Business Continuity Planning: What's at Risk?

Association of College & University Auditors

August 2017

PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

WEBINAR MODERATOR

ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS

Advancing Auditing in Higher Education

- Don’t forget to connect with us on social media!

ACUA SOCIAL NETWORKING

ACUA Distance
Learning Director

Jana Clark

Senior Internal Auditor
Kansas State University

Speakers

Mark Bednarz, MS, CPA, CISA, CFE is a Partner in PKF O'Connor Davies Risk Advisory Group. He combines more than twenty years of public accounting and Fortune 500 experience. Mark's extensive experience includes internal audit, business reengineering, forensic accounting, system implementations, regulatory compliance, Sarbanes-Oxley consulting, IT audits and governance, service organization control reporting (SOC) attestations and IIA QARs.

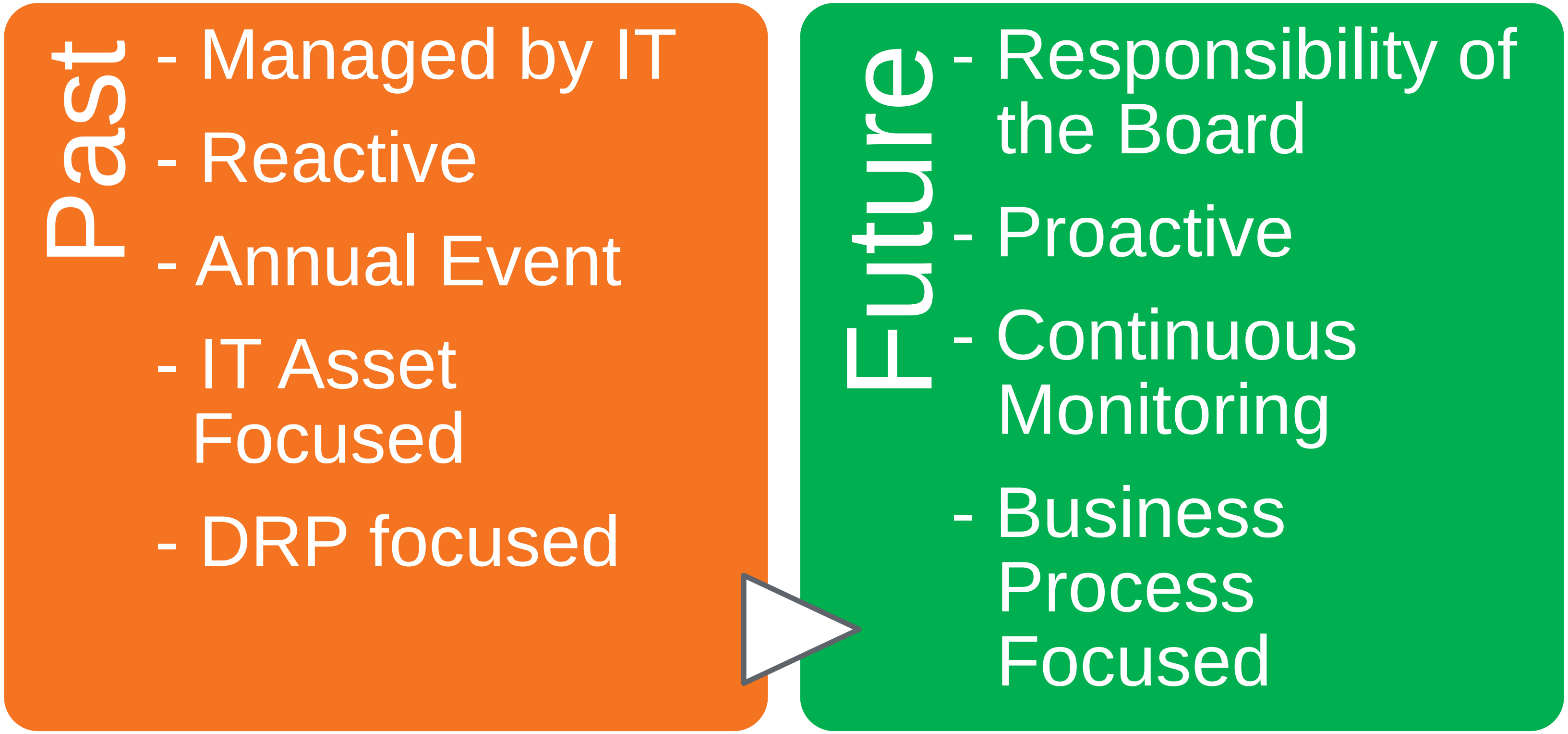
Mark has audited Fortune 500 and higher education BCP and DRP programs. He is on FDU's Information Technology Industrial Advisory Committee (ITIAC).

Lawrence (Larry) Baye, MBA, CISA, CMC is a Principal in PKF O'Connor Davies' Risk Advisory Practice. He recently joined our Firm after a 34 year career as a Principal in the Business Advisory and Risk Consulting Practice of one of the Global Six Accounting and Consulting Firms. During his tenure, Larry served as the Northeast Governance Risk and Compliance Leader and the Sarbanes-Oxley Task Force Leader and advisor to more than thirty public companies, Larry provides "hands on" direction for multiple internal audit outsourcing and co-sourcing projects and has implemented and audited multiple BCP and DR programs.

Learning Objectives

- Discuss the difference between Business Continuity Planning (BCP) and Disaster Recovery Plan (DRP)
- Understanding the importance of having a Business Impact Analysis (BIA)
- Discuss the challenges institutions face in implementing a BCP
- Understand why cybersecurity ties into your BCP program

Why Discuss BCP/DRP ?



Past

- Managed by IT
- Reactive
- Annual Event
- IT Asset Focused
- DRP focused

Future

- Responsibility of the Board
- Proactive
- Continuous Monitoring
- Business Process Focused

What is a BCP and DRP?

- **Business continuity planning** (BCP) is the creation of a **strategy** considering the **threats and risks** facing an institution, with a goal towards ensuring that people and assets are protected and able to function in the event of a disaster.
- A **Disaster Recovery Plan** (DRP) is a documented process or set of procedures to **recover** and protect a business IT infrastructure in the event of a **disaster**. Such a **plan**, ordinarily documented in written form, specifies procedures an organization is to follow in the event of a **disaster**.

Polling Question #1

My Institution has:

A. A Business Continuity Plan (BCP)Only
B. Disaster Recovery Plan (DRP) Only
C. A BCP and DRP
D. Don’t know
E. Do not have a BCP/DRP

BC Challenges On Campus

- Shared campuses: Closing one campus because of building issues while other campuses remain open
- Active shooter scenario
- Misconduct damages the school’s reputation and facilities
- Cyber attack scenario
- Civil unrest spills into the institution’s environment
- Neighborhood / community crisis
- Epidemic
- Security guard strike

What is a Business Impact Analysis?

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

How do they work together?

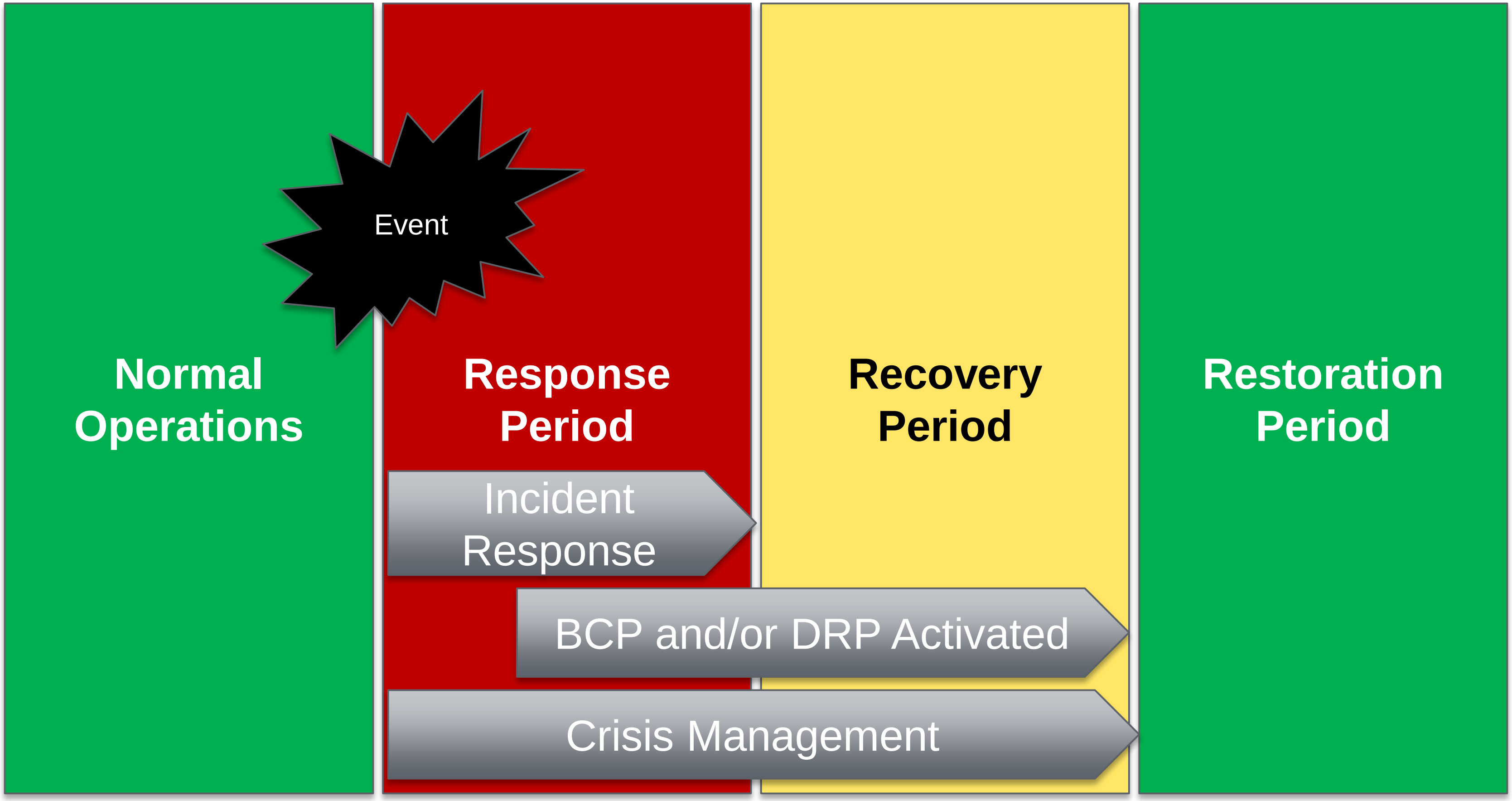
Business Continuity Plan

Risk Assessment

Disaster Recovery

Business Impact Analysis

Timeline



Event

Normal Operations

Response Period

Recovery Period

Restoration Period

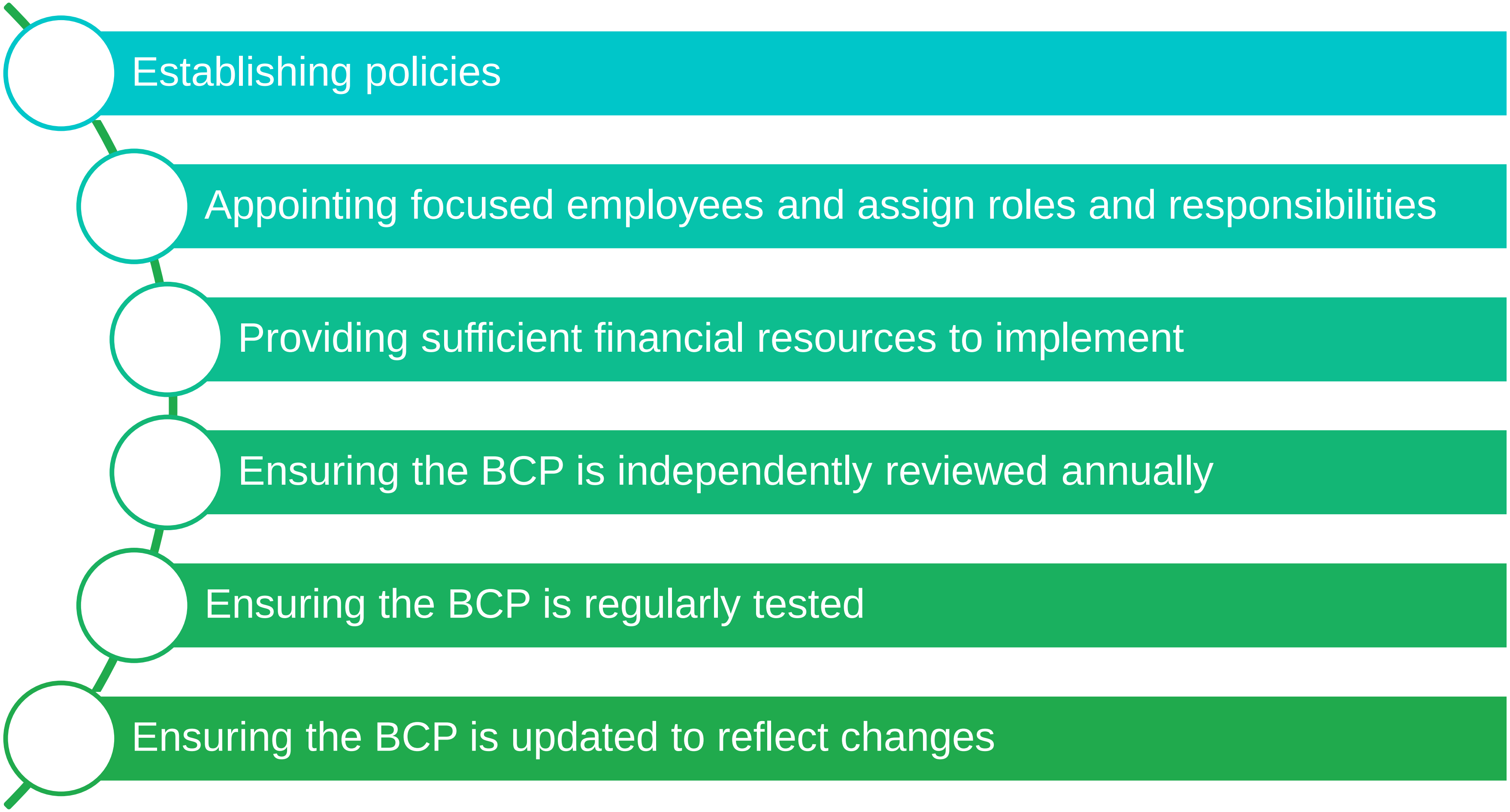
Incident Response

BCP and/or DRP Activated

Crisis Management

KNOW GREATER VALUE

Board and Senior Management Responsibilities



Establishing policies

Appointing focused employees and assign roles and responsibilities

Providing sufficient financial resources to implement

Ensuring the BCP is independently reviewed annually

Ensuring the BCP is regularly tested

Ensuring the BCP is updated to reflect changes

PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

Polling Question #2

Has your institution’s BCP and DRP been independently reviewed?

A. Yes, by external auditors/consultants

B. Yes, by Internal Audit

C. No

D. Don’t know/ Unsure

KNOW
GREATER
VALUE

Challenges in Implementing a BCP

- Lack of executive support as a real priority, limited participation and inadequate funding
  - Absence of a centralized command structure with vague assignment of roles and responsibilities
  - Questionable communication and notification protocols
- No clear focus on resilience that recognizes the importance of:
  - Cohesion between the organization's recovery and the IT disaster recovery
  - Proactive identification and mitigation of risks, as conditions change
  - Knowing what and where the data, records and other assets are located
  - Adequate insurance coverage

PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

Challenges in Implementing a BCP (cont.)

- Disconnect between Institution’s business and IT operations
  - Some systems maybe hosted in the cloud but what do we know about their BCP/DR preparation?
  - Disagreement as to the systems and processes that are recovery priorities (e.g. academic, administrative, research), the time/effort required to restore them and the identification and handling of vital records and data
- Non-holistic solution that maybe ad hoc/ siloed (e.g. departmental-focus, not institutional -wide) and not properly scaled to fit the institution’s operating structure, size and footprint
- Lack of a feedback mechanism to assimilate lessons learned from each testing round

Overcoming the Challenges

- Explain/ document what the goals/objectives of the BCP program are
- Senior Management and the Board need to make BCP a priority
  - Create a Steering Committee to ensure the plan is created, implemented, tested and refreshed after each test and as things change!
  - Ensure all departments actively participate in the BCP
- Have the Steering Committee proactively assess risks

KNOW GREATER VALUE

Business Continuity Planning: Essential Elements

Business Impact Analysis

- Assess and prioritize all critical institutional functions and processes, including their workflow, internal systems, applications, data interdependencies , equipment (e.g. ticketing or access or “charge” or debit-type swipe cards), etc. Are there specific points of failure (people, asset, process, outsourced provider dependencies), how significant are the risks and what might be worst case scenario?
- Identify of the prospective effect of any major non-specific (range of threats) disruption resulting events that impact institutional functions and processes
- Determine the associated legal and regulatory/compliance requirements, such as compromised student information, notification of authorities, etc.
- Estimate the maximum allowable downtime as well as the acceptable level of losses associated with these functions and processes, which may encompass the institution’s reputation, financial costs, information at risk, etc.
- Anticipate the recovery time objectives (RTO) and recover point objectives (RPO) and recovery of the critical path, including resources needed in terms of people, equipment and supplies for recovery?

PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

Business Continuity Planning: Essential Elements (cont.)

Business Continuity Plan Development

- Assumptions and administrative, academic and other priorities
- Internal and External Components, including personnel, communications, technology, facilities, treasury/banking arrangements, manual operations, etc.
- Risk Mitigation Strategies,
  - Succession or coverage for those unable to get to work or recovering “at home”
  - Facilities such as hot sites versus split operations/facilities (each backs up the others systems), multiple sites (distributed resource sharing) versus warm site (applications may not be installed on equipment yet) versus vendor-hosted, such as DRaaS models
  - Data and application/tools (software) backups and recovery strategy
  - Damage assessment
  - Recovery teams (management, infrastructure, etc) and status reporting

Business Continuity Planning: Essential Elements (cont.)

- Requisite Policies, Standards, Processes and Conventions
  - Oversight and “project management”
  - Security and remote access
  - Crisis management and/or incident response
  - Notification/communication (students, faculty, administrative staff, authorities, vendors, media, etc.)
  - Awareness and emergency response training

Business Continuity Planning: Essential Elements (cont.)

Testing and Evaluation

- Board visibility to formal testing policy, scope, staff, technology and facility participation, anticipated outcomes, results achieved and differences to be accounted for or addressed
- Scope of testing should be consistence of the criticality of the process/function to the University
- Annual or more frequent testing is the expected frequency
- Formal test planning should encompass:
    - Objectives and description
    - Schedule, participants, and locations
    - Decision makers, contact information and escalation steps
- Testing approach should be independently reviewed and monitored during execution

Business Continuity Planning: Essential Elements (cont.)

- Testing approaches may include one or more techniques, such as:
  - Tabletop exercise or desktop simulation, where those involved discuss their responsibilities, walk-through each step as outlined in the BCP, clarify or highlight critical plan components and note any problems encountered. The final step requires a debrief to determine what clarifications or further improvements must be attended to. Simulation of a real life scenario with role playing helps shed light on whether the BCP adequately covers the threat response
  - Functional drill with representatives of the effected critical areas to demonstrate emergency response, including notification, mobilization of teams, relocation to alternate site or geographies, restored of computing services and parallel processing to allow transactions to be compared to production results. A full-blown test would take this to the next level and require total interruption of normal operations, limit access to primary facilities and rely on processing based solely on restored backup files, on-location execution and decision-making, etc.
- After the testing is documented in terms of dates, location, recap of objectives and results along with the specifics, any problems encountered should be identified and a gap analysis should be performed to refresh/enhance the BCP after each round of testing.

KNOW
GREATER
VALUE

Polling Question #3

Has your institution performed cybersecurity risk assessment?

A. Yes

B. No

C. Don’t know

PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

KNOW
GREATER
VALUE

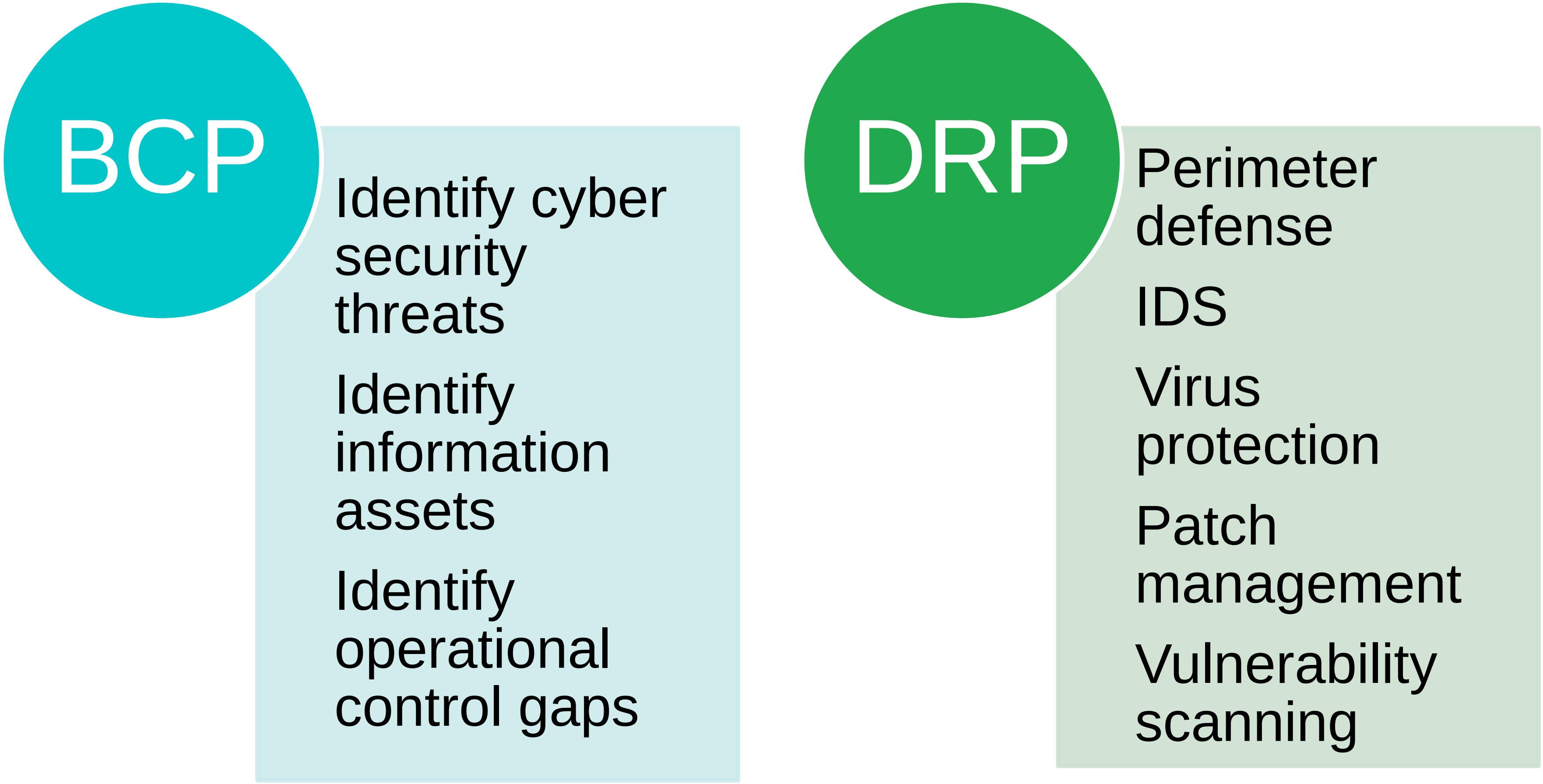
How does Cybersecurity tie into my BCP?

- There are several standards that IT groups typically adhere to when developing response strategies. Some of the most common security best practices that address BCP include NIST 800-53 and ISO 27001
  - Each of these standards outline best practices and specific procedures that IT should consider (and align to as necessary) when working to prevent or respond to cybersecurity threats.

Integrating Cybersecurity and BCP

- Make sure policies are aligned
- Identifying critical processes and related data
- BCP Committee needs to get IT security resources involved and establish regular touch points
- Perform a cybersecurity risk assessment
- Identify control gaps and weaknesses
- Determine strategy for continuity and recovery from a cyber attack disruption

Cybersecurity Considerations



BCP

- Identify cyber security threats
- Identify information assets
- Identify operational control gaps

DRP

- Perimeter defense
- IDS
- Virus protection
- Patch management
- Vulnerability scanning

Internal Audit’s Role

- Communicate the importance of senior management’s and board’s role
- Evaluate whether management has identified and analyzed threats and vulnerabilities in their risk assessments
- Evaluate whether critical processes and supported infrastructure has been identified and prioritized in the BIA.
- Monitor BCP/DRP testing and verify that exceptions were addressed

Polling Question #4

Has your institution ever had to activate your BCP/DRP due to an event?

A. Yes

B. No

C. Don’t know

KNOW
GREATER
VALUE

Hope to see you at the 2017 ACUA Annual Conference in Phoenix

Tuesday, September 26
Session 4 - 8:00 a.m. - 8:50 a.m.
Topic: No IT Staff? How to Hack an IT Audit
Mark Bednarz, Partner-in-Charge, Risk Advisory

Thursday, September 28
Session 10 - 9:00 a.m. - 9:50 a.m.
Topic: Audit and Tax Compliance in Employee Benefits World
Timothy Desmond, Partner, Director of Employee Benefit Services Group
Louis LiBrandi, Principal of Employee Benefit Services Group

PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

KNOW
GREATER
VALUE

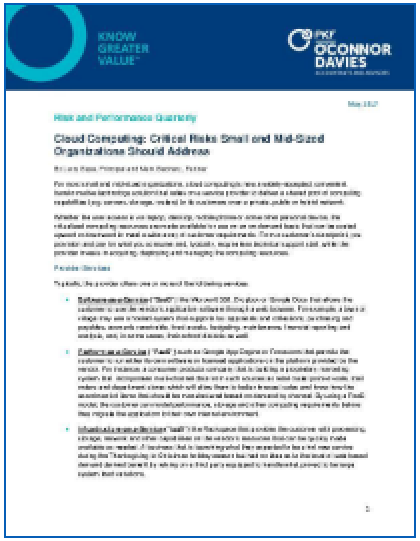
Cloud Computing: Critical Risks Small and Mid-Sized Organizations Should Address

5/22/2017

Article Excerpt:

For most small and mid-sized organizations, cloud computing is now a widely-accepted, convenient transformative technology solution that relies on a service provider to deliver a shared pool of computing capabilities (e.g. servers, storage, routers) to its customers over a private, public or hybrid network.

Whether the user access is via laptop, desktop, mobile phone or some other personal device, the virtualized computing resources are made available for use on an on-demand basis that can be scaled upward or downward to meet a wide array of customer requirements. From a customer's standpoint, you provision and pay for what you consume and, typically, require less technical support staff, while the provider invests in acquiring, deploying and managing the computing resources.



KNOW GREATER VALUE

PKF O'CONNOR DAVIES

May 2017

Risk and Performance Quarterly

Cloud Computing: Critical Risks Small and Mid-Sized Organizations Should Address

PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

Contact Info:
Mark Bednarz, MS, CPA, CISA, CFE
PKF O'Connor Davies, LLP
Partner, Head of Risk Advisory
P: 646-449-6376
E: mbednarz@pkfod.com

Larry Baye, MBA, CISA, CMC
PKF O'Connor Davies, LLP
Principal, Risk Advisory
P: 914.341.7035
E: lbaye@pkfod.com

UPCOMING ACUA EVENTS

August 22, 2017

- HIPAA in Higher Ed – Does your risk assessment get an A+ from OCR? (Baker Tilly)

September 24-28, 2017

- ACUA Annual Conference, Phoenix, AZ

October 12, 2017

- Sponsored Research: Using the data to Detect, Deter & Prevent Fraud (Melissa Hall & Paul Coleman)