Introduction to Business Continuity Management

Audio

Presented by ABD's Occupational Health and Safety Team
Featuring The Cross Connection
JULY 24, 2018

Speaker Panel

ABD Insurance & Financial Services
Diana Blake
Senior Claims Consultant

ABD Insurance & Financial Services
Rod Sockolov
EVP & Founding Principal, P&C

The Cross Connection
Warren T. Cross
Principal

Today's Topics

- ✓ Introduction of Speakers
- ✓ An Introduction to Business Continuity Management
- ✓ The Cross Connection Commitment
- ✓ Why Business Continuity Matters
- ✓ Holistic Global Resiliency
- ✓ What does program rollout look like
- ✓ The importance of doing Business Impact Analysis
- ✓ Discuss framework of a sound Business Continuity Plan
- ✓ Wrap-up

Business Continuity Management (BCM)

What is BCM?

BCM is a form of risk management that deals with the threat of business activities or processes being interrupted by external and/or internal factors. It involves making arrangements to ensure you can respond as effectively as possible in the event of a disruption so mission-critical functions will continue to provide an acceptable level of service.

Effective business continuity can be best attained through the implementation of a business continuity management system (BCMS) aligned to its international standard, ISO 22301.

Insurance & Financial Services

Disaster Recovery (DR) Planning

Disaster recovery planning prioritizes fully recovering and returning to full functionality in the event of an incident, whereas BCM focuses on preserving an organization's ability to function. Having said that, there is still a clear overlap, and disaster recovery does fit within an organization's business continuity framework.

Disaster recovery plans are often relatively technical and focus on the recovery of specific operations, functions, sites, services or applications. The BCP might contain or refer to a number of disaster recovery plans.

ISO 27031 – ICT continuity best practice

ISO 27031 describes best practice for information and communications technology (ICT) continuity management within an organization's overall business continuity framework. ISO 27031 can be used in conjunction with ISO 22301, but can also be used on a standalone basis, should an organization wish to address ICT continuity management specifically.

Laws Influence BC and DR in Industries

Healthcare

- Health Insurance Portability and Accountability Act (HIPAA) of 1996
- Food and Drug Administration (FDA) Code of Federal Regulations (CFR) Title XX1, 1999

Government

- Federal Information Security Act (FISMA), 2002
- Title III of the E-Government Act, 2002
- Executive Order on Critical Infrastructure Protection in the Information Age, 2001
- COOP and Contingency of Government (COG) Federal Preparedness, 1999
- National Institute of Standards and Technology (NIST) Special Publication 800-34, 2002
- NIST 800-53 Recommended Security Controls for Federal Information Systems, 2005

Finance

- Federal Financial Institutions Examination Council (FFIEC) Handbook, 2003
- Basel II, Committee on Banking Supervision, Sound Practices for Management, 2003

Laws Influence BC and DR in Industries, continued…

Finance

- Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System, 2003

- Expedited Funds Availability (EFA) Act, 1989

Utilities

- Governmental Accounting Standards Board (GASB) Statement No. 34, June 1999

- North American Electric Reliability Council (NERC) 1200 (1216.1), 2003

- Federal Energy Regulatory Commission (FERC) RM01-12-00 (Appendix G), 2003

- RUS 7 CFR Part 1730, 2005

- Telecommunications Act of 1996, Section 256, Coordination for Interconnectivity

- NERC Security Guidelines for the Electricity Sector, June 2001

The Goal

1. **To not go down**
   - Build a solid foundation and put processes in place to reduce the risk of service interruption

2. **Get the services back up and operational using the quickest method**
   - Fix the issue in PROD
   - Failover to DR

3. **Imbed resiliency into the DNA of your organization**

Insurance & Financial Services

THE CROSS CORRECTION

Who needs Business Continuity?

- All industries

Our Mission

To enable organizations to proactively anticipate, prevent, withstand, respond to and recover from business disruptive events

Types of Disaster

2017 Statistics...

- **Companies without a plan fail** – 80% of companies without a business continuity plan will go out of business within 13 months.

- **Data Loss is inevitable** – 20% of all companies will suffer fire, theft, flood, storm damage, power failures, hardware or software disaster this year.

- **Disaster threats are increasing** – Companies are at increasing risk of natural disasters, competitive espionage, human error, and power grid failures.

- **Data is critical to your companies success** – Data loss can happen at any time and your business depends on this data. Protecting this data is key to your companies future success.

- **Hardware failure is the leading cause of unplanned outages** – 45% of all unplanned downtime is attributed to hardware failures.

- **Power outages account for 35% of unexpected downtime** – While this fluctuates each year, power outages and other utility losses will always pose a threat.

- **90% of businesses without a disaster recovery plan will fail after a disaster.**

- **1 in 3 businesses were unprepared for disaster, despite having a plan.**

- **Unplanned downtime costs between $926 to $18k per minute** – These costs include lost revenue, lost productivity, recovery expenses, equipment replacement, and more.

- **The takeaway** – It is not a question of if, but when. Companies need to be doing everything possible to avoid downtime and expedite recovery should disaster strike.

Global Resiliency

Workplace/facility recovery

Emergency response

Pandemic planning

Disaster recovery

Incident response

Crisis management planning

Business process recovery

Governance

Governance, Training, Assurance
Insuring compliance, setting policy, standards, procedures, metrics and reporting

Global Resiliency

Crisis Management

Event Response
Response to an event, or a series of escalating events, that threatens our strategic objectives, reputation or viability

Global Resiliency

Business Continuity

People and Processes
Sustain acceptable uptime, and restore business operations to the acceptable level after a disruptive event.

Global Resiliency

Disaster Recovery

Technology
Restore or recover critical infrastructure and applications following a data center or systems failure

Global Resiliency

abd Insurance & Financial Services

Organizations must think beyond BC and DR plans
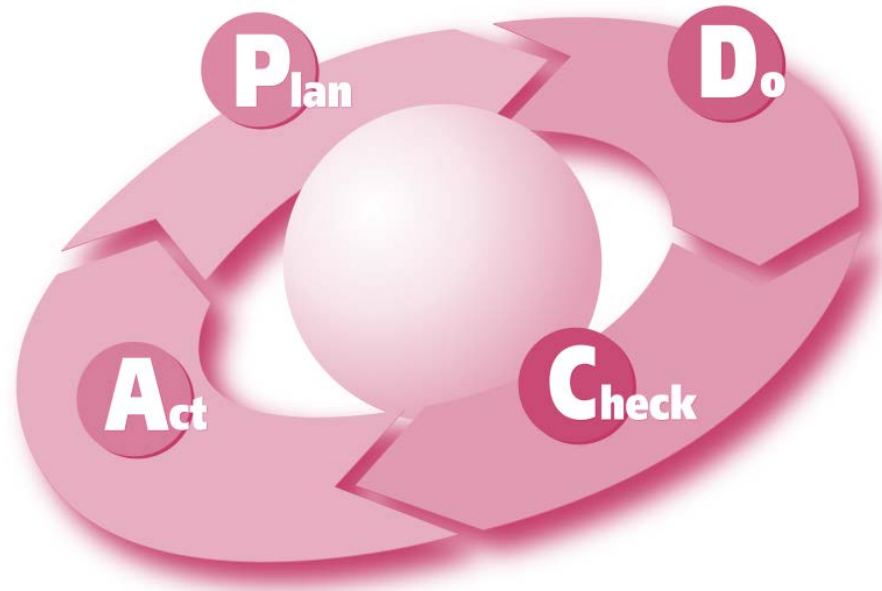
For the program to be effective we need to be:
- Strategic
- Holistic
- Sustainable

Business Continuity Management Lifecycle
Improving organizational resiliency

Business Continuity Management (BCM) is a holistic management process that:

1. Identifies potential threats to an organization and
2. The impacts to the business operations those threats might cause.
3. It provides a framework for building organizational resilience and effective response
4. Enables the business to stay on course whatever storms it is forced to weather

At the heart of BCM good practices sits the BCM lifecycle.

It shows the stages of activity that an organization moves through and repeats with the overall aim of improving organizational resilience.

Insurance & Financial Services

The Business Continuity Management (BCM) Lifecycle

Effective BCM "Best Practices" involves:

- Identifying critical activities;
- Performing a business impact analysis (BIA);
- Performing a risk assessment;
- Designing and implementing a business continuity plan (BCP);
- Testing and evaluating performance; and
- Putting a continual improvement process in place.

Phased Rollout of the Program
Initiative starting in the next 90 days

✓ Establish BCM Program within each organization

BC
Business Impact Analysis (BIA)

Crises Management
Establish EMT/CMT processes and protocols

DR
Technology Discovery

DR
Gap Analysis

DR
Begin documenting DR plans for critical systems

The Business impact Analysis

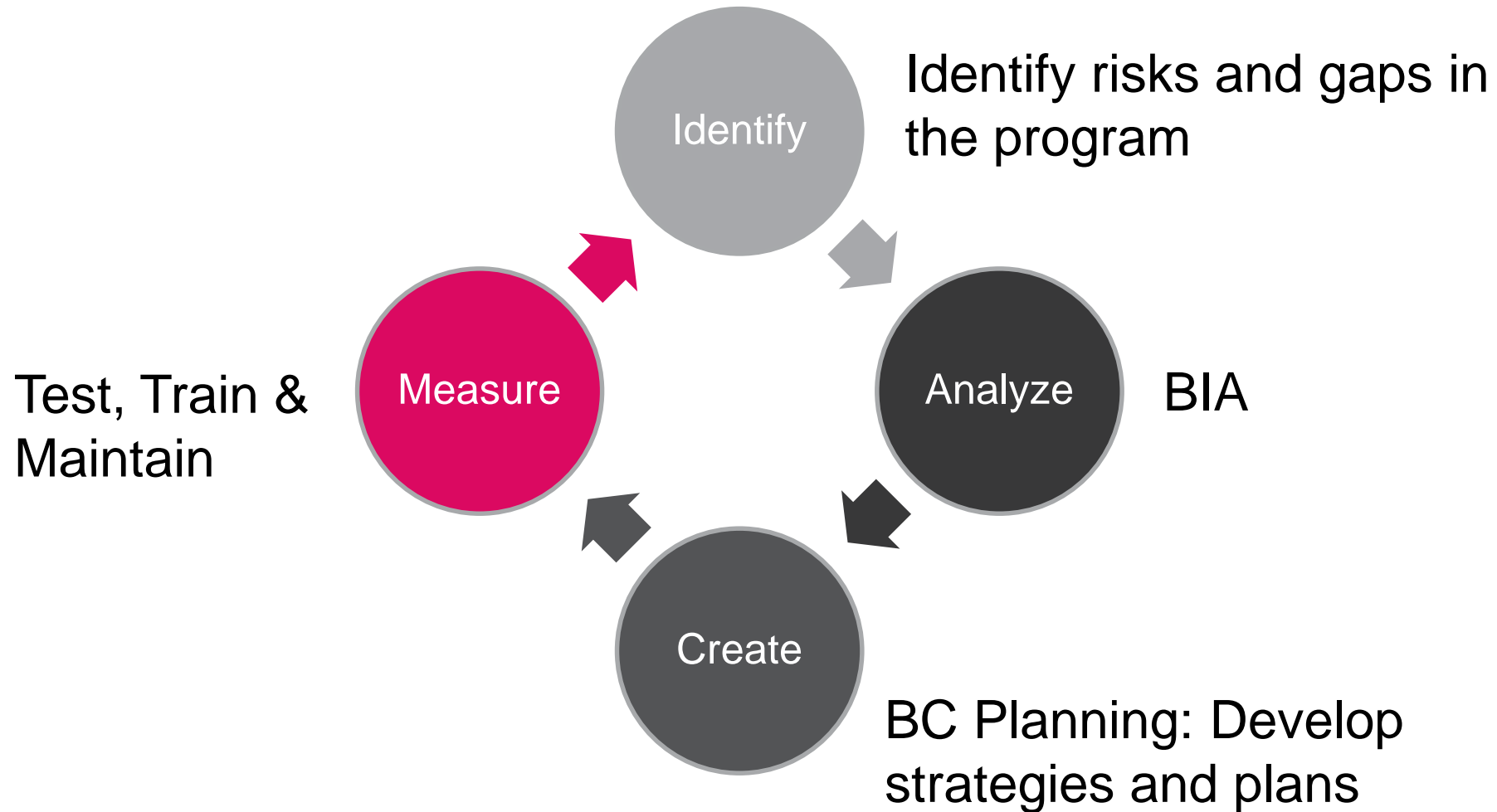The first initiative to engage your team

The Business Impact Analysis

A Business Impact Analysis (BIA) is a systematic process to determine and evaluate the potential effects of an interruption to business operations as a result of a disaster, accident or emergency.

Why conduct a BIA?

- Quantify the impact a business disruption will have on your departments ability to function over time
- Enable informed prioritization of department recovery in the event of a disruption
- Justify (or negate) the current or future time and expense invested in recovery strategies
- Identify critical dependencies (departments, vendors, applications, etc.)
- Explicit direction from Executive Leadership Team

The BIA in the Big Picture

Identify — Identify risks and gaps in the program

Analyze — BIA

Create — BC Planning: Develop strategies and plans

Measure — Test, Train & Maintain

BIA Steps:

Working through the Business Continuity Manager or Assigned Point Person:

- Meet with all department leaders for a BIA overview

- Schedule individual BIA interviews with department leader and SMEs

- Perform analysis on results of department sessions

- Provide each department manager with results for their review and approval

- Create holistic consolidated Treasury report for review and approval by Treasury's executive management

Some Key Components of a Business Continuity Plan:

- Plan revision and control tracker
- Plan purpose and plan scope
- Recovery Teams
- Team Member Responsibilities
- Instructions for using the Business Continuity Plan
- Emergency Management Standards
- Emergency Management Procedures
- Business Impact Analysis (BIA)
- System Recovery Strategy
- Business Continuity Procedure

Some Key Deliverables of a BCMP:

Business Continuity Plan (BCP)
- Business Recovery Procedures
- Business Resumption Procedures

Operational Recovery Plan (ORP)
- Contingency Planning Procedures
- Crisis Management Procedures
- Emergency Response Procedures
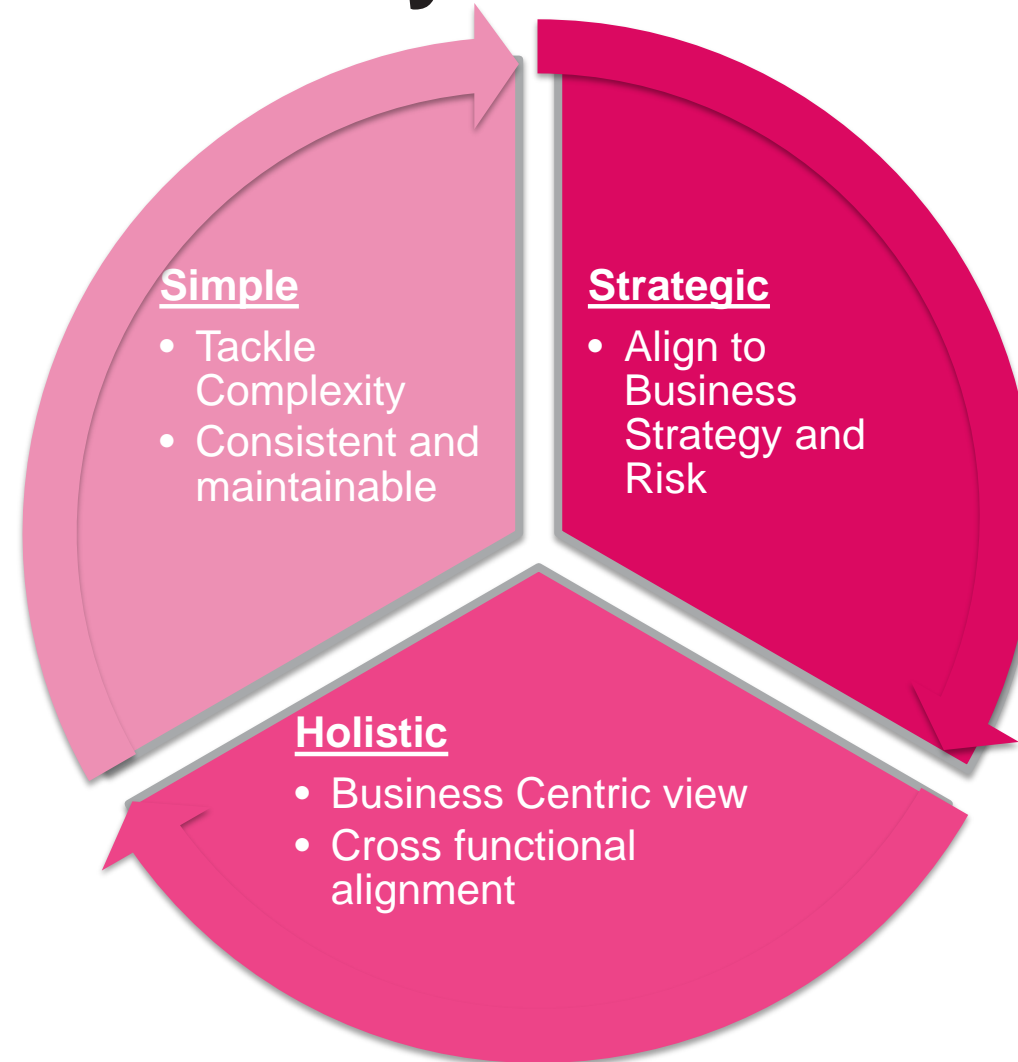- Emergency Operation Center Procedures

Disaster Recovery Plan (DRP)
- Resource Requirements
- Disaster Recovery Process Document

Remember, It's a Journey

As with any program, continuous improvements are needed to ensure a program is effective and is aligned with the business needs, priorities, as well as ingrained into the business culture

Simple
- Tackle Complexity
- Consistent and maintainable

Strategic
- Align to Business Strategy and Risk

Holistic
- Business Centric view
- Cross functional alignment

Focusing on these 3 key program principles will help drive us to the next level

What We Do

- The Cross Connection is a private minority business enterprise (MBE) offering:
- **Business Continuity (BC) and Disaster Recovery (DR) Services**
- Disaster Tolerance (DT) Services
- Program and Project Management Services (IT, regulatory compliance and government regulations; Basel II, FISMA, GLBA, HIPAA, NIST, ISO, SOX)
- Mergers and Acquisition (M&A) Services (conducting IT Due Diligence and Integration Implementation Strategies)
- Technical Account Management (TAM) Services
- IT Assessment Services (hardware, software, network, technology support, etc.)
- Operational Readiness (Enterprise Communication, Enterprise Training, and Enterprise Cultural Transformation)

THE CROSS CONNECTION

info@tcc-svcs.com
www.TheCrossConnections.com
916.730.6758

Let's wrap-up

Discussion Recap

- **Business Continuity Management responds to disruptions and ensures mission-critical functions continue**

- **Companies without a plan will fail**

- **Insurance coverages and program strategies will vary based on the exposures**

The takeaway – you can create a program to help avoid downtime and expedite recovery should disaster strike!

Thank You!

abd Insurance & Financial Services