FIPCO
COMPLIANT. CONSISTENT. CONFIDENT.

Surviving a Mock Disaster Building an effective Tabletop Exercise

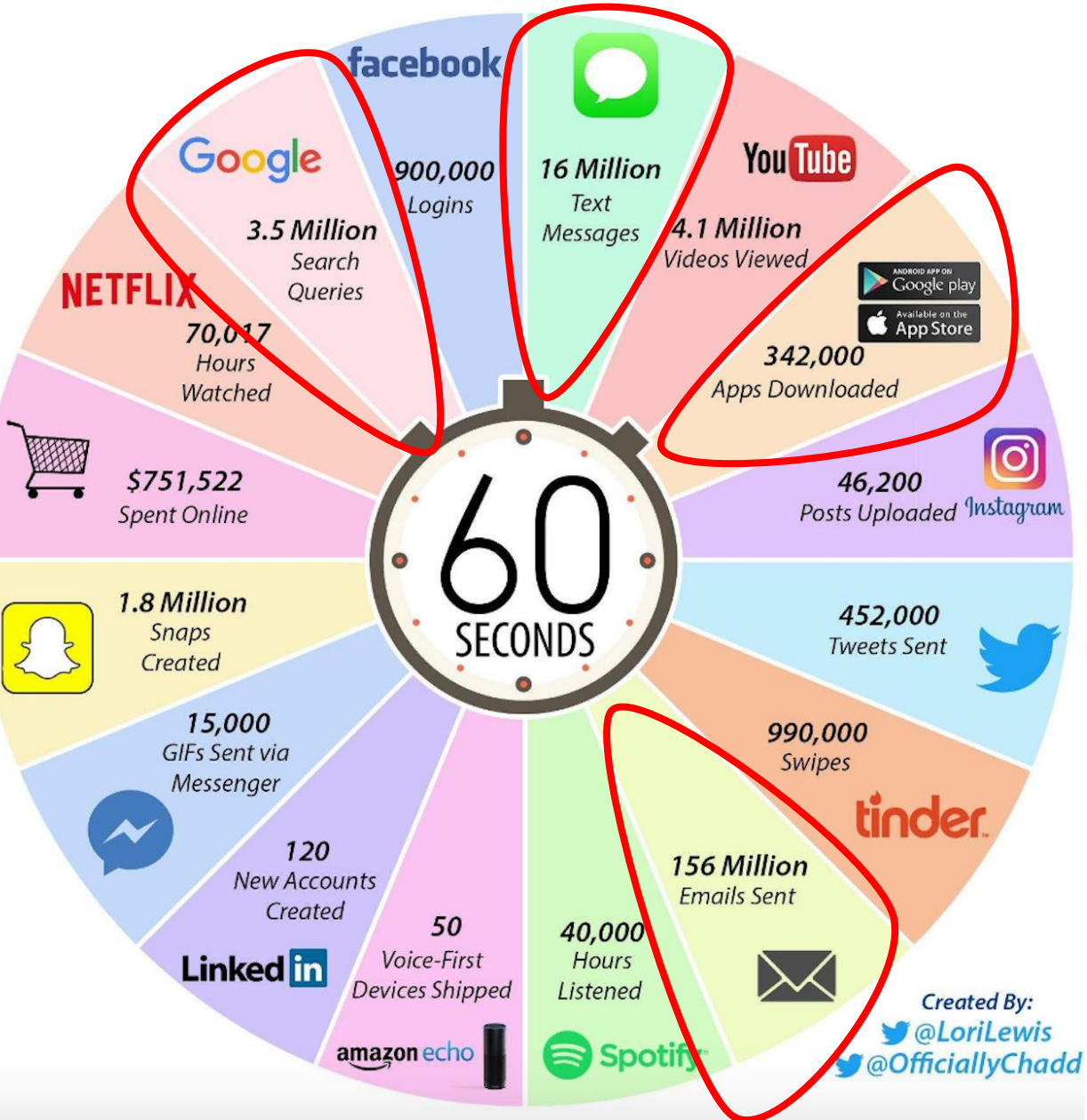
Government IT Symposium
December 2019

Ken M. Shaurette
CISSP, CISA, CISM, CRISC, NSA IAM
Director InfoSec and Audit
kshaurette@fipco.com
(608) 441-1251

Objectives

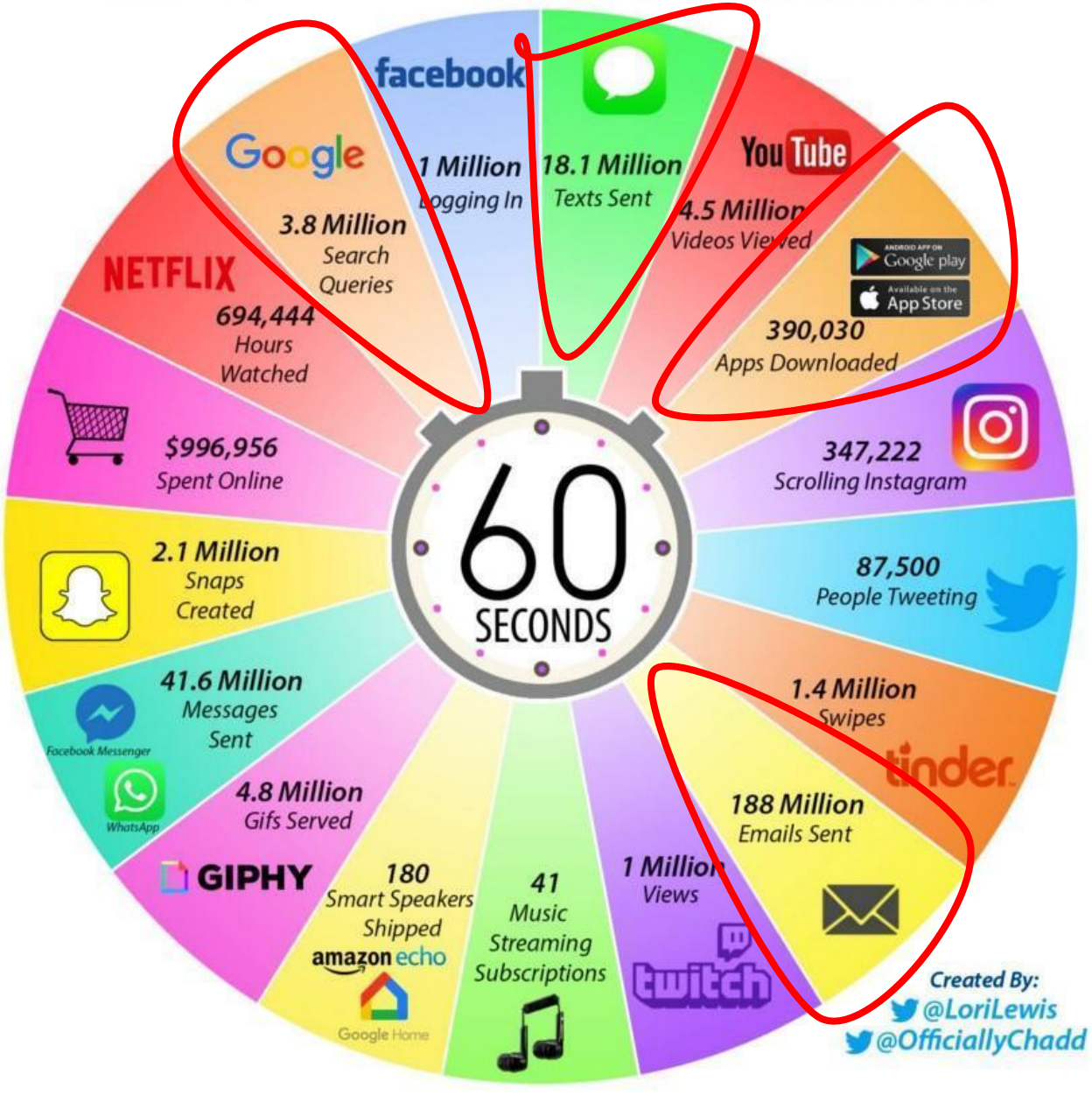
- Importance of Tabletop Exercises
- Identify the major components for BCP/DR.
- Understand the types of Testing.
- What is a Script versus a Scenario?
- Why is a timeline base script important?
- Discuss ties to Incident Response.

2017 This Is What Happens In An Internet Minute



Created By:
@LoriLewis
@OfficiallyChadd

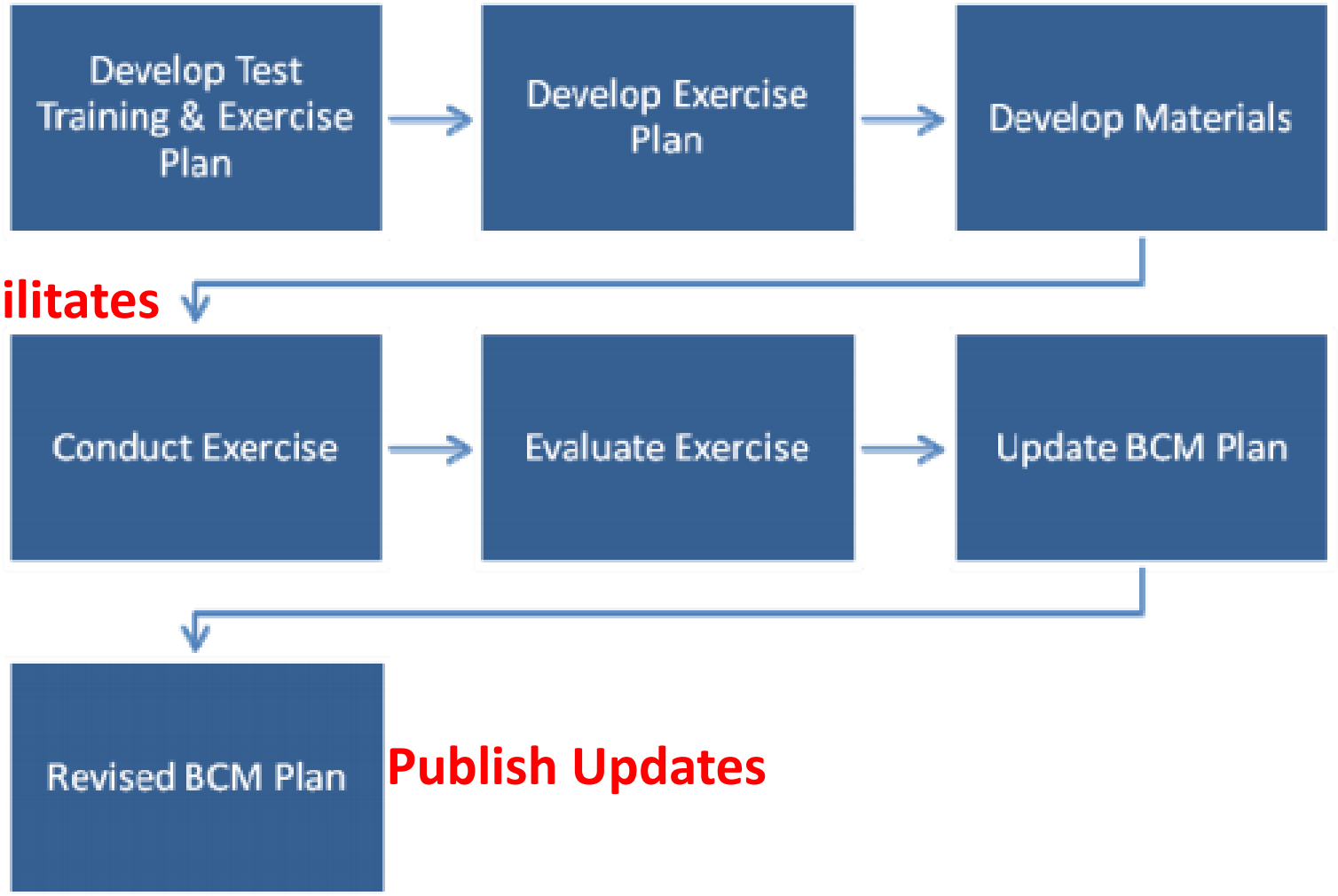
2019 This Is What Happens In An Internet Minute



Created By:
@LoriLewis
@OfficiallyChadd

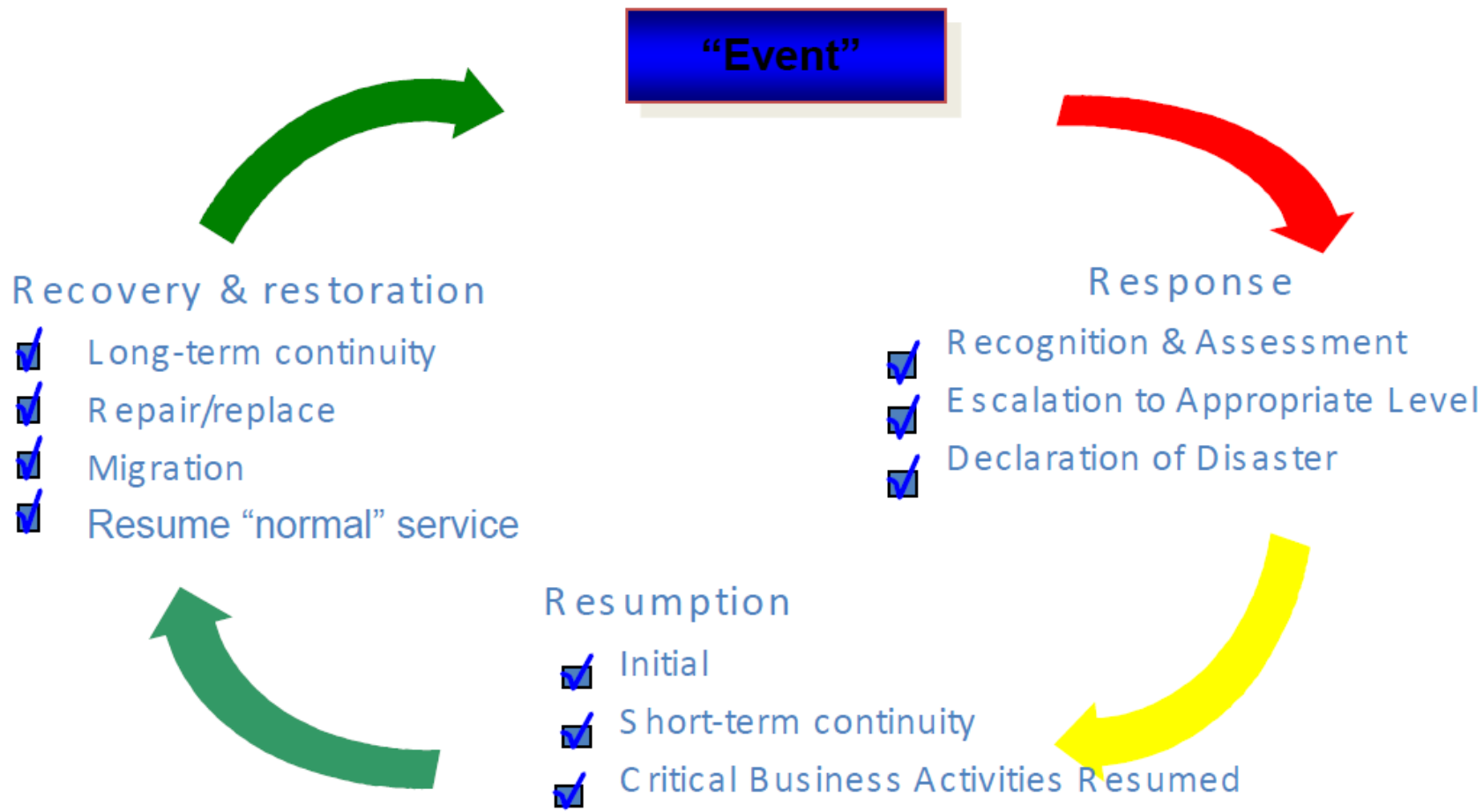
FIPCO
COMPLIANT. CONSISTENT. CONFIDENT.

Strategy



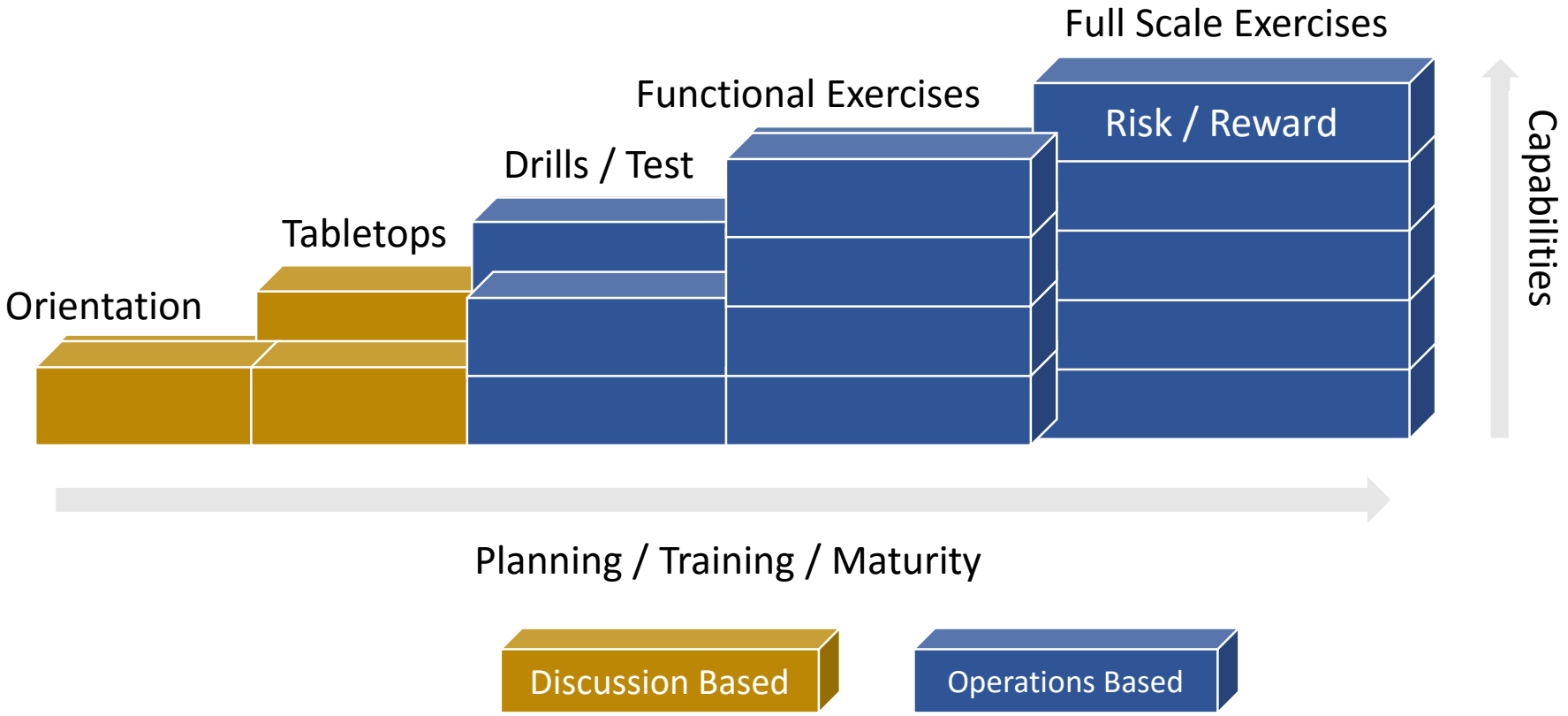
FIPCO
COMPLIANT. CONSISTEN

Business Continuity Cycle



FIPCO
COMPLIANT. CONSISTENT. CONFIDENT.

Ongoing Multi-Year Testing



FIPCO
COMPLIANT. CONSISTENT. CONFIDENT.

Types of Tests

Exercise Type	Description
Orientation	A seminar and/or briefing activity used to familiarize participants with BCM responsibilities
Test or Functional Drill	Coordinated, supervised activity normally used to test, develop, or maintain skills in a single operation or function in a single office or organization
Tabletop Exercise	Simulates emergency situation in an informal, stress-free environment; designed to elicit constructive scenario-based discussions for an examination of the existing BCM plan and individual state of training and preparedness
Functional Exercise **Combination Test**	Used to validate the capability of an organization to respond to a simulated emergency, in order to test one or more functions of the plan
Full Scale Exercise **ALL OUT TEST**	Simulates an actual emergency; intended to evaluate operational BCM procedures and capabilities under simulated stressful conditions

FIPCO
COMPLIANT. CONSISTENT. CONFIDENT.

Defining Roles and responsibilities

Position	Roles and Responsibilities
DR/BCP Coordinator / Information Security Officer	• Coordinate schedule / Exercise facilitator
Management Team	• Provide guidance and approval of Exercise Plan
IT – Manager / Network Admin	• Coordinate IT Recovery Plans • Plan and conduct IT Tests • Support BCP Coordinator in Development and exercising
Participants (all employees, DR/BCP Team, Business Area Managers/SME)	• Member of recovery team • Familiar with Plan • Know assignments • Perform specific business duties

FIPCO
COMPLIANT. CONSISTENT. CONFIDENT.

Functional and Full Scale Tests

- IT Recovery - test restore of technology, (i.e. data, network)
- Going offsite to a backup location tests recovery site preparedness, communications and utilities
- Trained and informed personnel are typically performing recovery steps
- Transaction testing verifies restore, connectivity and access using a person that knows the business process
- Community resources may be involved

What verifies the completeness of the Plan?

FIPCO
COMPLIANT. CONSISTENT. CONFIDENT.

Why Tabletop Exercises?

Provide a forum for the following:

- Team Building
- Discuss components difficult to exercise
- Validate the Plan Documentation
- Information Collection and Sharing
- Obtain consensus from team
- Evaluation of Differing Perspectives
- Practice makes Easier

FIPCO
COMPLIANT. CONSISTENT. CONFIDENT.

Why Tabletop Exercises?

Provide a forum for the following:

- Check that functional testing occurs
- Problem solving of complex issues
- Test considerations for new situations, ideas, processes and/or procedures
- Training/Awareness for management and staff

FIPCO
COMPLIANT. CONSISTENT. CONFIDENT.

Exercise Development Steps

Goals and Objectives –

What will success look like?

(SMART)

- Simple (concise)
- Measurable (how to document)
- Achievable (can this be done)
- Realistic (and challenging) (can it happen)
- Task Oriented (fits to business functions)

FIPCO
COMPLIANT. CONSISTENT. CONFIDENT.

Exercise Development Steps

Scope:

- Exercise Activities
- Departments Involved
- Hazard - Type of Threat Source
- Geographic or outage Impact Area
- Staff Impacted
- Facilities Impacted

FIPCO
COMPLIANT. CONSISTENT. CONFIDENT.

Exercise Development Steps

Building a Script from a Scenario

Threat
Risk Asmt

- Choosing a Threat to Test
  - Vulnerability – Threat Assessment
- Start with simple basic scenarios – basic Fire minimal damage

Note: For example tornado incidents in the Midwest increased awareness of their threat risk.

The state may provide ongoing tasks of planning, preparing, and training for Tornado preparedness.

FIPCO
COMPLIANT. CONSISTENT. CONFIDENT.

Threat Risk Assessment

Threat·Description¤	High¤ Medium¤ Low·¤ °¤	High¤ Medium¤ Low·¤ °¤	High¤ Medium¤ Low·¤ °¤	Risk·Rating¤
Accidental·explosion·—·off-site¤	°¤	°¤	°¤	°¤
Accidental·explosion·—·on-site¤	°¤	°¤	°¤	°¤
Aircraft·crash¤	°¤	°¤	°¤	°¤
Ancillary·equipment·failure¤	°¤	°¤	°¤	°¤
Arson¤	°¤	°¤	°¤	°¤
Bomb·threat¤	°¤	°¤	°¤	°¤
Bombing¤	°¤	°¤	°¤	°¤
Central·computer·equipment·failure¤	°¤	°¤	°¤	°¤
Computer·Intruder¤	°¤	°¤	°¤	°¤

FIPCO
COMPLIANT. CONSISTENT. CONFIDENT.

Exercise Development Steps

Using a Scenario and Building a Script

- As your DR/BC matures - make scripts more complex – increase maturity, add advanced “INJECTS”
- Consider the unexpected – not could it happen, but what if it did.
- Don’t share the scenario before the exercise
- Does the DR/BCP Team always know when a tabletop will occur?

FIPCO
COMPLIANT. CONSISTENT. CONFIDENT.

Exercise Development Steps

Building on a Scenario

- How quickly can you pull together key Business Team Members?
- How quickly can all key individuals be contacted and mobilized to the alternate location?
- Do you test the involvement of any outside parties? (i.e. law enforcement, safety, utilities, telephone, ISP

FIPCO
COMPLIANT. CONSISTENT. CONFIDENT.

Exercise Development Steps

Objectives of Exercise

Tabletop Exercise Program Objectives

- To improve operational readiness by demonstrating knowledge of the DR/BCP Plan overall
- To improve Company-wide coordination and response capabilities for effective disaster response
- To identify communication pathways and problem areas between IT, outside entities (utilities, media) business areas, regional and state emergency operations centers
- To establish timely response for safety, recovery and restore to normal operation.

FIPCO
COMPLIANT. CONSISTENT. CONFIDENT.

Tips for an Effective Tabletop

- **Decide how much gloom and doom you want.**
  - Do you want this to be a physical event with assets damaged and destroyed,
  - Do you just want things inaccessible?
  - Do you want death and injuries, or just to test the ability to get work up and going someplace else?
  - Do you test unavailable key people?
  - How long will your downtime duration be?

FIPCO
COMPLIANT. CONSISTENT. CONFIDENT.

Conducting the Exercise

- Set the Ground Rules
  - Silence Cell Phones
  - Establish timelines – Maximum 4 Hours - breaks, lunch etc..
  - Has Internal Audit been invited?
  - Who leads the exercise?
    - Can they facilitate and participate.
  - Consider issues that need to be tabled for later discussion

FIPCO
COMPLIANT. CONSISTENT. CONFIDENT.

Conducting the Exercise

- Set the Ground Rules (cont…)
  - Accept the Scenario as Real
  - Stay in the Scenario - stay in the mindset that the disaster is really occurring
  - Who will take notes – record issues / follow-up
  - Consider taping the exercise on an audio recorder

FIPCO
COMPLIANT. CONSISTENT. CONFIDENT.

Exercise – Evaluate - Update

- Planned Test scheduled in advance
  - Attendance by all BCP Team required
  - Team is aware of test scenario
- Document Team Member Attendance
- Confirm that all Team Members have their own up-to-date copy of the plan
- The BC/DR coordinator confirms updates are in the plan.

FIPCO
COMPLIANT. CONSISTENT. CONFIDENT.

Exercise – Evaluate - Update

- Review policies and procedures
- Discuss business area changes since last updates – detail continuity procedures
- Confirm accuracy of phone numbers
- Verify Secure and accessible storage of plan (at home)
- Executive summary of the test and discussion results

TESTING

Simulation can help you design your defense; An incident handling and disaster recovery life cycle shares similar characteristics with a business and military strategy known as OODA.

Observe, Orient, Decide Act

The OODA Loop

Military Strategist - Colonel John Boyd

Used to deal with human opponents, applicable to cyber security and cyber warfare.

OODA Loop and Disaster Recovery

- Use the OODA Loop to integrate process, technology and resources into incident response and recovery
- •The OODA Loop is not a static plan but rather a way to make accurate decisions in a rapidly changing environment
- The OODA Loop is not only about responding to an incident but preparing resources
- Incidents are often not static but rather an evolving set of events

FIPCO
COMPLIANT. CONSISTENT. CONFIDENT.

TIP

Experience has shown that well planned and interesting exercises yield a high level of preparedness with personnel who are able to better cope with the stressful environment of an actual emergency.

FIPCO
COMPLIANT. CONSISTENT. CONFIDENT.

Resources

- NIST SP800-84 - Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities (google it)
- Homeland Security Exercise and Evaluation Program (HSEEP) hseep.dhs.gov, FEMA: www.ready.gov/
- National Incident Management System (NIMS: https://www.fema.gov/national-incident-management-system
- Homeland Security and Emergency Management for Your State https://dps.mn.gov/divisions/hsem
- CSOonline Business Continuity, https://www.csoonline.com/resources/
- FIPCO, https://www.fipco.com/solutions/it-audit-security/cyber-security-resources-links

FIPCO
COMPLIANT. CONSISTENT. CONFIDENT.

If Time Allows,
if not:

https://www.fipco.com/solutions/it-audit-security/cyber-security-resources-links

Sample Tabletop Exercise Testing

FIRE

CLICK HERE

STORM

CLICK HERE

Cyber Incident

CLICK HERE