THE INSTITUTE OF INTERNATIONAL AUDITORS
IIA INTERNATIONAL CONFERENCE
DUBAI, UAE / 6-9 MAY 2018

Auditing the Corporate Business Continuity Plan

Seth Davis, CIA, CFSA, CPA, CISA, CISSP, CFA, CPCU

Background

RLI Insurance

- About 1000 employees, half in branch offices
- Hybrid IT Infrastructure
  - On-premises data center and cloud-hosted solutions
- Warm recovery site
- 72 hour recovery time objective
- Our role:
  - Auditors by day, BCP Coordinators by night

Key Areas

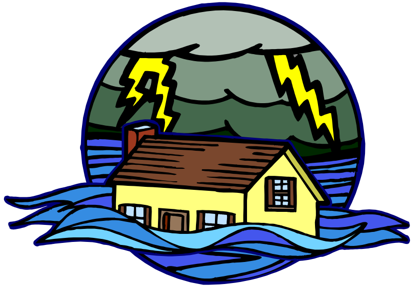
- BCP governance and corporate plan coordination
- BIA’s and Alternative Procedures for business units
- RTO / RPO
- Importance of regular plan review
- Internal and external communications
- Alignment of business and IT
- Third-party considerations
- Testing

Why Audit?

- Determine if your company is prepared to address risks of a disaster or disruption
  - Not a matter of if but when
  - Help ensure company can minimize loss of business and damage to reputation when systems, facilities and/or people are unavailable
- Can org continue to meet the needs of stakeholders
  - Customers
  - Shareholders
  - Employees
  - Board/Management

What is BCP?

Business Continuity Planning (BCP) is the preparation and testing of measures that protect business operations and also provide the means for the recovery of facilities, technology, equipment and people in the event of any loss, damage or disruption.



BCP Terms Defined

- **Disaster / Disruption**
  - Loss of facilities
  - Loss of infrastructure/technology/equipment
  - Unavailability of employees

- **Business Impact Analysis (BIA)** – Determination at business-unit level of what functions, information resources, and supporting applications are critical

- **Alternative Procedures** – Documents any workarounds necessary to continue operations from a recovery facility

- **Systems Continuity Plan (SCP)** – Outlines procedures necessary to restore technology and IT services in the event of a disruption

BCP Governance

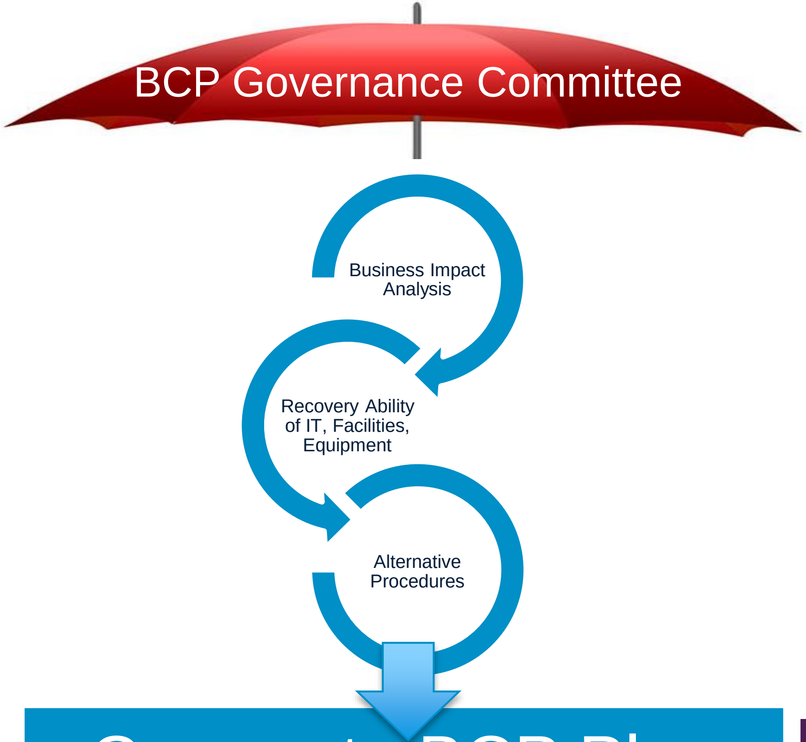
- Governance is key - Management must show support to properly prepare, maintain, and practice a BC plan by assigning adequate resources and people
- Is there a BCP Coordinator?
  - Insight into cross-department dependencies
  - Ideally someone in operations or administration rather than IT
  - Needs dedicated resource for constant maintenance
- Is there a BCP Governance Committee?
  - Cross-section of management
  - Prioritize and determine cost/benefit analysis
  - Avenue for escalation/support

BCP Governance

Is there an established BCP risk tolerance as part of ERM?

- For example, the organization would not want to be unavailable for more than X hours or XX days - Will likely flow from Business Impact Analysis
- Focus less on event and more on impact including number of days
  - Facility/equipment
  - People
  - Information

BCP Process Flow



BCP Governance Committee

Business Impact Analysis

Recovery Ability of IT, Facilities, Equipment

Alternative Procedures

Corporate BCP Plan

Two Audit Approaches

- Corporate view of BCP
  - Corporate Plan
  - Systems Continuity Plan
  - Governance/communication
  - Coordination across departments and with IT
  - Testing
- Business Unit / Department view of BCP
  - Business Impact Analysis (BIA) complete and current
  - Alternative procedures
  - Testing

Key Data From BIA

List processes performed by the department

- Frequency of processes
- Key inputs / outputs
- Assign a financial/compliance/reputational impact of being unavailable
  - Difficult but helpful to prioritize and allocate resources
  - Consider worst case scenario (e.g. quarter-end)

Key Data from BIA

Dependencies

- Systems
- Equipment
- Third party/vendor
- People – *Greatest challenge*
  - How many are trained to do process
  - Minimum that could perform process until fully recovered
  - How long to source/train others
  - Is there good process documentation?

Key Data From BIA

Recovery Point Objective (RPO)

- Indicates the maximum acceptable data loss. Based on backup frequency.

Recovery Time Objective (RTO)

- The maximum tolerable time to recover critical functions. Based on time needed to restore.

RPO **RTO**

RTOs / RPOs

- BCP Governance needs to determine if RTOs and RPOs can be met based on a cost/benefit analysis
  - Consider costs of downtime
  - Consider costs of reducing recovery time
- IF RTOs and RPOs are cost prohibitive, BCP Governance Committee needs to notify business units to develop alternative procedures/accept risk

Audit Considerations for BIA

- Are BIA’s reviewed and updated regularly?
- Do BIA’s reflect current dependencies?
- Do RTOs and RPOs meet needs of regulators and customers?
- Is there consistency with RTOs and RPOs across processes/departments

Alternative Procedures

- Does business unit have documented alternative procedures to continue operations in some form in the event their facility or systems are unavailable?
- Are there contracts with key vendors?
- Are key contacts (other departments, customers, etc.) accessible?
- Do alternative procedures address where employees go? Is there a contract with a facility?
  - Is it realistic to work from home?
  - Is there adequate risk separation between main facility and alternate recovery facility?
  - Can employees get there easily?

Audit Considerations for Alternative Procedures

- Risks for auditors to focus on:
  - Single location operations as these may present unique challenges
  - Paper dependencies/data stored locally which would not be available in a disaster
  - Interdependencies across departments
- Does plan address both short as well as long term disruptions
- Who can make day-to-day decisions?
  - Best if local with communication to BCP coordinator
- How will employees in affected facility be notified?
- Does alternative location have necessary systems/equipment/employee support?

Corporate BCP Plan

- Is the plan backed up and accessible?
- Are key teams established to coordinate efforts?
  - Emergency Response/Life Safety
  - Communications
  - Facilities
  - Systems Continuity Plan
    - Infrastructure & Application Recovery

Emergency Response Team

- Are emergency response procedures incorporated?
  - Do employees know where to go in an event?
  - Is regular training performed?
  - Is there a process to account for employees?
- How will plan take care of employees?
  - Plans quickly fall apart if key employees are unavailable
  - Can employees/family be housed in order to continue to work?
  - Can payroll be run?
  - Should there be a process to provide employees with cash advances, credit cards, increased limits?
- Does plan consider risk separation?
  - Analyze location of key employees and facilities: How many key employees could be personally affected by an event that affects facility?

Facilities Team

Multiple Tasks

- Pre-disaster
  - Ensure on-going facilities are disaster resistant
- Post-disaster
  - Ensure availability of alternative locations
  - Begin building replacement facility

Facilities Resiliency

- Withstand/minimize local perils – fire, hurricane, tornado, flood
- Power
  - Generator and uninterrupted power supply (UPS)
    - Enough fuel/regularly tested
- Telecommunications Continuity
  - Plan for all communications including data, voice, fax, WANs
  - Typically highly dependent on vendors
  - Redundancy of lines and providers
  - “last mile” protection should be considerations

Recovery Site Options

- **Hot Site** – equipped with exact configuration required to recover critical applications. May have production data replicated in real-time.
- **Warm Site** – equipped with some computing equipment but less capable than normal production environment. Applications need to be recovered before use.
- **Cold Site** – facility with space and basic infrastructure but lacking any IT or communications equipment
- **Mobile Site** – packaged, modular processing facilities mounted on transportable vehicles to be delivered.
- **Reciprocal Agreements** – agreements between separate, but similar companies to temporarily share IT facilities

Communication

- Subset of Crisis Communication
- Utilize alert system
- Regularly communicate the plan
  - Corporate plan
  - Business unit plans
  - Obtain acknowledgement of receipt, understanding and dissemination

Systems Continuity Plan

- Is there consistency with RTOs between business units and IT
  - Recovery timeline should be based on input from business units’ BIAs
  - High-risk, high-impact applications should be prioritized
  - Are inconsistencies communicated and alternative procedures developed or greater IT resources allocated by BCP Governance?
- How dependent are recovery processes on primary experts?
  - What if they are not available?
  - Mix up who performs recovery tests with alternate staff
- Does IT alternative site have the capacity during a disaster?
  - Hot/warm/cold

Audit Considerations for Systems Continuity

- Does timing of backups match business unit’s requested RPO?
- Common Back-up methods
  - Tape Backup - Data is written to tapes that are stored in secure onsite and offsite locations
    - Are backup tapes periodically tested by a restore to ensure integrity of the tape?
    - Are tapes encrypted? Tapes maintained in a secure area?
    - Is there risk separation between offsite tape storage and main facility?
  - Data Mirroring - Data is written to multiple disks simultaneously for redundancy

Testing is Key

- What testing is done and how are results communicated and action items tracked?
- Plans should be tested regularly –
  - Partner with business to create plans based on BIA
  - Log, track, and resolve exceptions
  - Involve business in IT Testing

Have employees work from alternative locations

  - Bring nothing with them as office/systems unavailable

Testing is Key

- Determine testing maturity – *Key is to do some testing regularly (annually)*
  - Tabletop
  - Actual test with prior notice
  - Actual testing without prior notice/key individuals unavailable

Testing is Key

- *Ok to fail*
- Ensure there are action plans and follow-up that is communicated to BCP Governance Committee
- Learn from other disasters

Challenges with Third Parties

Business Unit/Department who owns third party relationship should ensure there is effective BCP

- Read SOC1 / SOC2 although often not an assessed area but may be mentioned
- Include BCP in contract
  - Require testing – If key vendor, require coordinated testing
  - Require back-ups/redundancy SLAs

Apply BCP to Cyber

- Consider leveraging BCP for cyber incidents
  - Particularly denial of service such as crypto locker
- Very similar to IT disaster such as fire in data center
- Systems Continuity Plan should already contemplate loss of data, network resources

Key Risks / Pitfalls

- Plan doesn’t reflect current processes
- Inconsistency between RTOs/RPOs
- Too much dependency on one individual, lack of documentation
- Too much focus on large scale events and ignores frequent, less severe events
- Regularly communicate the plan
- Lack of testing
- Ineffective communication/decisions across departments

Resources

- GTAG – Business Continuity Management
  - Available through IIA web-site
- Business Continuity, Disaster Recovery, and Incident Management Planning by *Albert Marcella and Carol Stucki*
  - Available at the IIA Bookstore

Contact Info

Please feel free to contact me if you have any additional BCP questions!

Seth Davis

- Seth.Davis@rlicorp.com