


WOLF
& COMPANY, P.C.
*Certified Public Accountants
and Business Consultants*
Insight and Integrity

Business Continuity Plan
Audit Overview

ISACA, Hudson Valley Chapter
September 17, 2009


Boston • Springfield • Albany



WOLF
& COMPANY, P.C.
Certified Public Accountants
and Business Consultants
Insight and Integrity

Wolf & Company, P.C.

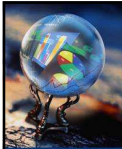
- Regional CPA firm founded in 1911 with ≈165 professionals
- Corporate offices in Boston & Springfield Massachusetts, and Albany, New York
- 40 professionals providing Risk Management Services
- Provide IT Assurance and Advisory services to over 200 organizations annually



WOLF
& COMPANY, P.C.
Certified Public Accountants
and Business Consultants
Insight and Integrity

L. Randy Marsicano, CISA

- IT Audit Manager
- Certified Information Systems Auditor
- Over eighteen years of information security experience
- Experience in Commercial and Financial Industries
- Frequent Speaker on Risk Management



Why do we need to worry about Business Continuity?

More than one in four businesses will experience a significant crisis in a given year. Of those businesses that experience a disaster and have no emergency plan, 43 percent never reopen. Of those that do reopen, only 29 percent are still operating two years later.

- Association of Small Business Development Centers



Insight and Integrity



Why do we need to worry about Business Continuity?

A national survey of small businesses found that while 94 percent of small business owners believe there is a potential for a disaster to seriously disrupt their business within the next two years, only 43% feel prepared for a one week disruption of their business, and 22% feel prepared for a one month disruption.

- American Red Cross and FedEx Corp.



Insight and Integrity

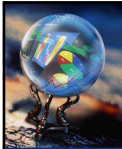


Overall Objective of the Audit

Determine the quality and effectiveness of the organization's business continuity planning process, and determine whether the continuity testing program is sufficient to demonstrate the organization's ability to meet its continuity objectives.



Insight and Integrity



Insight and Integrity

Individual Audit Objectives

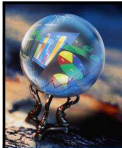
1. Examination scope and objectives
2. Quality of oversight
3. Adequacy of BIA and RA
4. Risk management
5. Enterprise wide
6. Hardware backup and recovery
7. Security procedures
8. Pandemic planning
9. Outsourced activities
10. Monitoring and testing



Insight and Integrity

Determine examination scope and objectives

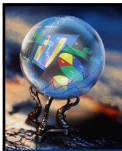
- Review prior examinations and reports*
- Review management responses*
- Identify key organizational changes
- Determine management's consideration of newly identified threats
- Establish the scope of the examination by focusing on those factors that present the greatest degree of risk to the organization or service provider



Insight and Integrity

Determine quality of oversight

- Determine if the Board established an on-going, process-oriented approach to business continuity planning
- Verify senior level management has been assigned responsibility
- Verify all relevant groups have been involved
- Ensure the DRP is enterprise wide
- Verify the annual review and approval
- Verify timely revision of the plan

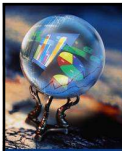


Determine adequacy of BIA and RA

- Verify all departments are included*
- Review prioritization of business functions*
- Determine whether the BIA identifies maximum allowable downtime*
- Verify the risk assessment includes disruptions from service providers*
- Verify that other business risks that are relevant to the organization are considered*



Insight and Integrity



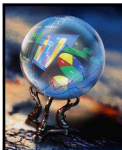
Disaster Recovery – Institution Name

Business Impact Analysis Report

Business Process	Non-Technology Vendors	Dependent Technologies	Priority Level:			
			Level 1 – Critical Recovery Time Objective: (w/in 24 hours, 1 business day)	Level 2 – Very Important (w/in 48 hours, 2 business days)	Level 3 – Less Essential (w/in 72 – 86 hours, 3-4 business days)	Level 4 – Best Effort
Branch Operations						
1. Account Opening	Disks	<ul style="list-style-type: none"> Windows 2003 Core Banking System 	High			
2. Account Maintenance	None	<ul style="list-style-type: none"> Windows 2003 Core Banking System 		Moderate		
3. Processing instant issue ATM cards	None	<ul style="list-style-type: none"> FIN Express Windows 2003 Core Banking System 			Low	



Insight and Integrity



Risk Management

- Review risk mitigation strategies*
- Ensure Geographic diversity*
- Verify appropriate policies, standards, and processes
- Verify appropriate training
- Determine whether interdependent components are included
- Verify appropriate maintenance and distribution of BCP
- Evaluate audit involvement*



Insight and Integrity



Insight and Integrity

Enterprise wide

Review and verify that the written BCP:

- Addresses the recovery of the entire business
- Addresses the recovery of vendors and outsourcing arrangements*
- Includes People, Process, and Technology
- Includes emergency preparedness and crisis management



Insight and Integrity

Hardware backup and recovery

- Verify contracts for alternative processing (if outsourcing)
- Verify capability of in-house recovery systems
- Verify capability of outsourced recovery systems
- Ensure synchronization of production and backup facilities



Insight and Integrity

Security procedures

- Physical security and access controls
- Intrusion detection and incident response
- Temporary access
- Authentication and authorization credentials



Insight and Integrity

Pandemic planning*

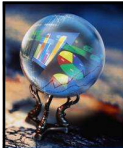
- Board oversight
- Assignment of responsibility
- Inclusion of:
 - Prevention
 - Strategy
 - Framework
 - Testing
 - Reviews and updates
- Incorporation into the BIA and BCP
- Monitoring of alert systems



Insight and Integrity

Pandemic planning* (continued)


- Internal and external communication
- Impact on functions provided by external parties
- Impact of significant staff unavailability
- Modifications to normal compensation and absenteeism
- Remote access requirements
- Appropriate testing



Insight and Integrity

Outsourced activities

- Communications
- Access
- Coordination
- Testing
- Adequacy of vendor BCP




Monitoring and testing

- Testing policy
- Testing strategy
- Execution, evaluation, and re-testing

WOLF & COMPANY, P.C.
Certified Public Accountants
 and Business Consultants

Insight and Integrity



Testing policy

- Sets expectations
- Identifies key roles and responsibilities
- Testing cycle with increasing levels of scope and complexity

WOLF & COMPANY, P.C.
Certified Public Accountants
 and Business Consultants

Insight and Integrity



Testing strategy

- Documentation
- Assumptions
- Requirements for enterprise wide and third party testing
- Frequency of testing
- Crisis management

WOLF & COMPANY, P.C.
Certified Public Accountants
 and Business Consultants

Insight and Integrity



Execution, evaluation, and re-testing

- Appropriate depth of testing*
- Compare results to objectives
- Independent observation
- Appropriate levels of re-testing



Insight and Integrity



Thank You / Questions

Randy Marsicano
Voice: 518-454-0880
Email: rmarsicano@wolfandco.com



Insight and Integrity
