Business Continuity Management Pandemic Planning

FDIC
FEDERAL DEPOSIT INSURANCE CORPORATION

Background Information

This presentation highlights information more fully described in the following resources:

- FIL-6-2008 Interagency Statement on Pandemic Guidance for Minimizing a Pandemic's Potential Adverse Effects
- FIL-14-2020 Interagency Statement on Pandemic Planning
- FFIEC IT Handbook Business Continuity Management, dated November 2019
- Part 364 Appendix B, FDIC Rules and Regulations

Agenda

- What is a pandemic?
- How is pandemic planning different from traditional business continuity processes?
- What processes may help ensure a successful pandemic program?
- What lessons have we learned from COVID-19?
- What questions do you have?

What is a Pandemic?

- **“An outbreak of a disease that occurs over a wide geographic area and affects an exceptionally high proportion of the population, possibly worldwide.”**
- **Pandemics have occurred throughout history, and experts predicted that we would experience at least one pandemic outbreak in this century.**
- **Experts also predicted a possible mutation of the virus and a significant financial and economic impact, both nationally and internationally.**

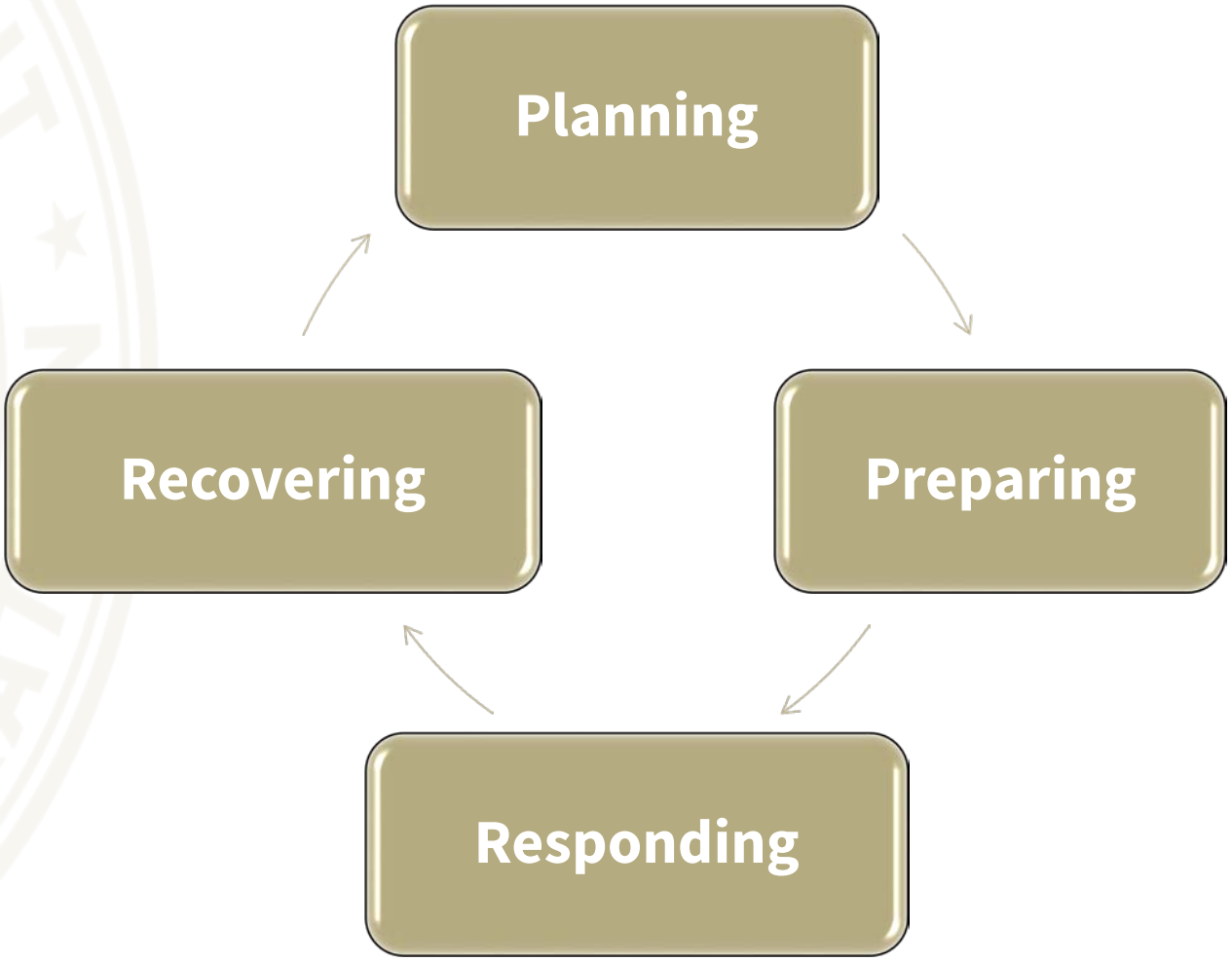
Resource: 2007 FFIEC Issued an Interagency Advisory on Pandemic Preparedness, which was updated in 2020 (FIL-14-2020)

How is Pandemic Planning Different?

Pandemics are unique because:

- **They are unpredictable and difficult to control.**
- **The overall, scale, duration, and impact is more challenging to estimate.**
- **They can occur in multiple waves.**
- **The economic and financial effects are not limited to one geographical area, one organization, or one group of people.**
- **The loss of life can be catastrophic.**

What are the steps that may help ensure a successful Pandemic Program?



Planning – Overview

Consider Board approved guidelines for:

- **Risk based analysis**
- **Employee safety standards**
- **Steps to ensure continuity of operations, resiliency, and timely recovery**
- **Supply chain dependencies**
- **Testing and training processes**
- **Responsibilities**

Planning – Risk Based Analysis

Considerations for an enterprise-wide Business Impact Analysis (BIA) and Risk Assessment (RA) Processes:

- Critical and essential services, not just IT functions.
- Cross-training, succession, and employee absenteeism.
- Likelihood and potential impact on institution, customers, and supporting resources.
- Potential legal and regulatory requirements and whether they can be fulfilled using alternative methods.
- Back-up arrangements and maximum tolerable downtime.

Planning – Risk Based Analysis

- A “gap analysis” may be used to compare the existing strategy to the desired strategy.
- The results can assist in developing a written, pandemic plan.
- Obtain Board or committee approval.
- Communicate the plan.
- Update the strategy as needed, and include testing parameters.

Planning – Employee Safety

Considerations for employee safety plans:

- **Personal Protective Equipment (PPE), including masks, gloves, and cleaning solutions**
- **Social distancing and quarantine requirements**
- **Travel restrictions**
- **Work-from-home opportunities**
- **Family care assistance**
- **Special accommodations for individuals with underlying health conditions**
- **Medical care and sick leave privileges**

Planning – Continuity

Operations:

- **Critical and essential customer facing services**
- **Branch facilities**

Resiliency:

- **Pandemic surveillance, tracking, and reporting**
- **Cybersecurity monitoring and alerting**

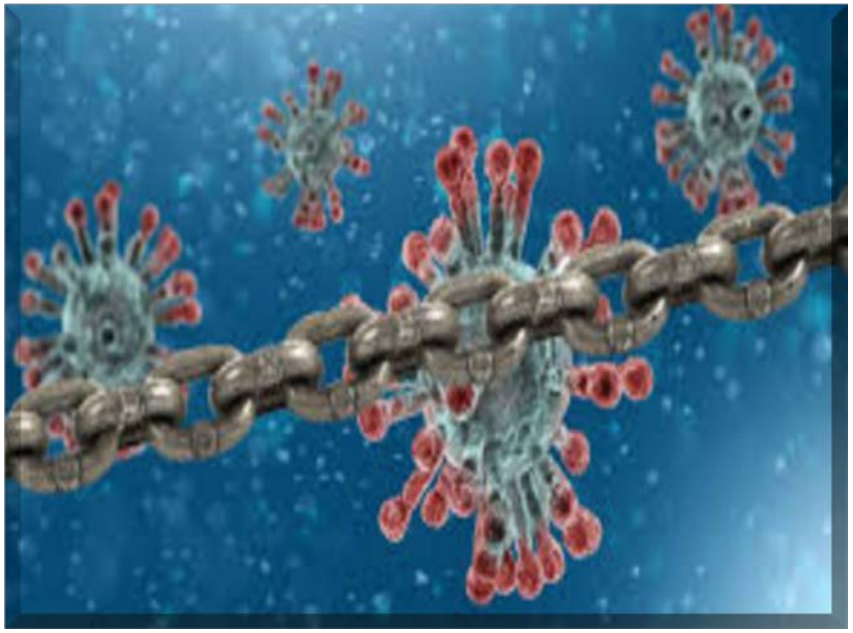
Recovery:

- **Accessibility, change management, back-up, replication, roll-back, and re-creation of critical data files, operating systems, applications, utility programs, data bases, software, and configuration settings**
- **Air-gapping**

Planning – Supply Chain Dependencies

Supply Chain Dependencies can include:

- **Core processing providers**
- **Telecommunications and utility providers**
- **Internet providers**
- **Correspondent bank services**
- **Currency services**
- **ATM services**
- **EFT (ACH and wire) services**
- **Security services**
- **Help desk services**
- **Critical and essential bank supplies**



Planning – Testing and Training

Considerations for Testing and Training Plans:

- **Clear assignment of roles and responsibilities**
- **Validation of people, processes, and technology**
- **Reasonable assumptions and "worst-case" scenarios**
- **Critical staff involvement**
- **Third-party involvement**
- **Documenting results and lessons learned**

Preparing – "Brace for Impact"

Before and during a pandemic, management can:

- **Monitor pandemic trends and threats**
- **Respond to local, state, and national government mandates**
- **Expect employee safety concerns and absenteeism**
- **Expect customer concerns**
- **Anticipate potential higher than normal cash demands and loan requests**
- **Prepare for financial impacts**

Responding

When responding to a pandemic outbreak, management can:

- **Collaborate with federal, state, and local officials and emergency responders**
- **Implement notification procedures for employees, customers, and stakeholders**
- **Share best practices with others and trade associations**
- **Abide by local, State, and Federal mandates**

Recovering

During recovery, management can:

- **Monitor pandemic trends**
- **Consider providing and storing PPE**
- **Follow CDC guidelines regarding proper sanitization procedures**
- **Follow local, State, and Federal guidelines regarding "open for business" procedures**
- **Consider flexible employee work hours and shift options**

Lessons Learned

- **Proactive planning, worst-case scenario testing, and employee training were important to withstand unexpected business disruptions.**
- **Maintaining close contact with industry, community, and medical experts/leaders enabled banks to develop an informed strategy for closures, staff needs, and gradual re-opening plans.**
- **On-going communication using website messages, public announcements, mail notifications, and branch signage kept customers informed and eased their concerns regarding access to their money.**
- **Internal controls helped prevent fraud attempts.**

Lessons Learned

- **Employee awareness, training exercises, and frequent touch-point meetings were crucial to ensure work-at-home activities conformed to security policy requirements and business functions were maintained.**
- **Employee work plan flexibility, including alternate schedules and staggered work days ensured continuity of services.**
- **Preventative, detective, and corrective controls were crucial to protect the bank from the increase in phishing attempts, e-mail spoofing (business e-mail compromise), brute force attacks, and wire fraud.**

Lessons Learned

- **On-going supply chain monitoring, communication, and back-up plans may have prevented disruptions in services and supplies provided by critical vendors, sub-contractors, and foreign providers.**
- **Remote access guidelines, tools, and security measures were paramount to maintain electronic funds transfer capabilities, access to desktop applications, authentication controls, Virtual Private Network (VPN) capacity, e-mail security, patch deployment, security monitoring, break-fix procedures, in-person repairs, use of employee-owned equipment, and regulatory exam activities.**
- **On-going IT Committee, Board, risk management, budget, strategy, and policy oversight allowed the bank to quickly respond to rapid operating changes.**

Lessons Learned

- **Are there other lessons learned from your experience working through the pandemic that you are willing to share?**

Contact Information

FDIC Banker Resource Center – Supervisory resources for banking professionals

https://www.fdic.gov/resources/bankers/

Cynthia E. Scott, Assistant Regional Director
cscott@fdic.gov

Kristopher T. Ferguson, Field Supervisor
kferguson@fdic.gov

Humberto Garcia, IT Examiner
hgarcia@fdic.gov

Charles A. Neal, IT Supervisory Examiner
cneal@fdic.gov

Questions