Course Materials

DISASTER RECOVERY AND BUSINESS CONTINUITY

Tom Williams
Gladiator Business Continuity Strategy Manager
Jack Henry & Associates
Northville, Michigan
toilliams@jackhenry.com
800-299-4411

August 10 & 11, 2017
Disaster Recovery and Business Continuity

Presented by
Gladiator - A Division of Jack Henry & Associates
And The Graduate School of Banking

August 10-11, 2017

Tom Williams - Gladiator Business Continuity Strategy Manager
Agenda

- Gladiator Services Overview
- Financial Industry Risk Environment
- FFIEC Regulatory Requirements
- Business Continuity / Disaster Recovery Plan Components
- Business Continuity Plan Assessment
- Role of the Information Security Officer
- Centurion Cyber Drill
Three Successful Brands

U.S. Community Banks

U.S. Credit Unions

U.S. & International FI’s
About Gladiator

Who We Serve

- Servicing only financial institutions since 1995
- Core agnostic
- Tightly integrated with Jack Henry Banking® and Symitar®
Brief Introduction to Gladiator Services

- Centurion Business Continuity Planning™/Centurion Disaster Recovery™
- Gladiator® CoreDEFENSE Managed Security Services™
- Gladiator® IT Regulatory Compliance/Policy Products™
- Gladiator® Managed IT Services™
- Gladiator® Hosted Network Solutions™
Gladiator Team Highlights

- Certified team of
  - IT, network, security, and compliance experts
  - Business Continuity / Disaster Recovery Consultants

- Gladiator operations:
  - (11) Disaster Recovery Centers
  - The Mountain (Hardened Recovery Center)
  - IT Regulatory Compliance Center
  - Remote End-user Help Desk
  - (2) Network Operation Centers
  - (2) Security Operation Centers
  - Fully redundant private cloud computing platform
Centurion Disaster Recovery Centers

San Diego, CA
St. Paul, MN
Lombard, IL
Angola, IN
Windsor, CT
Charlotte, NC
Lenexa, KS
Monett, MD
Birmingham, AL
Allen, TX
Financial Industry Risk Environment
Top Concerns Facing Banking Executives Today
Banking is a Risky Business

- Insider Fraud
- Policies and Procedures
- Systems, Personnel, and Budgetary Limitations
- Infrastructure
- Lack of Skills

+ Holistic Risk

- Disasters
- Cyber Threats
- Fraud
- Regulatory Pressure
- Vendors
- Infrastructure
What is Your Bank’s Holistic Risk Profile?

- **Low Risk**
  - Cyber Security
  - BSA/AML

- **Moderate Risk**
  - BCP/DR

- **High Risk**
  - Vendor Mgt
  - Internal Fraud

Risk Levels:
- Low Risk
- Moderate Risk
- High Risk
Banking is a Risky Business

INTERNAL

- Insider Fraud
- Policies and Procedures
- Systems, Personnel, and Budgetary Limitations
- Infrastructure
- Lack of Skills

EXTERNAL

- Disasters
- Cyber Threats
- Fraud
- Regulatory Pressure
- Vendors
- Infrastructure

HOLISTIC RISK
What is the Bank’s Disaster Risk Mitigation Profile?

- **Low Risk**: Business Continuity Plan
- **Moderate Risk**
- **High Risk**: No Business Continuity Plan

Each organization should continually strive to move toward the Low Risk area.
After the disaster?

Will your bank be able to put all the pieces together?
What some Executives think about customer expectations after a disaster?

- Our customers are loyal so they will be understanding and patient until we recover, no matter how long it takes.
- Our I/T team has a plan to get the systems and applications up and that is all the bank needs to recover operations.
- We have a veteran staff and we can handle whatever comes up on the fly.
- All of our critical personnel will be available to assist in the recovery efforts.
- Our core processing is outsourced so we will not be impacted.
Customer Expectations – As Told by Actual Customers

• “I expect the same level of service immediately following a disaster as I had before the disaster.”
• “I want immediate access to my accounts via mobile, internet and telephone banking immediately following a disaster.”
• “I expect expedited, or a higher level of service if the disaster impacted me and my family and I needed emergency monies.”
• “I want the ability to do cash withdrawals immediately following a disaster with no restrictions on the amount I can withdraw.”
• “I want to be able to increase my line of credit, or apply for a loan to help me rebuild if the disaster impacts my family.”
Executive Responses:

Good Question, I am not sure. “My IT team handles that.”

“We will be fully operational by the next day.”

“We really don’t have a real plan and we have not tested what we will do in a disaster situation in years, therefore I am not sure how long it will take to be operational.”

“It depends on the disaster, but I will think we will be operational between 18 – 24 hours.”

“I was told by my IT team that they will have Tier 1 applications up within 2 hours and Tier 2 applications will be available in 6 hours. The remaining applications will be available between 12– 18 hours.”
Comparison - Customer Expectations vs Executive Perception

Customer Expectations
- Same as Normal Service
- Slightly Delayed Service
- Delayed Service
- Severely Delayed Service
- No Service

Executive’s Perceived Recovery Level
- 1 Hour
- 12 Hours
- 24 Hours
- 36 Hours
- 48+ Hours

Actual Recovery Level

Service Level after Disaster

RECOVERY TIME LINE
The Gap: Customer Expectations-Actual Recovery Time?

• Lack of an Enterprise Wide Business Continuity Plan that has been tested at multiple levels.
• The recovery strategy for the Core (In-house processing) is tape based.
• The recovery strategy for the Win-Server environment needs improvement.
• Extensive data re-entry required due to lost of data.
• Did not account for physical recovery of personnel.
• Availability of skilled personnel.
What is the Bank’s Cyber Security Risk Mitigation Profile?

- LOW RISK
  - Incident Response Plan

- MODERATE RISK

- HIGH RISK
  - No Incident Response Plan

Each organization should continually strive to move toward the Low Risk area.
IT Regulatory Exam Focus

2014 – 2015
- Business Continuity
- IT Risk Assessments
- Log Archiving

2015 – 2016
- Vendor Management
- CyberSec Assessment Tool
- Ongoing VA Scanning

2016 – 2017
- Information Security Officer
- SIEM & Breach Detection
- Cyber-Prep & Resiliency
ISO & FFIEC Handbook Guidelines

- Independent ISO or Committee
- Separate InfoSec oversight from IT
- Sufficient knowledge and training
- Rightsized InfoSec program

Source: FFIEC 2006
FFIEC – Information Security Officer Responsibilities

- Information Security Strategy and Policies
- Information Security Risk Assessment
- IT Risk Mitigation
- IT Audits
- Interface with Examiners and Auditors
- Business Continuity Planning
- Disaster Recovery Management
FFIEC – Information Security Officer Responsibilities

- Vendor Management
- Vulnerability Assessments
- Incident Response Management and Threat Information Sharing
- Security Status Reporting
- Information Security Awareness Training
- Board of Directors Reporting
Ensure alignment of Domain Maturity levels to the Inherent Risk Profile Summary

<table>
<thead>
<tr>
<th>Risk/Maturity Relationship</th>
<th>Inherent Risk Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Least</td>
</tr>
<tr>
<td>Innovative</td>
<td></td>
</tr>
<tr>
<td>Advanced</td>
<td></td>
</tr>
<tr>
<td>Intermediate</td>
<td></td>
</tr>
<tr>
<td>Evolving</td>
<td></td>
</tr>
<tr>
<td>Baseline</td>
<td></td>
</tr>
</tbody>
</table>

Although there is no single expected level, as your inherent risk rises, your cybersecurity maturity level should increase.
FFIEC Cybersecurity Assessment Tool (CAT)

Assess maturity and inherent risk
Identify gaps in alignment
Determine desired state of maturity
Implement plans to maintain/sustain maturity
Reevaluate

Source: FFIEC June 2015
The Incident Response Plan
# TABLE OF CONTENTS

- EXECUTIVE SUMMARY ................................................................. ii
- INCIDENT RESPONSE PLAN ....................................................... 1
  - 1.0 OBJECTIVES .................................................................... 1
  - 2.0 INCIDENTS ........................................................................ 1
    - 2.1 Incident Categories ....................................................... 1
  - 3.0 RESPONDING TO AN INCIDENT ........................................ 1
    - 3.1 Organization .................................................................. 2
    - 3.2 Escalation Levels ........................................................... 3
    - 3.3 Escalation Considerations .............................................. 3
    - 3.4 The Incident Response Process ..................................... 3
    - 3.5 Incident Response Team Roles and Responsibilities .......... 6
      - 3.5.1 Escalation Level 0 .................................................... 6
      - 3.5.2 Escalation Level 1 .................................................... 6
      - 3.5.3 Escalation Level 2 .................................................... 6
      - 3.5.4 Escalation Level 3 .................................................... 7
      - 3.5.5 Post Incident ............................................................ 8
- APPENDIX A ............................................................................. 9
  - Contact Lists .......................................................................... 9
- APPENDIX B ............................................................................. 11
  - List of Sources for Alerts or Notification of a Threat ............ 11
- APPENDIX C ............................................................................. 12
  - Federal Reserve Reporting Requirements ............................ 12
- APPENDIX D ............................................................................. 13
  - Reviews and Approvals ......................................................... 13
Incident Response Severity Levels

Level 0
- Normal Operations. IT Technical groups monitoring for alerts from various sources.
- Technical Assessment and Support Team

Level 1
- A threat has been discovered, determine defensive action to take. Communicate with employees of required actions if necessary.
- Technical Assessment and Support Team
- Incident Response Coordinator
- Communication Team

Level 2
- A threat has manifested itself. Determine course of action for containment and eradication. Communicate with employees of required actions, if necessary.
- Incident Response Management
- Incident Response Coordinator
- Technical Assessment and Support Team
- Communications Team

Level 3
- Threat is widely spread or impact is significant. Determine course of action for containment and eradication. Communicate with employees and customers if applicable. Prepare to take legal action for financial restitution etc.
- Incident Response Management
- Incident Response Coordinator
- Technical Assessment and Support Team
- Communications Team
Incident Response Procedures

1. Identify Event
   - Unusual Outbound Traffic
   - Anomalies in privileged accounts
   - Data in wrong places

2. Inform Appropriate Personnel
   - Information Security Officer
   - Executive Team / Legal
   - Others based on IRP

3. Initiate Documentation Process
   - Date & Times of incident
   - How event was reported
   - Identification of information asset

4. Assign Incident Severity Level
   - Preserve system & audit logs
   - Record/preserve evidence for authorities
   - Work with authorities

5. Contain & Eradicate Event
   - Unusual Outbound Traffic
   - Anomalies in privileged accounts
   - Data in wrong places
Incident Response Procedures (Cont)

- **Implement Preventive Measures**
  - Change passwords & ID’s
  - Don’t turn off compromised machines
  - Place holds on customer accounts

- **Notify Regulators / Customers**
  - Recommendation to customers
  - Fraud alerts & monitor credit reports
  - Data in wrong places

- **Establish Media Communications**
  - Media scripts
  - Websites-Email-News Conference
  - Social Media sources

- **Perform Follow-up Forensic Analysis**
  - What happened-Where-When-How
  - Follow-up with external organizations
  - FBI-FCC—Federal Trade Commission, etc.

- **Post Incident Activities / Testing**
  - Create Executive Report
  - Store Info Security Incident & Evidence
  - Follow-up Testing
• Calculating cyberattack impacts have focused mainly on the direct costs
• Be aware that there are many hidden factors

Impact of a Breach

Beneath the surface of a cyberattack

Deloitte. Beneath the surface of a cyberattack, 2016
Operational Impact of a Breach

Fourteen cyberattack impact factors

A wide range of direct and/or intangible costs contribute to the overall impact of a major cyber incident.

- Technical Investigation
- Customer breach notification
- Post-breach customer protection
- Regulatory compliance
- Public relations
- Attorney fees and litigation
- Cybersecurity improvements

Above the surface
better-known cyber incident costs

Source: Deloitte. Beneath the surface of a cyberattack, 2016
Operational Impact of a Breach

Insurance premium increases
Increase cost to raise debt
Impact of operation disruption
Lost value of customer relationships
Value of lost contract revenue
Devaluation of trade name
Loss of intellectual property

Source: Deloitte. Beneath the surface of a cyberattack, 2016
Analyzing the Information

During the analysis phase of the BIA, results of the vulnerability assessment should be analyzed and interpreted to determine the overall impact of various threats on the financial institution. This analysis process should include an estimation of maximum allowable downtime (MAD) that can be tolerated by the financial institution as a result of a disruptive event. MAD estimates that may be used include the following:

- Nonessential - 30 days
- Normal - 7 days
- Important - 72 hours
- Urgent - 24 hours

**Critical** - minutes to hours

Each business function and process should be placed in one of these categories so that management can determine applicable solutions to ensure timely recovery of operations. Management should then determine which business functions represent the highest priority for recovery and establish recovery objectives for these critical operations. The Business Continuity Planning Committee or Coordinator should discuss the impact of all possible events that may never occur. For example, documenting the impact of an event such as a fire, flood, or power outage that may result in equipment failure, destruction of facilities, data loss, loss of backup facilities, vendors, or service providers. Each business function and process should estimate MADs.
Business Continuity Planning Challenges

- Meeting FFIEC BCP requirements:
- Building an enterprise-wide plan
  - Recovery plan for each Business Unit vs a DR Plan for the IT Business Unit
- Standardization of plan and content between business units
- Plan Testing at various levels, i.e., technology, business units
- Repository of plan information in a web-based BCP tool
- Incorporating new acquisitions/mergers into BCP
- Lack of plan development skills and time to develop BCP
FFIEC BCP Guidelines

Risk Monitoring
- Plan Maintenance
- Plan Testing
  - Business Units
  - Systems / Apps

Business Impact Analysis (BIA)
- Critical Business Functions
- Disaster Impacts
- Prioritization
- Recovery Windows
- Recovery Strategies
- Resources

Risk Management
- Enterprise-wide BCP
- Emergency Plans
- Crisis Management Plans
- IT & Business Unit Plans
- Family Disaster Plan

Risk Assessment
- Threats
  - Natural
  - Human
  - Technical
  - Cyber Attacks
RTO’s of Critical Business Functions – BIA Based

- Cash Checks
- Customer Inquiries via phones
- Handle deposits & withdrawals
- Accept loan payments
- Account transfers
- Balance cash drawers
- Handle security issues
- Handle stop payments
- Issue cashier’s checks

15 minutes – 4 Hours
4 – 8 Hours
8 – 24 Hours
24 – 48 Hours
RTO’s of Critical Business Functions – BIA Based

- Order ATM cards/debit card
- Calculate Payments using projection screens
- Loan status calls
- Do cash advance
- Fund home equity loans
- Fund second trustee loans
- Issue onsite ATM cards
- Issue temporary checks

15 minutes – 4 Hours
4 – 8 Hours
8 – 24 Hours
24 – 48 Hours
<table>
<thead>
<tr>
<th>Department or Business Unit</th>
<th>Business Function/Activity</th>
<th>Corporate Impact</th>
<th>System Required</th>
<th>Application Required</th>
<th>Manual Process</th>
<th>Recovery Time Objective (RTO)</th>
<th>Recovery Point Objective (RPO)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch Operations</td>
<td>Cash checks</td>
<td>High</td>
<td>iSeries</td>
<td>Silverlake</td>
<td>Yes</td>
<td>4 Hours</td>
<td>15 Min</td>
</tr>
<tr>
<td>Telephone Express Center</td>
<td>Process loan payments</td>
<td>High</td>
<td>iSeries</td>
<td>Silverlake</td>
<td>Yes</td>
<td>8-24 Hours</td>
<td>15 Min</td>
</tr>
<tr>
<td>Telephone Express Center</td>
<td>Process wire transfers</td>
<td>High</td>
<td>iSeries</td>
<td>Silverlake</td>
<td>No</td>
<td>8 Hours</td>
<td>15 Min</td>
</tr>
<tr>
<td>Information Technology</td>
<td>Administer backups</td>
<td>High</td>
<td>Client Server</td>
<td>ProcessPro</td>
<td>Yes</td>
<td>4-8 Hours</td>
<td>N/A</td>
</tr>
<tr>
<td>Deposit Services</td>
<td>Set up close day, close month process</td>
<td>High</td>
<td>Client Server</td>
<td>ProcessPro</td>
<td>Yes</td>
<td>3+ Days</td>
<td>24 Hours</td>
</tr>
<tr>
<td>Electronic Banking</td>
<td>Prepare VRU report</td>
<td>High</td>
<td>Client Server</td>
<td>ProcessPro</td>
<td>Yes</td>
<td>3+ Days</td>
<td>6 Hours</td>
</tr>
<tr>
<td>Electronic Banking</td>
<td>Hot card entry</td>
<td>Low</td>
<td>Client Server</td>
<td>InTouch</td>
<td>Yes</td>
<td>8 Hours</td>
<td>12 Hours</td>
</tr>
<tr>
<td>Electronic Banking</td>
<td>Set up new Internet accounts</td>
<td>Medium</td>
<td>Client Server</td>
<td>PinPoint</td>
<td>No</td>
<td>8 Hour</td>
<td>12 Hours</td>
</tr>
<tr>
<td>Item Processing</td>
<td>Set up new Internet accounts</td>
<td>Medium</td>
<td>Work station</td>
<td>NetTeller</td>
<td>No</td>
<td>4 Hours</td>
<td>2</td>
</tr>
</tbody>
</table>
Business Continuity – Disaster Recovery
Plan Components
# The Major Components of the BCP

## People
- Employees
- Customers
- BCP / DR Teams
- Vendors
- Fire / Police
- Utilities
- Regulators
- Plans / Procedures
- Documentation

## Facilities
- Alternate work areas
- Repaired facilities
- Recovery centers
- Hospitals
- Shelter areas
- Mobile Recovery Units
- Off-site storage facilities

## Technology
- Systems
- Servers
- Applications
- Data
- Telecommunications

+ A Plan ties it all together
The Most Critical Component – People

Team members require consistent training and testing
Facilities - Physical Recovery Considerations

- Branch Offices
- Work from Home
- Vendor Recovery Site
- Internal Recovery Site
- Mobile Recovery Unit
- Office/Remote Workspace
- Temporary Lease Facility
Technology - Equipment Recovery Considerations

- Store equipment in advance
- Purchase equipment when needed
- Drop Ship Equipment Service
  - Mainframe
  - Servers
  - Workstations
  - Printers / Fax Machines
  - Phones
  - Routers / Switches
- Vendor provided at Recovery Site
- What is your equipment recovery strategy?
Business Continuity Plan Documentation

- Emergency Management Plan (Per Facility)
- Crisis Management Plans
- Information Systems Recovery Plan
- Business Unit Recovery Plans
- Branch Office Recovery Plans
- Executive Summary
- Plan Testing & Exercise Guide
**Business Continuity Team Structure**

### Crisis Management Team
- **Management**
  - Team Leader
  - Alt. Team Leader

### Business Unit Recovery Teams

#### Administration
- Team Leader
- Alt. Team Leader
- Audit
- Compliance
- HR
- Training
- Marketing
- Investments
- Maintenance

#### Information Systems
- Team Leader
- Alt. Team Leader
- Information Systems

#### Finance
- Team Leader
- Alt. Team Leader
- Bookkeeping
- Accounting
- Finance
eBanking

#### Deposit Operations
- Team Leader
- Alt. Team Leader
- Deposit Operations
- Retail Banking/Consumer Lending

#### Loan Operations
- Team Leader
- Alt. Team Leader
- Loan Analyst
- Loan Processing
- Commercial Lending
- RE Mortgage

*ProfitStars®*
1. Team Information
   1. BU Recovery Team - Recovery Organization Charts
   2. Workspace & Equip. Summary - Facilities & Locations
2. Notifications
   1. Personnel Notification Script - Business Unit Call List
   2. Call List Team Leaders – External/Internal Notifications
3. Recovery Tasks
   1. Recovery Phases – Recovery Tasks for Rec. Team
4. Business Impact Analysis (BIA) Reports
5. Business Function Recovery Procedures
6. Recovery Forms
7. Appendix
Business Continuity Planning Software Tool

- Based on Best Practices of the Financial and Business Continuity industry.
- Designed solely for financial institutions and based on the FFIEC BCP Guidelines.
- Web-based and hosted on an independent network.
- Ability to access software 24/7.
- Built on a Relational Database platform, i.e. SQL.
- Fosters plan ownership at the business unit level.
- Access plans for planning purposes, testing, maintenance and plan execution from any web browser.
- Supported by experts in the business with a solid financial backing and a strong record of consistency and support.
Communications Tool to communicate with Employees – Customers - Vendors
<table>
<thead>
<tr>
<th>Plan Elements</th>
<th>In Plan</th>
<th>Not In Plan</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emergency / Evacuation Plan</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Succession Plan – Escalation Plan</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alternate Work Locations Identified</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Impact Analysis Conducted</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recovery strategies in place to restore critical functions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recovery Timeline Identified</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Critical Documentation Identified</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resource Requirements Identified per business function</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Assessment-Risks Identified and Prioritized</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plan Elements</td>
<td>In Plan</td>
<td>Not In Plan</td>
<td>Comments</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>--------</td>
<td>-------------</td>
<td>----------</td>
</tr>
<tr>
<td>Media Spokesperson Identified</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Command Center Identified</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plans per department with specific information for that team?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Designated employee call list documented</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manual Procedures Documented</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Notification List – External Contacts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Notification List – Internal Contacts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recovery Teams Identified</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recovery Tasks Identified for Personnel</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Critical forms identified</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Business Continuity Plan Assessment

<table>
<thead>
<tr>
<th>Plan Elements</th>
<th>In Plan</th>
<th>Not In Plan</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core Processing System (Software) Recovery Strategy / Procedures in place</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Win Servers Recovery Strategies in place</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telecommunication Recovery Strategies</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Electronic interface recovery strategies i.e., Internet, voice response,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vital Records Recovery Strategy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plan Testing Strategy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Evacuation Drills</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hot Site Test</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recovery Team Exercises</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plan Maintenance Program in place</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Plan Execution Phases

Pre – Disaster Activity

Disaster Strikes

Crisis Management Phase

Relocate Phase

Restore Operations Phase

Rebuild Phase
Plan Execution / Recovery Timeline

Minutes to Days – How long for your bank?

Disaster

Crisis Management Phase
- Evacuation & Safety
- Damage Assessment
- Communications
- Disaster Declaration

Relocate & Restore Phase
- Notifications
- Mobilization
- Relocation
- Restore

Recover Business Functions Phase
- Restore Business Unit Functions & Processes using Business Unit Recovery Plans

Services Resumed
Rebuild & Return Phase

- Warnings / Public Information
- Debris clearance, removal & disposal
- Utilities & communications restoration
- Temporary housing
- Detailed building inspections
- Redevelopment planning
- Environmental assessments
- Demolition
- Reconstruction
- Hazard mitigation

Disaster Crisis Management Phase
Relocate & Restore Phase
Recover Business Functions Phase

Plan Execution / Recovery Timeline
Plan Execution Phases

Crisis Management Phase – Use the Crisis Management Plan

Emergency / Crisis Management Plan

Relocation Phase – Use Business Continuity Plan consisting of IT & BU Plans

I/T Disaster Recovery Plan

Business Unit Recovery Plans

Recover Business Functions Phase

Restoration Plan - Rebuild & Return Phase

Disaster Timeline
Emergency Management Plan for each location

- Notification List for Main - Branch Offices – Local Authorities
- General Emergency Policies
- Evacuation Policy
- Emergency Tasks
- Accounting for Personnel After a Disaster
- Reacting to a Disaster
- Evacuation Meeting Place per Facility / Department
- Disaster Scenarios
  - In Case of Fire:
  - In Case of Severe Tornado:
  - In Case of Flood:
  - In Case of Hurricane Watches/Warnings:
Crisis Management Phase Tasks

- **C**: Provide safety and shelter for employees / customers. Provide medical assistance as required. Activate Business Continuity Plan
- **R**: Declare official disaster with employees, customers, vendors, etc.
- **I**: Shut off gas, water and other utilities. Secure vaults, cash drawers, etc. Power down and protect equipment. Perform damage assessment
- **S**: Order fuel in advance for generator if applicable
- **I**: Perform a system backup if applicable
- **S**: Take employee / customer head count prior / after the event
- **I**: Notify Human Resources and authorities of people not accounted for
Crisis Management Phase Tasks

- Secure the facility. Establish a liaison to interact with authorities as required. Establish Emergency Command Center for the bank.
- Determine who is available to work and conduct initial status meeting. Assign initial tasks based on available resources.
- Communicate with vendors, i.e. alarm company, recovery center, temp. workspace provider, telecommunications, regulatory agency, etc.
- Secure critical documents, files, etc.
- Salvage equipment as required.
- Establish communication protocol.
- Update web site and status hotline as required.
Team members must protect their family first

Family Disaster Plan and

V. IF YOU EVACUATE

1. Take with you:

- Medicines and first aid kit
- Flashlight, radio and batteries
- Important documents and cash
- Blankets and extra clothes
- Personal sanitary items
- Any additional items you feel are necessary
Four Steps to Family Preparedness

1. Get Informed
2. Make a Plan
3. Assemble Disaster Kit
4. Test Maintain Plan

Family Disaster Plan
<table>
<thead>
<tr>
<th><strong>R</strong></th>
<th>Retrieve critical resources, documents from off-site location</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>E</strong></td>
<td>Set up alternate work locations; mobile trailer, internal recovery center, alternate workspace</td>
</tr>
<tr>
<td><strong>S</strong></td>
<td>Travel to alternate work locations. Set up security at alternate facility</td>
</tr>
<tr>
<td><strong>T</strong></td>
<td>Put signage on damaged facility</td>
</tr>
<tr>
<td><strong>O</strong></td>
<td>Re-establish communications between alternate data processing site and branches</td>
</tr>
<tr>
<td><strong>R</strong></td>
<td>Provide authorities and security staff with list of employees allowed to enter damaged facility</td>
</tr>
<tr>
<td><strong>E</strong></td>
<td>Notify vendors of alternate work address for deliveries. Redirect mail and courier deliveries</td>
</tr>
</tbody>
</table>
Recover Business Function Tasks

- Execute Business Unit Recovery Plans
- Determine time needed to process backlog work
- Reconstruct / Re-enter “Work in Process”
- Implement business unit contingency strategies
- Install salvaged equipment
- Develop personnel work schedule
- Update web-site and media sources
Banking Technology Landscape

Simple, Easy to Support
- Core Apps
- Green Screen Terminals
- Item Processing
- IVR
- Simple WAN
- ATM’s

Moderate, Increased Support
- Teller Capture
- Online Banking
- More Complex WAN
- New Account Platform
- CRM
- SaaS
- Profitability Applications

Complex, Difficult to Support
- Document Imaging
- Windows Based Products
- Browser Based Apps
- VPN’s
- Citrix Thin Clients
- Terminal Servers
- Mobile Banking
- IP Telephony
- IaaS
- Cloud Computing
- Virtual Desktops
- DR replication
- Smart Branches
- Heavy Reliance on Internet
- Social Media
- Integrated AD Apps
- PaaS
- Very Complex WAN
- Server Virtualization
Application Backup / Recovery Strategies

- What is our **Recovery Time Objective** (RTO) for your core and Windows server environment?
- What is our **Recovery Point Objective** (RPO) for your core and Windows server environment?
• Backup methods – Where is data going?
  – **Tape**
    • Onsite in vault, offsite at another branch, offsite at vendor
  – **Hard Drive**
    • Onsite in vault, offsite at another branch, offsite at vendor
  – **Virtualization**
    • Snapshots locally
    • Snapshots to another branch
    • Snapshots to offsite vault (vendor-provided)
• Restore Methods – Where are you going to restore?
  – Tape – Hard Drive – Virtualization
    • A physical computer to restore information to
    • A computer room with the proper infrastructure, i.e., electrical, air
    • Network connectivity
    • Generators
    • Matching configurations of equipment at both locations
Levels of Recovery

1. **File & Folder Recovery**
   - Data

2. **System Recovery**
   - Assemble Technical Team
   - Procure Hardware to Restore Data (Dissimilar)

3. **Workgroup Recovery**
   - Assemble Technical Teams
   - Procure Hardware to Restore Data (Dissimilar)
   - Procure Communications
   - Applications

4. **Enterprise Recovery**
   - Resume Critical Business
   - Procure Location HVAC/Utilities
   - Provision Security
   - Assemble Technical & Recovery Teams
   - Procure Communications
   - Applications
   - Data
   - Procure Hardware to Restore Data (Dissimilar)
The plan must address different recovery levels

System Failure

Network Failure

Site Failure

Branch 1

Branch 2

Branch 3

Production Processing
System / Application Recovery Strategies

- Traditional Media Device Backup
  - Tape – USB – Hard Drive – CD
- Virtualization / Replication
- Electronic Vaulting
- High Availability
Recovery Time – Recovery Strategies

- **Continuous Availability**
  - Replicate core in-house and to another system at an off-site data center
- **Virtualization**
  - Electronic backup of servers to an off-site location.
  - Windows, Linux, and Unix
- **Virtual Server Recovery (VSR)**
  - A virtual server environment that can be configured to match your needs
- **Tape Recovery**
  - Regional hot sites mirror diverse financial institutions’ operational infrastructures and recreate unique business environments

![Graph showing Recovery Time Objective and Criticality Level]

- **Recovery Time Objective**
  - Min HRS
  - 4 HRS
  - 8 HRS
  - 24 HRS
  - 48 HRS
  - 72 HRS
- **Criticality Level**
  - Non-Essential
  - Important
  - Urgent
  - Critical

Tape Recovery
Virtualization
Continuous Availability
Challenges of In-House Technology

• Technology obsolescence
• Unpredictable capital expense costs
• 24/7 monitoring
• Uptime and availability
• DR-BC (RTO / RTP)
• IT regulatory compliance
• Staffing and retaining IT personnel
Inherent Problems with Traditional Tape Recovery

- Personnel may not be available to transport tape.
- Tapes may not be accessible due to the disaster.
- Data loss based on when the last backup was stored off-site.
- Tapes may be damaged as a result of the disaster.
- Tape errors when trying to restore at the recovery center.
- Roads may be damaged or crowded due to evacuations.
- Airports may be closed.
- Recovery Time Objectives (RTO) may not be met.
Take advantage of technology to:

• Reduce the human dependency on restoring your technology infrastructure.
• Eliminate having to transport tapes and paper documents to the recovery center.
• Electronically replicate systems & servers,
• Communicate with employees through an Emergency Notification System that they can also use to provide updates of their status.
Typical Operating Environments

**SCENARIO 1**
- CORE: In-House
- SERVERS: In-House

**SCENARIO 2**
- CORE: Outsourced
- SERVERS: In-House

**SCENARIO 3**
- CORE: In-House
- SERVERS: Outsourced

**SCENARIO 4**
- CORE: Outsourced
- SERVERS: Outsourced
In-House Processing Considerations

- Responsible for the restoration of the following:
  - Recovery of Core System
  - Recovery of Server / Network Recovery
    - Exchange Servers - Domain Controllers
    - Application Servers
  - Telecommunications - Voice Recovery
  - Equipment setup & Reconfiguration
  - Facilities
SCENARIO 1 – Bank A - CORE: In-House
SERVERS: In-House – Tape Recovery Strategy

Last EOD Backup of usable data
Friday 8:00 pm

Disaster Strikes
Monday 3:47 pm

67.47 Hours of Data Loss

Disaster

Declare Disaster

5 Hours

Travel to Recovery Center

13 Hours

Last EOD Tapes Friday 8:00 PM

6 Hours

System Restored

7 Hours

System Available

Tape Recovery Strategy

Time to Recover = 31 Hours

ProfitStars
**SCENARIO 1 – Bank B - CORE: In-House**

**SERVERS: In-House – Bank B – Replication**

- **Last Data Snapshot**: 3:32 pm Monday
- **Disaster Strikes**: Monday 3:47 pm
- **Data Loss**: 15 Minutes
- **Time to Recover**: 30 Minutes
Disaster Avoidance Concept – Bank B

- Disaster Avoidance Decision
- Switch to Secondary System
- Potential Disaster Event
- Disaster
- Disaster Avoidance Period
- Recovery of Technology Avoided (RTO)
- Recovery of Business still Required
- TIME
Out-Sourced Processing Considerations

- Responsible for the restoration of the following:
  - Connectivity back to the Core Processing Site
    - (jConnect Backup Router)
  - Server / Network Recovery
    - Exchange Servers - Domain Controllers
    - JHA & 3rd Party Applications
  - Telecommunications - Voice Recovery
  - Equipment setup & Reconfiguration
  - Facilities
- A plan to deal with a disaster that strikes the facility
The FFIEC Testing Principals

- Define roles / responsibilities for testing and evaluation.
- Use the BIA/Risk Assessment as the test foundation.
- Enterprise-wide testing should be conducted annually.
- Testing should be viewed as a continuous cycle.
- The testing program should be reviewed by an independent party.
- Test results should be compared against the BCP to identify any gaps between the testing program and business continuity plan. guidelines.
Develop a Test Plan

Identify Scope
Set Test Objectives
Select Training Methods
Identify Resource Requirements
Identify Schedule Options
Identify Participants
Identify Test Budget
Conduct Test
Test at Multiple Levels

- DR Plan Testing for IT
  - Test the restoration of the technology
- Business Continuity Plan Testing
  - Test the Business Unit Plans
- Communications Plan Testing
  - Test communications between employees, customers, media, etc.
- Relocation Plan Testing
  - Test where employees will relocate to
- Enterprise Testing
  - Test multiple test components simultaneously
Mock Disaster Drill Testing Model
Mock Drill: Background

• For the past few days, local weather forecasters have been talking about the potential for severe weather.

• The prediction is due to a particularly strong storm cell that is moving toward the Madison, WI area.
Mock Drill: Sunday, May 1

- Local weather forecasts are warning Madison, WI residents of the possibility of a very strong thunderstorm “super cells” in the area during the next 24 hours.
- These storms are likely to contain very heavy rain, lightning and high winds. Hail and tornadoes are a good possibility.
Mock Disaster Scenario-Monday – May 2 - 8:20 AM

- Employees at ABC Bank had settled into their daily work routines.
- Chris Woodson and John Brita were discussing Chris’s vacation last week and the fantastic time he had.
While in the break room, Brenda Amburgey and Keli Reif started to discuss the latest weather report on the news station which stated the following:

- “A Severe Storm is now in effect for Allen County.”

- The station also states that “A Tornado Watch” has been issued for the Madison, WI area and the surrounding areas.”
• The National Weather Service has spotted heavy rains, hail, high winds, and tornados near Madison, WI and are moving northeast.

• As a result of these conditions, an official **Tornado Warning** for the area is declared.
Monday – May 2 – 10:00 AM
The FAA orders a shutdown for all inbound and outbound flights at Indianapolis and Ft Wayne International Airport until further notice due to the weather moving into the area.
The courier enters the Service Center screaming that he has seen the tornado heading this way.
• The tornado hits the Madison, WI area and is rated a level F3 with winds up to 206 miles per hour.
• The Service Center has sustained serious damage.
• The windows are blown out and the roof is severely damaged.
• The bank structures is also in question.
The storm has passed through the area, and a steady rain is now falling.

It is obvious the Service Center has been badly damaged.

Windows have been broken, and there is debris scattered throughout the bank area.

There is a natural gas smell in the area, possibly from a leaking gas line.

Media is reporting a tornado touchdown that has left a path of destruction.
Outside the office...

- Vehicles in parking lots and garages have been damaged or destroyed.
- Debris from the storm damage is scattered about.
- Some streets are blocked with obstacles.
- The police are arranging for transportation into the area for support personnel to assist with the evacuation.
- There is no cell phone service available.
- Land telephone service is out in the area.
- Many homes and businesses are severely damaged.
All area schools announce that they are suspending classes for the day and perhaps several additional days.

Bus routes are being activated.

Parents who wish to pick up children are requested to do so immediately.
Monday – May 2 – 12:30

- Electrical power is off in the Madison, WI area.
- There is no indication on when power will be restored.
- The Service Center has severe damage to the roof and there is no power to the facility.
- No one is allowed into the building until repairs and inspections have been completed. Possibly 2 weeks.
- The generator that services the Service Center has been damaged as a result of the tornado.

Centurion Disaster Recovery Services
Power is out throughout Madison, WI.
The Crisis Management Phase

- You are now in the “Crisis Management Phase”.
- List the action items that should be done to deal with this phase of the disaster event.
DAY 1
The Crisis Management Phase

<table>
<thead>
<tr>
<th>Identify the tasks that should occur during the Crisis Management Phase.</th>
<th>Resources Required</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify the tasks that should occur during the Crisis Management Phase.</td>
<td>Resources Required</td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>1. Command Center Establishment</td>
<td>Team Location, Telecom,</td>
</tr>
<tr>
<td>2. Damage Assessment</td>
<td>Facilities Manager, Insurance, Emergency Personnel, Contractor</td>
</tr>
<tr>
<td>3. Employee Assessment</td>
<td>Human Resources, Management</td>
</tr>
<tr>
<td>4. Declaring a Disaster</td>
<td>Executive Team Member/Crisis Mgmt Team</td>
</tr>
<tr>
<td>5. Disaster Recovery Plan Coordination</td>
<td>Command Center Team and Business Unit Team Team Leaders</td>
</tr>
<tr>
<td>6. Insurance Company Notification</td>
<td>Command Center Team, Facilities Manager</td>
</tr>
<tr>
<td>7. Public Notification</td>
<td>Marketing Director or COO</td>
</tr>
<tr>
<td>8. Create Work Transfer Strategy</td>
<td>Command Center Team, Business Unit Team Team Leaders</td>
</tr>
</tbody>
</table>
**The Relocate / Restore Phase**

<table>
<thead>
<tr>
<th>Identify where your business unit will relocate to and the tasks that should occur during the Relocate / Restore Phase</th>
<th>Resources Required</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The T1 line between the Service Center and the data center is down. You don’t know the circuit ID or what contact to make to get service restored. Where can you get this information?

Challenge: _______________________________________________________________________________________

What is your plan of action to respond to this challenge?
____________________________________________________________________________________________________

Document the steps required to respond to this challenge?:
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________

What resources will you need?: _________________________________________________________________________
• It is now **Tuesday, Day 2**, of the disaster event.

• You have a skeleton operations process in place at your alternate site.

• Your core system is still down.
Monday – 4:30 PM

- Television reporters from Fox and CBS affiliates are asking for an on-camera interview with a spokesperson for the bank.

- They want a response to allegations from someone claiming to be a bank Team Member who stated that “the building is flattened, files and computers are destroyed, and the bank cannot operate.”
Top DR Trends for 2017

• Managed Recovery solutions will become the industry standard due to:
  – Cost
  – High data requirements
  – Skills
  – Personnel requirements
  – Geographic separation

• Electronic vaulting will replace tape backup for Disaster Recovery

• RPO’s will be measured in minutes
Next Steps

1. Ensure you have Executive support for the BCP & Cyber Security.
2. Have your BCP & Incident Response Plan (IRP) reviewed by Experts.
3. Conduct a Mock Disaster Drill using your BCP and IRP.
4. Determine if outside expertise is required to improve your plan, or if the work will be done internally.
5. Ensure that your BCP is structured at the department level.
6. Build / improve your plan and test it regularly.
Plan Execution Process

Event Occurs

1. Evacuation
2. Stabilize Environment
3. Assess and Report Damage
4. Declare Disaster

Crisis Mgmt Team Leader

1. Activate Command Center
2. Conduct Crisis Mgmt Status Meetings
3. Relocate Staff To Alt Workspace
4. Conduct Bus Unit Status Meeting
5. Activate Recreation Procedures - WIP
7. Restore System Applications
8. Restore Telecommunications
9. Restore Item Capture
10. Restore Data Processing
11. Prepare to Re-occupy Primary Site

Escalation Process

1. Activate Management Team
2. Activate I/S Team
3. Activate Administrative Team
4. Activate Damage Assessment Team

Begin Salvage

1. Begin Media Relations / Press Release
2. Mobilize Recovery Teams
3. Relocate Staff To Alt Workspace

Begin Restoration Of Affected Site

1. Travel to Hot Site (I/S Team)
2. Activate Hot Site(s)

Prepare to Re-occupy Primary Site

1. (Crisis Mgmt Team)
2. (Business Unit Team)

ProfitStars
Partnering with Gladiator Will Improve Your BCP & Cybersecurity Strategy

- Business Continuity
- Disaster Avoidance – Disaster Recovery
- Multilayered security to mitigate cybersecurity risk
- 24/7 security monitoring
- Provide visibility into security and controls
- Certified security and compliance staff
- Empower management oversight
- Protect your reputation
Disaster Recovery Motto

- Manage **Resources**
- Manage **Relationships**
- Be prepared to deal with any **Situation**
- Conduct the above three in a **Timely** matter
Additional Information on BCP and Disaster Recovery

- Centurion Disaster Recovery (www.centuriondr.com)
- Disaster Recovery Journal (www.drj.com)
- FFIEC (www.ffiec.gov)
- American Red Cross (www.redcross.org)
- Federal Emergency Management Agency (www.fema.gov)