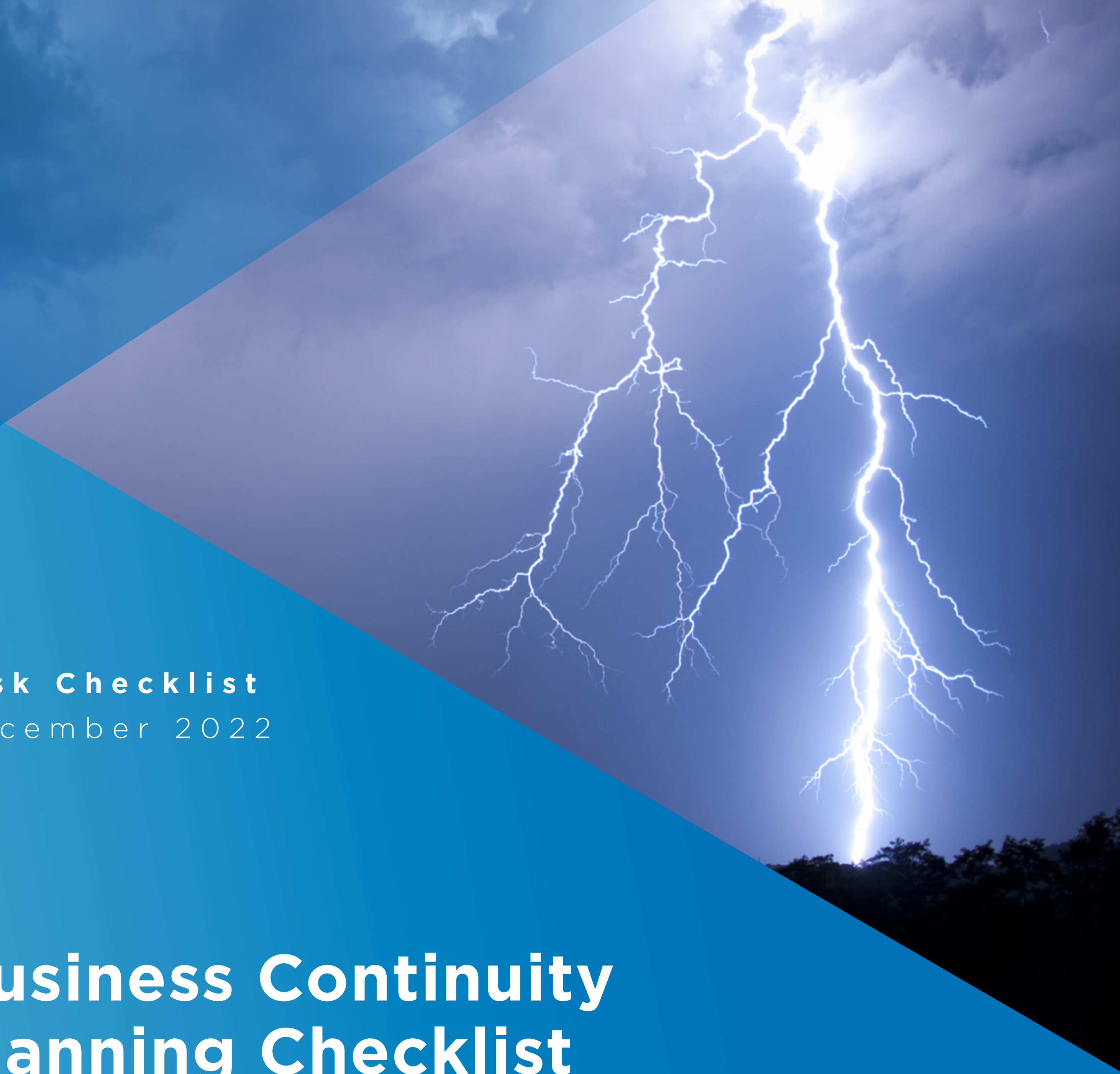

Risk Checklist

December 2022

Business Continuity Planning Checklist

Weather events. Pandemic. Cyberattacks.

These are all potential reasons to enact a business continuity plan, and it is critical that your institution has a plan in place and is ready to execute it as needed.

Follow this checklist to mitigate business risk and continue serving accountholders during an unplanned event.

Allied Solutions

alliedsolutions.net

Business Continuity Planning Checklist

- □ Build response measures that will address any impact to accountholder needs; such as financial, product, communication, and service support needs, including:
  - □ Identify communication strategies, messaging, and channels for affected or potentially impacted accountholders
  - □ How accountholders can reach out for support
  - □ Any action that is required of accountholders to keep themselves or their information secure
  - □ Warnings about fraudulent communications or potential phishing scams
- □ Map out plans to address any potential scenario that would affect your core business or accountholder service operations.
- □ Proactively consult with staff members, suppliers, and service providers regarding how you will tap them for recovery assistance, should you need it.
- □ Identify facilities, systems, and procedures that will allow for the continuance of critical operations in the event a large number of employees become unavailable for a prolonged period.
- □ Make plans for purchasing or renting the equipment needed to continue running your business.
- □ Define which roles can operate out of alternative workspaces to continue operating your business and serving your accountholder if one or more offices close.
- □ Identify contingency plans to address any potential damage caused by a potential disaster. These should include:
  - □ Building damage
  - □ Power outages
  - □ Road closures
  - □ Alarm system or building security failures
  - □ Phone or internet malfunctions
  - □ Supplier shipment issues
- □ Evaluate systems for any security breaches, documenting and reporting any common points of compromise immediately.

Visit our website for more risk education: ***alliedsolutions.net/resources***

- ☐ Build plans that specifically address pandemic response and recovery procedures. These should include:
  - ☐ Multi-phased preparation and response procedures that align with the severity of the pandemic exposure – i.e. plans for when outbreak first hits the nation, versus plans for when a member of your staff contracts the virus
  - ☐ Exposure monitoring procedures
  - ☐ Employee education materials or programs
  - ☐ Internal and external communication strategies
  - ☐ Vendor contingency plans
  - ☐ Rules for employee hygiene
  - ☐ Personal Protective Equipment (PPE) requirement guidelines and corresponding supplies for employees and branch visitors
- ☐ Develop a committee to plan, manage, and oversee continuity plans.
- ☐ Develop an oversight committee to review plans year-over-year and ensure policies, standards, and procedures to sustain compliance and effectiveness.
- ☐ Define a clear chain of command and authority to employ, clearly stating decision makers if an event occurs.
- ☐ Keep an employee roster with employees' addresses, phone numbers, or non-work email addresses.
- ☐ Develop procedures for safely backing up print and electronic data in case computers or servers are destroyed.
- ☐ Develop procedures for documenting intellectual data. Share with employees on a regular basis.
- ☐ Test recovery and response plans to ensure that the practices and capabilities will work effectively and allow critical operations to continue.
- ☐ Share contingency plans with staff, making everyone understands what to do and where to go in the event of a disaster or pandemic.
- ☐ Invest in comprehensive bond coverage to protect your financial institution from expected losses.

Contact us for support with developing your business continuity plan: alliedsolutions.net/contact-us.