• Main library plus 5 branch facilities
• Mid-size ARL library

Experiences
• THEN: Major, non-university events
• NOW: Local disruptive events
Define a Disaster

• “any unplanned disruption of service beyond an acceptable period of time”

Planning History

• 2002 – Risk Assessment
• 2003 – First Recovery Plan complete
• 2005 – IT Audit
• 2007 – Risk Assessment
• 2007 – COOP Planning

Risk Assessment (2007)

• Developed by campus IT Security Office
• Based on frameworks from outside organizations such as NIST and CERT
• 1: Inventory and classification
• 2: IT Security Policy and Process
• 3: General Background Questionnaire
Process and Documents

- IT Security Office Risk Assessment site
  http://www.colorado.edu/its/security/triskmanagement/

- CU Boulder Risk Management Framework

End Result?

- Risk Assessment Report
  - Evaluation of IT Related Risk
  - NOT an in-depth technical review of security controls
  - Example finding
IT Audit

• Uh-oh, an audit!
• Review goals, objectives, opportunities, and barriers…in order to better align work with the institutions priorities

Audit Timeline (all 2005)

• Entrance conference – April
• Information gathering – April through July
• Preliminary report – August
• Review report, develop action plan – Fall
• Exit conference – November
• Final report – November

Audit Reporting

• Quarterly reports to campus until all items complete
• Campus reports on audit status to President and Regents
• Took 12-18 months to complete all items
Sample Audit items

- Some easy items
- Some items required collaboration with others in Libraries, campus, or vendors
- Some really hard

Tabletop Exercise

- Recommended in audit as a way to test in-place disaster plans
- New experience
- Completed Summer 2006

Tabletop Exercise

- Create scenario
- Raise initial questions to fuel discussion
- Don’t discuss with participants in advance
- Have copies of current disaster plans for review during exercise
SNOW EMERGENCY

• On Tuesday, November 16, Boulder is hit with a major snowstorm. The campus was closed as of noon that day. The next day, the campus remains closed. The Boulder Turnpike is closed and most roads leading into Boulder are still impassable.

SNOW EMERGENCY

• At 10:00 am, John receives a phone call that the roof over the main reading room in Norlin Library has caved in. This broke a pipe and caused a flood in the building and there is likely water standing in on the west side first floor. Although no one has been in the machine room, Chinook and the Libraries web server are not responding over the Internet. It is unlikely that anyone can enter the library until sometime November 18.

SNOW EMERGENCY

• The Dean has requested that Systems restore critical IT services no later than Friday, November 19. The campus plans to reopen that day. Some staff will be expected to return to assess damage to the physical library collection.
Discussion Questions
1) What are the first steps?
2) How will the department establish communication?
3) What is needed to reestablish IT services?
4) Think about priorities – this is a week before Thanksgiving – one of the busiest times of the semester.

Tabletop Results
• Slow to start conversation (will depend on your group)
• Became like a game
• Excellent team building opportunity
• Sample outcomes

ILS Vendor Backup Testing
• Service offered by Innovative
• Audit point called for testing of our ability to backup
• This is for ILS – you could perform similar testing for any server on your own hardware
Why Bother?

- ensure backups have meaningful data
- test system restore capability
- peace of mind

How Innovative’s Service Works

- Library sends FULL backup tape to Innovative
- Innovative restores your system on a server at their headquarters

What Innovative Does

- System checks on data and indexes
- Provides your library with the server IP address so that YOU can connect via telnet and Millennium to test the system
What To Look For?

- Chinook Oversight Group developed a list of the functionality we wanted to test.
- Systems Department either performed or coordinated the test.
- Has all of your data been restored properly?
- In the case of emergency, what would you need a restored system to do immediately?
Things to Remember

• You’re working on your restored server – use your regular logins
• Don’t mix up PRODUCTION server and RESTORED server
• You can’t hurt your database – you’re not on your production server
• Some things will not work

Advice

• Invest in a service like this (for vendor-provided ILS) or test on your own (other servers)
• Develop your own list of what functionality needs to be tested on the restored server – and store the list with your disaster plans

Advice

• Understand and follow your backup plan
• Plan this when you have time to test
• Maintain a backup log
Advice

- Clean tape drives according to manufacturer specs
- Replace tapes regularly
- Store backups in a secure, off-site location
- Do NOT provide broad access to test server

Audit vs. Risk Assessment vs. Business Continuity Planning

- Yikes!
- Audit = formal process, action expected/required
- Risk Assessment = formal process, action recommended
- BCP = planning for future