InfoSight®
www.infosightinc.com

When Disruption Hits,
Improvising Isn't a Plan

Business Continuity & Disaster Recovery Planning

Downtime Doesn't Check Your Budget First.
Building a real BCP/DR strategy spans every department, process, and system — and most organizations face limited budgets, skill gaps, evolving regulations, and vendor dependencies without a dedicated Certified Business Continuity Professional (CBCP) to pull it together.

www.infosightinc.com | info@infosightinc.com | 305-828-1003

Where Continuity Falls Apart

- **Limited Budgets & Skill Gaps:** Few organizations have a dedicated CBCP or the resources to build a real plan in-house.
- **Evolving Regulatory Compliance:** GLBA, PCI, HIPAA, and NERC requirements keep shifting the target.
- **Vendor & Supply Chain Dependencies:** Third-party disruptions can take you offline even when your own systems hold up.
- **Escalating Cyber Risk:** Ransomware and human error are now leading causes of business disruption, not just natural disasters.

InfoSight's U.S.-based BCP team crafts a bespoke continuity and disaster recovery strategy — aligning RTOs, RPOs, and compliance frameworks so you stay online, compliant, and cyber-resilient when it matters most.

Turn Disruption Into a Non-Event

- ✓ **Customized Continuity Plan:** Built around your organization's actual operations, not a generic template.
- ✓ **Workable, Not Just Written:** A BCP document employees can follow when it counts.
- ✓ **Faster, Confident Recovery:** A drivable DR strategy that mitigates risk and accelerates recovery.
- ✓ **Regulatory Compliance Built In:** Continuity planning that satisfies examiners as well as operations.

www.infosightinc.com | info@infosightinc.com | 305-828-1003 | InfoSight® www.infosightinc.com

OUR 5-STEP APPROACH

1. **Risk Assessment**
   Identify threats, assess likelihood and impact, and pinpoint the critical business functions that need continuity.

2. **Business Impact Analysis (BIA)**
   Quantify the effect of disruptions on operations, define RTOs and RPOs, and prioritize recovery requirements.

3. **Technology Strategy**
   Confirm your IT/OT infrastructure aligns with departmental RTOs and RPOs, then design a resilient technology strategy.

4. **Documentation**
   A formal BCP framework and Emergency Response Plan, with policies, procedures, and communication protocols built for compliance.

5. **Testing**
   Tabletop exercises, simulations, and DR drills validate the plan and refine recovery steps in real-world scenarios.

WHY CHOOSE INFOSIGHT

- ✓ *24×7×365 U.S. SOC/NOC: Continuous monitoring, rapid escalation, and strict data sovereignty compliance.*
- ✓ *SOC 2 Type II Certified: Independent attestation of our security controls, year-round.*
- ✓ *25+ Years of Regulatory Expertise: Proven track record across GLBA, PCI DSS, HIPAA, NERC CIP, and AWIA.*
- ✓ *Certified Experts: CISSP, CISA, CEH, OSCP, AWS, and AWWA credentials across our team.*

KEEP YOUR BUSINESS RUNNING — 24 HOURS A DAY

Schedule a 15-minute consultation with a Certified BCP Professional. One follow-up from a security expert, no spam, ever.