The Best Offense

Presented by:
Kimberly Hirsch
MBCP, MBCI, ISO22301 Lead Auditor
Fusion Risk Management
Agenda

• Welcome and Introduction
• Governance and Compliance
• Liability Issues
• BC Standards Requirements
• Policy
• Your Organization’s Requirements
• Vendors
• Exercise and After Action Documentation
• Suggested Approaches
• Q & A
AUDIENCE PROFILE
Liability Issues

Impacts from records non-availability could result in:

1. Regulatory Violations
2. Fines
3. Legal Actions
4. Damage to Brand/Organizational Reputation
5. Additional Operating Expenses
6. Operational inefficiencies
ISO 22301

4.2.2 Legal and regulatory requirements must be understood

4.3.2 Scope of the BCMS

5.3 Policy
BC Standards Requirements

NFPA 1600

4.4.1 Program Administration

4.5.2 Laws and Authorities

4.7 Records Management
BC Standards Requirements

ASIS

ASIS is an organization for security professionals world-wide.

www.asisonline.org
An Organization is a Puzzle

Information Management is how we tell the story of how we are all connected and dependent on each other to execute and ensure the success of the institutional strategy/mission.
Successful programs drive engagement and deliver outcomes based on a solid Information framework that enables and empowers BCM to be in Command & Control at every stage.
Policy

- Define key terms
- Scope and boundaries for the program
- Identify chain of command
- What a business continuity incident is… and isn’t
- Standards references
- Funding
- Other related policies
- Participation requirements
- Exercise testing and maintenance
Impact Assessments

• Business Impact Assessment (BIA)
  • Process, Function, Department, Functional Area

• System/Technology Impact Assessment (SIA/TIA)
  • Application, IT System, IT Service

• Facility/Site Impact Assessment

• Vendor Risk Assessment
  • Vendor/Third-Party/Supply Chain
Vendor Documentation

You can’t outsource risk.
Vendor Risk Analysis

**OBJECTIVE**

Control BCM risks associated with vendors used in performing business processes

1. **Vendor Criticality**
   - Vendors
   - Criticality Factors
   - Critical vendors
   - Important vendors
   - Deferrable vendors

2. **Vendor Resiliency Risk**
   - Vendor BCM Risk Analysis
   - Plans/Procedures to mitigate risks
   - Vendor requirements gaps - (KPIs / KRIs)

Tweet along: #Sec360 www.Secure360.org
### Exercise Documentation

<table>
<thead>
<tr>
<th>Required Application: Application Name</th>
<th>Business Function Name</th>
<th>How is this Application Used</th>
<th>Recovery Time</th>
<th>Recovery Point Objective</th>
<th>Recovery Gap</th>
<th>Application RTO</th>
<th>RTO Gap</th>
<th>Manual Processes / Workarounds</th>
</tr>
</thead>
<tbody>
<tr>
<td>Works Service Center</td>
<td>Research historical data</td>
<td>Greater than 48 hours</td>
<td></td>
<td>2</td>
<td>0</td>
<td>Defer until restored. Could use backup CDs (1 for every pay group) that is in storage.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Citrix (6 records)</td>
<td>Financial Data Warehouse sits behind Citrix. Users must access</td>
<td>24 hours</td>
<td>Up to 24 hours</td>
<td>999</td>
<td>975</td>
<td>Access directly through VPN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ecommerce (1 record)</td>
<td>Accounting and Financial Reporting</td>
<td>Accept credit card payments and obtain charge-back information</td>
<td>30 hours</td>
<td>Up to 24 hours</td>
<td>999</td>
<td>951</td>
<td>purchase manual swipe machine</td>
<td></td>
</tr>
<tr>
<td>DataExchange (4 records)</td>
<td>Business Systems and Services (Formerly Financial Systems Team)</td>
<td>Connection between Oracle R12 and external systems for upload/download file transfers (intermediary service that eliminates direct access to Oracle database). Systems include: Harris/Ecom, SCS, SEI, SIS, ICS, HRS, UL, LDAP, DC3IT, MAXIMO.</td>
<td>24 hours</td>
<td>Up to 24 hours</td>
<td>5</td>
<td>0</td>
<td>No workaround identified.</td>
<td></td>
</tr>
<tr>
<td>Ecommerce (1 record)</td>
<td>Accounting and Financial Reporting</td>
<td>Accept credit card payments and obtain charge-back information</td>
<td>30 hours</td>
<td>Up to 24 hours</td>
<td>999</td>
<td>951</td>
<td>purchase manual swipe machine</td>
<td></td>
</tr>
<tr>
<td>Ecommerce (1 record)</td>
<td>Accounting and Financial Reporting</td>
<td>Accept credit card payments and obtain charge-back information</td>
<td>30 hours</td>
<td>Up to 24 hours</td>
<td>999</td>
<td>951</td>
<td>purchase manual swipe machine</td>
<td></td>
</tr>
</tbody>
</table>
Exercise Documentation

- List of participants
- Description of the exercise scenario
- Event summary
- What went well
- Needs improvement
- Remediation plan
- Update it as you close items
Activation After-Action
Why Perform a Vital Records Impact Assessment?

- To determine the resilience and recovery requirements (IT, Facilities, Suppliers) to support records availability
- To identify the most critical IT (Systems and Applications) and determine recovery priorities
- To support the business case for investments in IT resiliency
- To identify the most critical Facilities
- To identify the most critical Suppliers/Vendors

- To identify the most critical records to the organization
- To quantify, measure and report on the availability of records
- To determine appropriate strategies for the availability of records
- To prioritize efforts for improving records availability
- To quantify, measure and report on the availability of records
- To determine appropriate strategies for the availability of records
- To prioritize efforts for improving records availability
Begin With the End In Mind

What questions are you trying to answer?
What Decisions are you driving?
What Actions must be taken?

Criticalities
Exposures
Frequencies
Preparedness
Impacts
Dependencies
Least Resilient
Priorities
Quality
Gaps
Build an Information Foundation

Questions need answers!

1. What are the critical functions and why?
2. On what assets do our operations depend?
3. What are our most critical assets and why?
4. How are our operations interdependent?
5. How would operations be impacted by various threats?
6. What would upstream and downstream effects be?
7. How do peak processing periods change the picture?
8. How would a disruption impact...
   a) Employee or client well being?
   b) Ability to provide services?
   c) Ability to provide product?
   d) Perception of the brand?
9. What options and alternatives do we have?
10. What outage durations could be expected from various events?
11. What resources and assets can we leverage to minimize impact?

Answers drive buy-in!

1. Understanding the inner-workings of our operations.
2. Visibility to operational risks AND areas for improvement.
3. Set expectations for potential disruptions.
4. Filled information gaps and clarified misinformation.
5. Improved communication and raised credibility of BC Team.
6. Raised the level of dialogue and quality of decision-making.
The Payoff: Program Success!

You will build a network of advocates and champions.

You will establish command & control over your program.

We will have become part of the solution!
Making It Work For You

Minor Adjustments. Major Results.

• Make yourself invaluable
  • Build your information foundation.
  • Know more than anyone else.
  • Anticipate questions and frame the answers.

• Drive engagement. Drive Outcomes
  • Go deep. Go wide.
  • Prepare to act.
  • Prove it.
Questions & Answers