When New Normal Isn’t A Choice- Resiliency In A Time Of Crisis

University of Washington- Information Technology
Presented by: Randy Coggan, UW-IT Business Continuity Manager
Mat McBride, UW-IT Disaster Recovery Manager
Today’s Agenda

- UW-IT’s Business Continuity Program
- UW-IT’s Disaster Recovery Program
Business Continuity
“The continuity of operations during a disaster as it relates to people and processes.”

This should be distinguished from

Disaster Recovery
“The recovery of technology (i.e., applications, information & infrastructure) during a disaster”

YOU NEED TO KNOW YOUR BUSINESS CONTINUITY NEEDS BECAUSE THEY WILL IN TURN DRIVE YOUR DISASTER RECOVERY EFFORTS!
UW-IT’s 4 Step Business Continuity Process

- Business Impact Analysis (BIA)
- Dependency Analysis
- Gap Analysis
- Business Continuity Plan
Business Continuity is an Ongoing Program
Know Your Business Processes?

“A structured activity or task that provides a specific service or product for a particular customer or group of customers.”

For example, “Incident Management” would be considered a business process.
The Business Impact Analysis (BIA)

A Business Impact Analysis is a process to review and determine what impact over time a disruptive event would have on your Business Processes or the functions you perform.

The purpose of the BIA is to:
1. To identify your Business Processes and then
2. To determine whether each Business Process is critical or not using a “ranking process” that we will discuss later.

This analysis focuses on a “reasonable” worst-case scenario. *(Not the “Black Hole”!)*
CRITICAL BUSINESS PROCESSES USED BY UW-IT (MAPPED TO ITIL LIFECYCLE STAGES)

**Strategy**
- Service Strategy
- Financial Management
- Service Portfolio Management
- Demand Management

**Design**
- Service Catalog Management
- Service Level Management
- Capacity Management
- Availability Management
- IT Service Continuity Management
- Information Security Management
- Supplier Management

**Transition**
- Transition Planning & Support
- Change Management
- Service Asset & Configuration Management
- Release & Deployment Management
- Service Validation & Testing
- Evaluation
- Knowledge Management

**Operations**
- Event Management
- Incident Management
- Request Fulfillment
- Problem Management
- Access Management
The Five BIA Impact Criteria

Organizational Scope or Impact

Impact on Trust and/or Reputation

Legal/Compliance/Environmental Impact

Customer Impact

Impact on Revenue/Operating Income

Each Business Process is then ranked as to its’ impact on these areas, from “High” to “No Impact” for several different time frames.
## BIA QUESTIONNAIRE

### Calculated Recovery Time (hrs)
- **5-12**
  - **Selected MTD**
  - **Criticality Rating**
    - **Organizational Scope**: 0.6-High
    - **Trust/Reputational**: 0.6-High
    - **Legal/Compliance/Regulatory**: 0.4-Medium
    - **Customer**: 0.4-Medium
    - **Revenue/Operating Income**: 0.2-Low
  - **Critical-Medium**
    - **Organizational Scope**: 0.6-High
    - **Trust/Reputational**: 0.6-High
    - **Legal/Compliance/Regulatory**: 0.4-Medium
    - **Customer**: 0.4-Medium
    - **Revenue/Operating Income**: 0.2-Low
  - **Business Process**
    - **Organizational Scope**: 0.6-High
    - **Trust/Reputational**: 0.6-High
    - **Legal/Compliance/Regulatory**: 0.4-Medium
    - **Customer**: 0.4-Medium
    - **Revenue/Operating Income**: 0.2-Low
  - **Incident Management**
    - **Organizational Scope**: 0.6-High
    - **Trust/Reputational**: 0.6-High
    - **Legal/Compliance/Regulatory**: 0.4-Medium
    - **Customer**: 0.4-Medium
    - **Revenue/Operating Income**: 0.2-Low

### Calculated Recovery Time (hrs)
- **73-168**
  - **Selected MTD**
  - **Criticality Rating**
    - **Organizational Scope**: 0.2-Low
    - **Trust/Reputational**: 0.2-Low
    - **Legal/Compliance/Regulatory**: 0.2-Low
    - **Customer**: 0.2-Low
    - **Revenue/Operating Income**: 0.2-Low
  - **Important**
    - **Organizational Scope**: 0.2-Low
    - **Trust/Reputational**: 0.2-Low
    - **Legal/Compliance/Regulatory**: 0.2-Low
    - **Customer**: 0.2-Low
    - **Revenue/Operating Income**: 0.2-Low
  - **Business Process**
    - **Organizational Scope**: 0.2-Low
    - **Trust/Reputational**: 0.2-Low
    - **Legal/Compliance/Regulatory**: 0.2-Low
    - **Customer**: 0.2-Low
    - **Revenue/Operating Income**: 0.2-Low
  - **Request Fulfillment**
    - **Organizational Scope**: 0.2-Low
    - **Trust/Reputational**: 0.2-Low
    - **Legal/Compliance/Regulatory**: 0.2-Low
    - **Customer**: 0.2-Low
    - **Revenue/Operating Income**: 0.2-Low

### Calculated Recovery Time (hrs)
- **13-72**
  - **Selected MTD**
  - **Criticality Rating**
    - **Organizational Scope**: 0-No Impact
    - **Trust/Reputational**: 0-No Impact
    - **Legal/Compliance/Regulatory**: 0-No Impact
    - **Customer**: 0-No Impact
    - **Revenue/Operating Income**: 0-No Impact
  - **Critical-Low**
    - **Organizational Scope**: 0-No Impact
    - **Trust/Reputational**: 0-No Impact
    - **Legal/Compliance/Regulatory**: 0-No Impact
    - **Customer**: 0-No Impact
    - **Revenue/Operating Income**: 0-No Impact
  - **Business Process**
    - **Organizational Scope**: 0-No Impact
    - **Trust/Reputational**: 0-No Impact
    - **Legal/Compliance/Regulatory**: 0-No Impact
    - **Customer**: 0-No Impact
    - **Revenue/Operating Income**: 0-No Impact
  - **Access Management**
    - **Organizational Scope**: 0-No Impact
    - **Trust/Reputational**: 0-No Impact
    - **Legal/Compliance/Regulatory**: 0-No Impact
    - **Customer**: 0-No Impact
    - **Revenue/Operating Income**: 0-No Impact

### Calculated Recovery Time (hrs)
- **73-168**
  - **Selected MTD**
  - **Criticality Rating**
    - **Organizational Scope**: 0-No Impact
    - **Trust/Reputational**: 0-No Impact
    - **Legal/Compliance/Regulatory**: 0-No Impact
    - **Customer**: 0-No Impact
    - **Revenue/Operating Income**: 0-No Impact
  - **Knowledge Management**
    - **Organizational Scope**: 0-No Impact
    - **Trust/Reputational**: 0-No Impact
    - **Legal/Compliance/Regulatory**: 0-No Impact
    - **Customer**: 0-No Impact
    - **Revenue/Operating Income**: 0-No Impact
The Dependency Analysis is a process to determine what each “Critical” Business Process as identified in the Business Impact Analysis, depends upon to function. In UW-IT we look at:

- Applications or Features
- Suppliers
- Workforce & Locations
- Vendors
- Data & Vital Records
- Office Equipment

NOTE: In UW-IT only Business Processes that are deemed “Critical” have a “Dependency Analysis” performed.
Gap Analysis

- How long you can function without a Critical Business Process - AKA “Maximum Tolerable Downtime”
- How long you can be without the dependencies that process needs

If you identify gaps between the two then you need to develop viable workarounds or temporary solutions that can be employed until the dependency is restored so your process can resume
Planning Scenarios are those “reasonable” events or risks that are most likely to happen. Some of the most likely scenarios we consider in UW-IT are:

- Loss of Primary Building (i.e., fire or extended loss of power)
- Technology Disruption (i.e., Data Center damage or physical destruction)
- Critical 3rd Party Disruption (i.e., labor disputes or 3rd party financial issues)
- Workforce Disruptions (i.e., HazMat incident or pandemic)
- Broad Regional Event (i.e., earthquake, civil unrest or volcanic eruption)

Once you choose the scenarios to use...
Recovery Strategies

You then consider one or more of the Recovery Strategies to mitigate the scenario’s impact—(“What do I do if this happens?”). In UW-IT we consider these Recovery Strategies:

● Work from an alternate location
● Transfer your workload to existing internal personnel or team
● A third party transfers their workload internally
● Transfer internal workload to an alternate third party (i.e., Supplier, Vendor, etc.)
● Employ other manual workarounds that you develop
Business Continuity Plan Elements

UW-IT Business Continuity Plans contains, at a minimum, the following:

**Basic Elements:**
- Triggers that will cause the Plan to be activated
- Procedures for activating the Plan
- Response procedures and activities
- Recovery procedures and activities
- Stand-down procedures
- Exercise criteria
- Lessons learned from previous exercises

**Basic Components:**
- Contact Lists
- Roles & Responsibilities
- Critical Business Processes
- Detailed Response Procedures and Workarounds
The Business Continuity Plan

The goal of any Business Continuity Plan is to minimize the impact of a disaster to your customers, and to provide an acceptable level of service until normal operations are resumed.

As previously discussed when we looked at “Planning Scenarios”, in UW-IT we decided that the below scenarios were the most likely risks of disaster that we were apt to confront:

- Loss of Primary Building (i.e., fire, extended loss of power)
- Technology Disruption (i.e., Data Center damage, physical destruction)
- Critical 3rd Party Disruption (i.e., technology outage, labor issues, 3rd party financial issues)
- Workforce Disruptions (i.e., localized power outage, pandemic)
- Broad Regional Event (i.e., earthquake, civil unrest, volcanic activity)

A good Business Continuity Plan should be an “All-Hazards” plan- one that is capable of being used during any of the above types of disasters.
Why You Need A Business Continuity Plan

The Gartner Group studied previous disasters and came to the following conclusions:

• 43% of companies without any type of Business Recovery Plan were immediately put out of business by a “major loss” of computer records

• 51% of those companies permanently closed their doors within two years.

While a Higher Ed Institution like the UW might not close its doors permanently, the ability to quickly resume basic operations, such as administrative functions, research and teaching would be impacted by a disaster.

Business Continuity planning provides strategic value by ensuring that the University of Washington can SIGNIFICANTLY minimize those impacts.
YOU NEED TO KNOW YOUR BUSINESS CONTINUITY NEEDS BECAUSE THEY WILL IN TURN DRIVE YOUR DISASTER RECOVERY EFFORTS!
“Information is not knowledge”
- Albert Einstein
90% of DR is **Preparation**

Preparation, in DR terms, is the creation of Resiliency:

- Resiliency in *Architecture*
- Resiliency in *Knowledge*
- Resiliency in *Culture*
Resiliency Approach
Recovery Time and Point

Recovery Objectives

Recovery Point Objective (RPO) vs. Recovery Time Objective (RTO)

- Critical Systems
- Warm Spare
- Cold Spare
- Assigned Recovery
- Deferable Systems

Recovery Point Objective (RPO)
The point in time to which data must be restored in order to resume processing transactions. RPO is the basis on which a data projection strategy is developed. "What I am Willing to Lose".

Recovery Time Objective (RTO)
The point in time from the event occurrence to the recovery of functionality. RTO is the basis on which a service restoration strategy is developed. "How Long I am Willing to Wait".
Recovery Groups

Application

Platform
Middleware/Database

Infrastructure
Server/Virtual/Mainframe/Network
Levels of DR Planning

- **Discrete – DR Plan**
  - Single System or CI
  - Defines parameters for recovering named system or CI
  - Tracks testing and documents changes over time

- **Comprehensive – Ordered Recovery List**
  - All systems defined as Critical or Important
  - Defines Recovery Order, by classification, in terms of Recovery Objective
  - Each entry corresponds to an individual DR Plan

- **Meta – Major Incident**
  - Major Incident management and team structure
  - Defines area(s) of engagement and reporting structure
  - Utilizes both Ordered Recovery List and DR Plans
Disaster Recovery Plan

Covered Areas:

- Plan Information
- Architecture
- Local Recovery
- Failover and Failback
- Backup and Restore
- Exercise Script
- Process Restore Order
## Ordered Recovery List

### Category 1
**Recovery Time Objective 0-2 Hours**

<table>
<thead>
<tr>
<th>System</th>
<th>Owner</th>
<th>Team</th>
<th>Restore Level</th>
<th>Time</th>
<th>Point</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Tools</td>
<td>Paul Lockab</td>
<td>CI-AE</td>
<td>Full</td>
<td>0-1 Hours</td>
<td>0-24 Hours</td>
</tr>
<tr>
<td>Enterprise Disk</td>
<td>Doug Luft</td>
<td>CI-SS</td>
<td>Full</td>
<td>0-1 Hours</td>
<td>N/A</td>
</tr>
<tr>
<td>Enterprise Load Balancing</td>
<td>Scott Norton</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td>Matier Storage</td>
<td>Doug Luft</td>
<td>CI-SS</td>
<td>Full</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td>NTP</td>
<td>David Cox</td>
<td>CI-AE</td>
<td>Full</td>
<td>0 Hours</td>
<td>N/A</td>
</tr>
<tr>
<td>Network Tools Bastion Hosts</td>
<td>Paul Lockab</td>
<td>Net-Tools</td>
<td>Full</td>
<td>6-48 Hours</td>
<td>TBD</td>
</tr>
<tr>
<td>RDS for TierPoint</td>
<td>Scott Hansen</td>
<td>CI-WE</td>
<td>Full</td>
<td>0 Hours</td>
<td>N/A</td>
</tr>
<tr>
<td>Shared Infrastructure</td>
<td>Scott Hansen</td>
<td>CI-WE</td>
<td>Core</td>
<td>6 Hours</td>
<td>TBD</td>
</tr>
<tr>
<td>TSM (Tivoli)</td>
<td>David Cox</td>
<td>CI-AE</td>
<td>Core</td>
<td>0-1 Hours</td>
<td>0-1 Hours</td>
</tr>
</tbody>
</table>

| Directory Services            | Jonathan Pass| IAM-Support | Core | TBD  | TBD  |
| DNS Tools                     | Paul Lockab   | CI-AE       | Core | 0-1 Hours| N/A  |
| Email Infrastructure           | James Morris  | TBD         | Core | TBD  | TBD  |
| Entrust Token Service          | Michael Brogan| IAM-Support | TBD  | TBD  | TBD  |
| Kerberos                      | Michael Brogan| IAM-Support | Core | TDB  | TBD  |
| Melville                      | Jonathan Pass| IAM-Support | Core | TDB  | TBD  |
| Person Registry                | Michael Brogan| IAM-Support | Core | TDB  | TBD  |
| Radius                        | Michael Brogan| IAM-Support | Core | TDB  | TBD  |
| Shibboleth                     | Michael Brogan| IAM-Support | Core | TDB  | TBD  |
| UWWPI (Windows Infrastructure) | Brian Arkills| IAM-Support | Core | TDB  | TBD  |
| Weblogin Service               | Michael Brogan| IAM-Support | Core | TDB  | TBD  |
| UCSADMIN Domain                | Brian Arkills| IAM-Support | Core | TDB  | TBD  |

| Crisis Communication Tools     | Ben Roy      | Crisis Comm | Core | TDB  | TBD  |
| Monitoring Service             | James Morris | TBD        | Core | TDB  | TBD  |
| eOutage                       | Andy Ward    | TBC        | Core | TDB  | TBD  |
# Major Incident Plan

## Disaster Recovery Group – Infrastructure

Activates as part of a Major Incident or Disaster Declaration as directed by the Operations Chief or Disaster Recovery Group Supervisor:
- Restoration of datacenter, network, mainframe, and server environment(s)
- Interim availability and optimization of environment(s) during recovery
- On-site and remote management of failover location(s)
- Communication of operational status and interim availability

### Mobilize

<table>
<thead>
<tr>
<th>Core activation (as determined by Infrastructure Lead):</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Network Engineers</td>
</tr>
<tr>
<td>- Mainframe/Windows/Unix Engineers</td>
</tr>
<tr>
<td>- Critical Environment Engineers</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Expanded activation:</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Facilities (Power, HVAC)</td>
</tr>
<tr>
<td>- Contracted staff / resources</td>
</tr>
<tr>
<td>- Relocation of staff to Failover location</td>
</tr>
</tbody>
</table>

### Assess

<table>
<thead>
<tr>
<th>Potential to Escalate and Situation Assessment to Disaster Recovery Group Supervisor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receive and Distribute any information via the DR Group Supervisor</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Availability and capacity of In Place and Failover recovery locations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interim availability and optimization proposals</td>
</tr>
<tr>
<td>Resource requirements</td>
</tr>
</tbody>
</table>

### Recover

<table>
<thead>
<tr>
<th>Area of Compromise</th>
<th>Interim availability</th>
<th>Optimization</th>
<th>Environment</th>
<th>Communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Datacenter</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mainframe and servers</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Repair/replace hardware</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network adjustment</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server creation (virtual)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bandwidth</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server consolidation / transition to Cloud</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management of In Place environment</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management of Failover environment</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Stabilize

<table>
<thead>
<tr>
<th>Repair, configure, or build the infrastructure environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify stress points in recovery and determine interim availability</td>
</tr>
<tr>
<td>Identify mid/long term operational recovery requirements</td>
</tr>
</tbody>
</table>

| Communicate availability and interim availability status to Disaster Recovery Group Supervisor |
| Optimize infrastructure systems for best performance in recovery environment |

### Return to Normal

| Obtain additional infrastructure (physical hardware or cloud) as necessary to support ongoing recovery |
| Communicate Issues and status to Disaster Recovery Group Supervisor |

<table>
<thead>
<tr>
<th>Environment status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interim availability status</td>
</tr>
<tr>
<td>Capacity status</td>
</tr>
</tbody>
</table>
10% of DR is **Mobilization**

Most of the time, things just fail. But sometimes, they FAIL. Disaster Recovery is concerned with the latter:

- ** Declaring a Major Incident **
- ** Mobilizing Teams **
- ** Executing Scripts **
Major Incident

Major Incident Process
Unit Response Center

TITLES:
COMMAND- OFFICER
SECTION-CHIEF
BRANCH- DIRECTOR
GROUP- SUPERVISOR
UNIT- MANAGER
TEAM- LEADER
Key Takeaways

Everything fails.

But! With resiliency planning, failure is just a correctable aspect of any undertaking.

New Normal is not always a choice you get to make. Business Continuity and Disaster Recovery do not predict the future - they protect it.
Questions?
Thank You!

- UW-IT Technology Business Continuity
  help@uw.edu