Business Continuity/Disaster Recovery Best Practices Checklist

Natural disasters, hardware failures, human errors and cyber-attacks are just some of the disruptions that could cause catastrophic damage to your business. Making Business Continuity/Disaster Recovery (BC/DR) a priority is crucial to the success of your organization. Use this Best Practices Checklist to get started developing or updating your BC/DR plan.

Planning Basics

- [ ] Confirm participation, sponsorship and buy-in from corporate executives.
- [ ] Ensure BC/DR is sufficiently funded and included in the budget.
- [ ] Build a team representing all functional areas for developing and maintaining your BC/DR plan.
- [ ] Establish a team leader with an alternate and define roles for everyone.
- [ ] Create a team list with critical contact information and update it regularly.
- [ ] Develop a comprehensive plan, including both business continuity and disaster recovery (hint: business continuity is business operations centric and disaster recovery is data and systems centric).
- [ ] Define a clear decision-making hierarchy to prevent delays when the worst happens.
- [ ] Identify workforce contingencies for safety, evacuation, remote access and communications.
- [ ] Compile third-party Service Level Agreements (SLAs) for a comprehensive reference.
- [ ] Make sure your plan includes scenarios for cybercrime or cyber-attacks.
- [ ] Keep documentation and distribution lists updated and accessible from more than one location.

Risk Assessment and Business Impact Analysis

- [ ] Identify processes, systems and services critical to your business and prioritize them and associate costs from disruption to them.
- [ ] Evaluate your current systems for data backup and storage.
- [ ] Determine recovery time and how much downtime is tolerable.
- [ ] Identify your organization's weaknesses and vulnerabilities by assessing threats (hint: fire, flood, hurricanes, cyber-attacks are threats or hazards that lead to business risks).
- [ ] Perform a risk assessment to identify situations that can disrupt your ability to deliver the products or services vital to your business (include risks to your workforce, property, operations and reputation).
- [ ] Assess the readiness of your suppliers/vendors to respond or deliver during a disruption and make sure they have BC/DR plans in place.
- [ ] Understand the impacts of supplier/vendor disruptions to your processes.
- [ ] Use the outcomes from your BIA and risk assessments as a foundation for developing plans to ensure business continuity and disaster recovery in each scenario.

For more resources on this topic, visit:
WWW.INTEGRATELECOM.COM/BCDR

Communications

- [ ] Develop a crisis communications plan for internal and external communications.
- [ ] Include your website communications and social media.
- [ ] Create an internal list of key individuals who should be contacted in a crisis and keep it updated.
- [ ] Ensure the crisis communications team is aware of the decision-making hierarchy (see Planning Basics) and has a plan to access the decision maker.
- [ ] Keep a list of the audiences that need communication (employees, partners, suppliers/vendors, customers, authorities).
- [ ] Identify primary spokespersons during a crisis with backups for each person.
- [ ] Prepare scripted communications for key scenarios and update regularly.

Continuous Improvements

- [ ] Maintain a regular schedule for testing disaster/disruption scenarios.
- [ ] Integrate testing with normal business operations (example: text failover processes when your servers have to be taken down for maintenance).
- [ ] Add suppliers/vendors involved in critical processes to your testing process and confirm they perform regular tests.
- [ ] Establish frequent audits of more vulnerable processes and systems.
- [ ] Identify deficiencies in both planning and procedures.
- [ ] Integrate learnings after each test or audit.
- [ ] Evolve your plan as changes occur in processes and technology.
- [ ] Train your teams and awareness for your organization's BC/DR plans through regular communication (see Communications above).
- [ ] Draw upon different methods such as walkthroughs, tabletop, functional and full-scale exercises to train and evaluate your plans.
- [ ] Assess the response capabilities of your resources and identify additional resources as needed.
- [ ] Consult with local and federal agencies for guidance on your plan.
- [ ] Add redundancies and backups as needed to support contingency plans.
- [ ] Ensure new processes and projects include business continuity plans before implementation.
- [ ] Keep BC/DR on the annual budget to guarantee on-going investment and support.
- [ ] Be flexible – your plan should evolve with your organization.

Integra offers a range of reliable, secure solutions from advanced networking, communications, managed services to cyber security solutions. Every business has unique needs and we work with you to find the right solution. Contact Integra to discuss your business continuity/disaster recovery needs.