We possess a unique blend of knowledge and experience which combines the focus, dedication and independence of a specialist firm, with the methodologies & tools, global presence, and deep skill-sets of the Big 4 or larger consulting firm.

MHA Consulting
MHA combines the strengths of the large consulting companies and independent alternatives...without compromise

Big Four:
- Methodologies & tools
- Experienced professionals
- Depth of risk consulting services
- Financial & management stability

Boutique:
- Responsive client service
- Focus on core offerings
- Senior personnel
- Timely
MHA’s knowledgeable professionals have decades of experience working with clients in a broad array of industries. We have deep competency in the following industry categories:

<table>
<thead>
<tr>
<th>Education</th>
<th>Financial &amp; Insurance Services</th>
<th>Industrial Products</th>
<th>Energy &amp; Utilities</th>
<th>Consumer Products</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arizona State University</td>
<td>American Express</td>
<td>Dial Corporation</td>
<td>Public Service Co. New Mexico</td>
<td>Forever Living Products</td>
</tr>
<tr>
<td>Mesa Community College</td>
<td>Blue Cross Blue Shield Arizona</td>
<td>Henkel</td>
<td>Central Arizona Project</td>
<td>Guitar Center</td>
</tr>
<tr>
<td>University of Phoenix</td>
<td>Discover Card</td>
<td>Phelps Dodge (Freeport McMoran)</td>
<td>Metropolitan Water District California</td>
<td>PetSmart</td>
</tr>
<tr>
<td>Johnson &amp; Wales University</td>
<td>Early Warning Services</td>
<td></td>
<td></td>
<td>Varian Manufacturing</td>
</tr>
<tr>
<td>Thunderbird School Intl Mgmt</td>
<td>FPIC Insurance Group</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Health Alliance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ohio National</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Scottsdale Insurance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Healthcare &amp; Life Sciences</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Amgen</td>
<td>Centra Health</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Medicis Pharmaceutical</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>OhioHealth</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Phoenix Children’s Hospital</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Scottsdale Healthcare</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TriWest Healthcare</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Travel &amp; Entertainment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Harrah’s Entertainment</td>
<td>Regal Entertainment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Pegasus Solutions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SkyWest</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Government Services</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>City of Tempe Arizona</td>
<td>Integrated Criminal Justice Info. Systems</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Overview

- Business Continuity Management (BCM) Defined
- The Business Impact Analysis (BIA)
- Recovery Strategies
- The Business Continuity Plans (BCP)
- IT Disaster Recovery Plans (DRP)
- Questions
BCM Defined

…the development of *strategies*, *plans* and *actions* which provide protection or alternative modes of operation for those activities or business processes which, if they were to be interrupted, might otherwise bring about a seriously damaging or potentially fatal loss to the enterprise.

BCM = Crisis Management + Business Resumption Planning + IT Disaster Recovery Planning
**BCM - A Common Language**

- **Business Resumption Planning** – The process initiated to resume business operations to a level consistent with the business requirements.

- **IT Disaster Recovery Planning** – The recovery of information technology processes, systems, applications, databases, and network assets used to support critical business processes.

- **Crisis Management** – A series of actions taken to gain control of the event quickly to minimize the affects of an interruption and prepare for recovery.
The Business Continuity Lifecycle

1. Business Alignment
2. Risk Assessment & Business Impact Analysis
3. Compliance Monitoring & Auditing
4. Executive Management Support & Sponsorship
5. Plan Development & Strategy Implementation
7. Testing & Maintenance
8. Training & Awareness
10. Support & Sponsorship
BCM Regulatory Requirements

- NFPA 1600
- HIPAA
- GLBA
- FFIEC
- OSHA
- FCPA
- SEC
- ISO 9000 & 14000
- QS 9000
- State Insurance Departments
- Critical Infrastructure Protection
  - Security Standards for Electric Market Participants
  - Sound Practices to Strengthen the Resilience of the US Financial System

Primary Reasons Organizations Have a BCP (2002)

- Regulatory Compliance: 28%
- Stakeholder Protection: 33%
- Past Business Interruption: 27%
- Corporate Image: 6%
- Other: 6%

Past Business Interruption: 27%
Stakeholder Protection: 33%
Regulatory Compliance: 28%
Corporate Image: 6%
Other: 6%
Holistic planning begins at the business process level (highlighted) with IT disaster recovery planning and technical architecture adapting to business recovery requirements.
Threat and Risk Assessment

- Environmental Risks

- Man-made Risks (Accidental and Intentional)

- Business Process-related Risks
  - Single Points of Failure
  - Personnel
  - Supply Chain

- Information Technology Availability Risks
Business Impact Analysis Defined
The careful study of individual business process and support functions, as well as the system of business processes in their entirety, to better understand objectives regarding continuity of operations.

Methodologies and Approaches
• The “BCP Blue Print”
• The Business Case for Business Continuity Management
• Relationship between the BIA and Risk Assessment
• Objectives
  – Quantify the loss potential
  – Qualify other types of loss
  – Establish Recovery Time Objective
  – Establish Recovery Point Objective
A rigorous Business Impact Analysis (BIA), including an analysis of recovery options, helps address the gap between Business Requirements and IT Capabilities currently experienced by many organizations.
Recovery Strategies

Recover strategies are the high-level, cost-effective approaches, methodologies and decisions that will drive future planning efforts.

- Outsource versus insource
- Disparate versus coordinated efforts
- Facility strategies
- Key partners and their strategies
- Data centers (co-lo, hot, warm or cold sites)
- Cost-benefit analysis is key
- Alignment with company strategy
- Vendor strategies
- Interdependencies
Business Continuity Plans (BCP) are the detailed, documented recovery plans that give management and staff the blueprint to adjust to and continue to operate despite the impacts of a disruption. At a minimum, the BCP contains:

- Roles, responsibilities, rules and structures to document/approve the plan
- Emergency procedures to ensure safety of all affected staff members
- Response procedures to bring business to functional state
- Recovery procedures to bring business back to pre-incident state
- Coordination procedures with public authorities
- Communication procedures
- Critical information on continuity teams, staff, customers, suppliers, etc.
- Linkage to critical application programs, third-party services, operating systems, databases, data files, personnel and supplies and timeframes needed for recovery
- Off-site storage of critical back-up media, documentation and other pertinent resources
- Copies at various secure locations
Disaster Recovery Plans

The DRP includes all the technology processes, systems, applications, databases and network assets used to support the critical business processes. Disaster recovery testing reduces risk that an organization could incur given a severe disruption of business if the data center and system custodians are unable to recover processing or key technology infrastructure in the event of a disaster.

- Disaster/Contingency plans developed for each critical IT process which identifies:
  - Alternative equipment/facilities adequate to recover critical systems
  - Prioritization of recovering critical and non-critical applications
  - Personnel requirements/skills in the event of a disaster

- Annual or periodic testing requirements based on system risk assessments to ensure that recovery can be accomplished accurately and timely

- Post-test analysis

DR plans must be tested to ensure documented procedures and systems are recoverable during a disaster or risk extended business interruption or the inability to recover at all.
Testing and Maintaining the Plans

The BCPs and DRPs must be periodically tested to ensure the plans are comprehensive enough and practical to ensure the continuity of critical business and IT processes.

- Tabletop Tests
- Fully Functional Tests
- Component Tests
- Practical Scenarios

Plans must also be regularly updated and maintained to reflect current operating procedures, processes, IT infrastructure and systems, as well as changes to the environment.
## Characteristics of Capability

<table>
<thead>
<tr>
<th>Process Maturity</th>
<th>Optimizing</th>
<th>Managed</th>
<th>Defined</th>
<th>Repeatable</th>
<th>Ad Hoc</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Business continuity management</strong></td>
<td>Business continuity management is a competitive advantage. Management “advertises” the existence of the business continuity process internally and externally with customers. Continuity-related service level agreements, associated with uptime, performance and continuity, are utilized to drive efficiencies internally and build strategic relationships with customers.</td>
<td>Comprehensive, organization-wide business continuity strategies are aligned with strategic objectives and customer expectations. BCM operates as a core business function, chartered with clear accountability and responsibility. Regular BCP testing and maintenance occurs. Personnel are well trained regarding their roles and responsibilities. Metrics are collected and managed to ensure continuity-related service level agreements are met.</td>
<td>Business functions and IT assets supporting the delivery of products and services, as well as customer service, are protected from long-term business interruptions. Customer expectations regarding product and service delivery have been taken into account. Testing and training limitations may result in isolated recovery issues, often taking the form of recovery capacity constraints and missed recovery objectives.</td>
<td>Management relies on untested or under-tested continuity-related processes to manage the effects of business interruptions. IT asset recovery is often the most mature aspect of the continuity process, although some organizations emphasize either crisis management or business resumption planning. Employees have limited knowledge regarding their roles during recovery, potentially impacting the likelihood of a successful response effort.</td>
<td>Significant risk of continuity-related impacts are present. Business interruptions, ranging from isolated infrastructure failures through regional events, have the potential to cause serious financial harm and/or reputational impairment. The organization relies on “force majeure” clauses to minimize contractual violations.</td>
</tr>
</tbody>
</table>

## Method of Achievement

<table>
<thead>
<tr>
<th>Process Maturity</th>
<th>Optimizing</th>
<th>Managed</th>
<th>Defined</th>
<th>Repeatable</th>
<th>Ad Hoc</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Business continuity management</strong></td>
<td>Business continuity management is a competitive advantage. Management “advertises” the existence of the business continuity process internally and externally with customers. Continuity-related service level agreements, associated with uptime, performance and continuity, are utilized to drive efficiencies internally and build strategic relationships with customers.</td>
<td>Comprehensive, organization-wide business continuity strategies are aligned with strategic objectives and customer expectations. BCM operates as a core business function, chartered with clear accountability and responsibility. Regular BCP testing and maintenance occurs. Personnel are well trained regarding their roles and responsibilities. Metrics are collected and managed to ensure continuity-related service level agreements are met.</td>
<td>Business functions and IT assets supporting the delivery of products and services, as well as customer service, are protected from long-term business interruptions. Customer expectations regarding product and service delivery have been taken into account. Testing and training limitations may result in isolated recovery issues, often taking the form of recovery capacity constraints and missed recovery objectives.</td>
<td>Management relies on untested or under-tested continuity-related processes to manage the effects of business interruptions. IT asset recovery is often the most mature aspect of the continuity process, although some organizations emphasize either crisis management or business resumption planning. Employees have limited knowledge regarding their roles during recovery, potentially impacting the likelihood of a successful response effort.</td>
<td>Significant risk of continuity-related impacts are present. Business interruptions, ranging from isolated infrastructure failures through regional events, have the potential to cause serious financial harm and/or reputational impairment. The organization relies on “force majeure” clauses to minimize contractual violations.</td>
</tr>
</tbody>
</table>

---

### Managed

In addition to a customer focus and the desire to minimize financial loss and reputation impairment, management addresses regulatory compliance through the design of solutions with characteristics mandated by industry and governmental organizations. Specific compliance categories include data protection, financial reporting process continuity, strategy testing and plan maintenance processes.

### Defined

Business functions and IT assets supporting the delivery of products and services, as well as customer service, are protected from long-term business interruptions. Customer expectations regarding product and service delivery have been taken into account. Testing and training limitations may result in isolated recovery issues, often taking the form of recovery capacity constraints and missed recovery objectives.

### Repeatable

Management relies on untested or under-tested continuity-related processes to manage the effects of business interruptions. IT asset recovery is often the most mature aspect of the continuity process, although some organizations emphasize either crisis management or business resumption planning. Employees have limited knowledge regarding their roles during recovery, potentially impacting the likelihood of a successful response effort.

### Ad Hoc

Significant risk of continuity-related impacts are present. Business interruptions, ranging from isolated infrastructure failures through regional events, have the potential to cause serious financial harm and/or reputational impairment. The organization relies on “force majeure” clauses to minimize contractual violations.

---

### Process Maturity

- **Process Maturity**
- **Optimizing**
- **Managed**
- **Defined**
- **Repeatable**
- **Ad Hoc**

---

### Charateristics of Capability

- **Business continuity management**
- **Method of Achievement**

---

### Method of Achievement

- **Business continuity strategies**
- **Process Maturity**
- **Optimizing**
- **Managed**
- **Defined**
- **Repeatable**
- **Ad Hoc**

---

### Managed

Business continuity strategies address core business functions, information technology assets and supply chain relationships. Management fully supports this effort. The organization’s business continuity management process, to include crisis management, crisis communications, business resumption planning and IT disaster recovery planning, operates as a single function. The BCM process reflects the current business and technology environment.

### Defined

A formal business continuity strategy has been designed and deployed. A risk assessment has been performed to identify and assess continuity risks. A business impact analysis (BIA) has been performed, but there are no processes to keep it current. Testing is infrequent or fails to address all aspects of the continuity process. Plan maintenance activities have not occurred in over twelve months. Metrics for key BCP tasks require refinement.

### Repeatable

The organization’s business continuity strategy addresses crisis management, business resumption or IT disaster recovery. Continuity processes are designed and developed separately and lack integration. A high-level risk assessment and/or business impact analysis has been performed. Although some continuity-related processes exist, plan maintenance and testing procedures have not been implemented.

### Ad Hoc

BCP goals and expectations were derived without a risk assessment or business impact analysis. Business continuity strategies are characterized as ad hoc; a formal documented plan does not exist. Business continuity accountability and responsibility remain unassigned. Business continuity testing and training and awareness processes have not been designed. The organization lacks confidence in its ability to survive following a business interruption.
Reporting Relationships

- Finance
  - CFO/Direct Report to CFO
  - Risk Management / Loss Prevention
- Executive Council
  - Legal
  - Human Resources
  - Corporate Communications
- Operations
  - Direct Report to the COO
  - EHS
  - Security
- Information Technology
- Internal Audit
Internal Audit Can Add Value

- Keeping Management Informed on Progress Toward BCM Development and Implementation
- The Internal Sales Person – Making the Case for Business Continuity
  - Participation in the Risk Assessment and Business Impact Analysis
- Defining Key Business Functions By Assisting with the BIA
- Defining Key Controls and Guide Toward a Process, not a Plan
- Project Management Standards
- Help Craft Maturity Levels and Definitions
- Audit the BCP Process – Initially and in the Future
Help Center: Business Continuity Plan Summary

Purpose
In accordance with mandated regulations from the Office of Thrift Supervision (OTS), the Securities and Exchange Commission (SEC), the New York Stock Exchange (NYSE), and the National Association of Securities Dealers (NASD), E*TRADE Financial Corp. would like to make you aware of our Business Continuity Plan (BCP).

Our program is designed to help ensure that we can continue to do business with little or no disruption, that your assets will be secure and accessible, and that you will be able to transact regardless of the unplanned business interruption or scope of the situation.

Recovery Strategies & Plans
E*TRADE Financial's BCP addresses the recovery of technology systems. In general, our technology systems are located in multiple sites that are at least 100 miles apart. This design ensures that if one of our locations suffers a downtime in service, systems at an alternate location can be used to continue to provide service.

Should there be an event that prevents E*TRADE Financial from having access to a building, because of a disaster to the building, a business district, city, or even the region, we can rely on the systems in the other location(s) to allow us and our customers to continue to conduct business with little or no disruption within a few minutes.

E*TRADE Financial's BCP also contemplates recovery contingency plans and teams. These plans are designed to address various scenarios including incidents at a specific business location, another E*TRADE Financial location, as well as when a technology or other service provider stops working for some reason. Whenever the event, our plans are designed to enable us to be back in operation within 24 hours or less.

Recovery teams are in place to address the immediate response to an incident, the management of the situation from the time the incident occurs until the matter is resolved. Each member is assigned specific responsibilities within each plan role.

In an event our BCP, you do assume that the locations we have identified as 'pre-designated alternative sites' are available, that we have sufficient personnel, and that external organizations, such as government agencies and market systems, are operational. If any of these assumptions are not met, our business could be disrupted until matters are resolved.

Nevertheless, there can be no assurance that service will continue without interruption in certain circumstances, such as a regional blackout, a natural disaster or a terrorist attack. However, in the event that E*TRADE Financial has determined that it cannot resume operations within a reasonable amount of time, E*TRADE Financial will provide as much advance notice as possible regarding its operations.

Preparation:
Although E*TRADE Financial is committed to have access to your accounts in the event of a significant business disruption, it is possible that there may be some temporary disruption or change in the manner in which you can access your account. E*TRADE Financial will notify customers of any such changes or disruptions by posting a notice on the firm's Web site or through a message on its telephone system.

Talent prepare for such contingencies, we suggest that you become familiar with the various means through which you can access your account and share these means, including:

- Online at e-trade.com
- By telephone, 1-800-678-1234 (1-800-678-1234)
- A local E*TRADE Financial office that you can access or call (for details contact your E*TRADE Financial branch).
Summary Points for a Smooth Process

• Dedicate resources to stay on top of recovery planning
• Follow a holistic project approach
• Utilize tools to execute the project
• Execute a Risk Assessment and Business Impact Analysis
• Research and develop business and IT recovery strategies
• Develop and formalize crisis management, crisis communication, IT disaster recovery and business recovery plans
• Provide a framework and methodology for understanding, discussing and developing plans
• Institute training and awareness
• Conduct post-test analysis and make adjustments accordingly
• Implement a maintenance strategy
Questions??
Patrick Potter  
Vice President  
Business Development and Service Delivery  
MHA Consulting  
potter@mha-it.com  
623.521.3900 (mobile)  
www.mha-it.com