CYBER AWARE

The Challenge

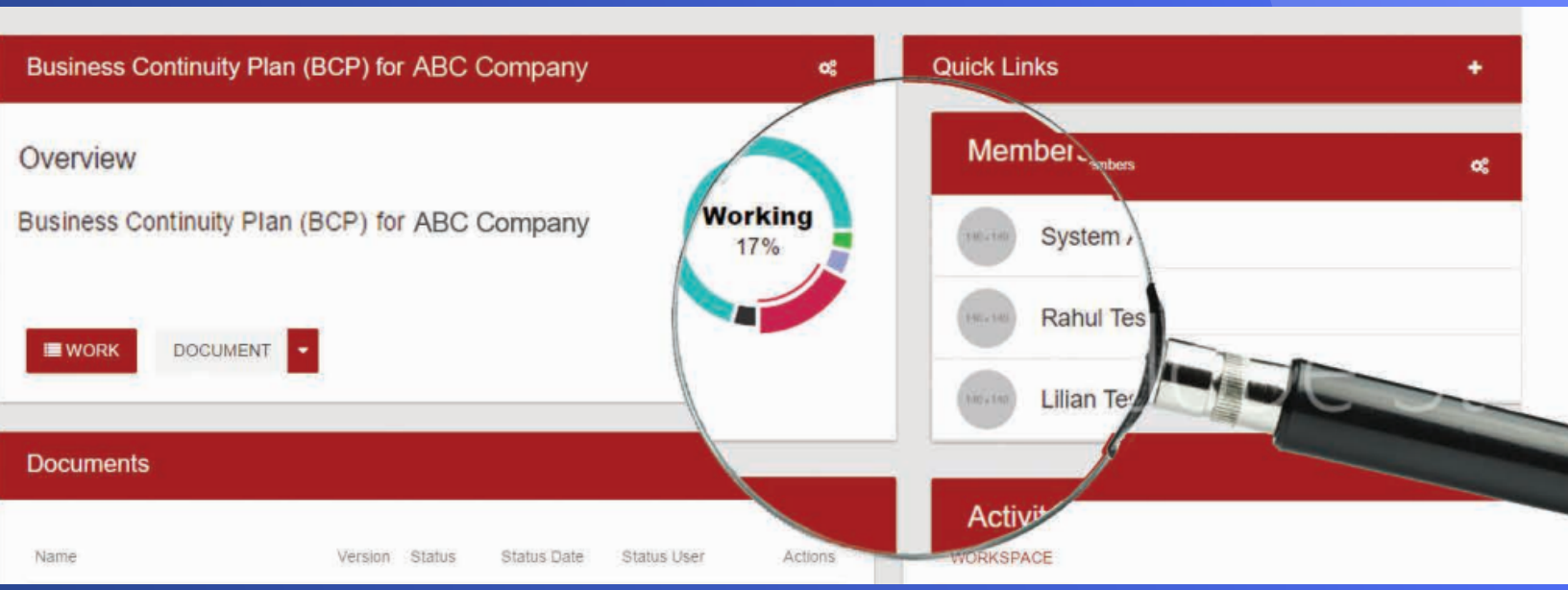
As a business continuity leader, you are bombarded daily with new challenges and threats. Ever-changing regulations, malware, ransomware, and hackers are an increasing drain on your IT department With limited resources and a staff that has grown more reactive than proactive, you face a daunting challenge to stay on top of operational and recovery strategies. When crisis occurs, you can only hope you've done your best — but you know that's not good enough. You need a BCP champion that will deliver an accurate, reliable solution — a team of experts that will be there for every phase of the process.

Cyber Aware Solution-based Services

Cyber Aware is a leading-edge Business Continuity Plan (BCP) solution that allows users to view all resource dependencies of an organization and how they interact. Our web-based, enterprise-wide SaaS platform includes an end-to-end Business Continuity Management System (Cyber AwareS) tool, performance-oriented scalability, and best-in-class hosting and self-hosting options. It supports multiple Cyber Aware standards, such as ISO 22301, FEMA, ISO 27001, and features data import and export connections with external databases via API. Other functions include an intelligent rules engine with metadata-driven process automation, central management of tasks, content and documents, and workflow-driven run-time plan access.

Contact Us: Info@tpcm-usa.com • 833-TPCM-USA • www.tpcm-usa.com

CYBER AWARE



Business Impact Analysis (BIA)
The BIA is the foundation of Cyber Aware. Without it, you'll become reactive rather than proactive to critical needs. The Cyber Aware BIA package involves:

- BIA sessions that dig deep into your organization's infrastructure to identify your critical processes and dependencies.
- Identifying gaps in critical processes and their Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).
- Drill down from the process level to the IT Disaster Recovery (DR) server matrix to identify gaps.

Risk Assessment
• Multiple threat scenario assessment (cyber, human, terrorist, environmental).
• Likelihood and Impact-based on quantitative input.
• Financial impact (quantitative) alignment of risk where available.
• Reporting on high risk areas and mitigation plans.

Plan Development (Strategic and Departmental)
• Plan development in collaboration with organization subject matter expert (SME), based on the BIA and risk assessment.
• Ensuring mitigation plans are developed for critical processes.
• Web-based and mobile-based access to ensure availability when needed.

Maintenance & Updates
• Annual plan reviews and BIA updates.
• Centralized location for both real and unplanned event analysis.
• Software releases in conjunction with technology and/or regulatory changes.

Work the Plan
• Annual tabletop exercises that help to identify gaps in organization readiness.
• Educational blogs.
• Think tank sessions with your peers

Contact Us: Info@tpcm-usa.com • 833-TPCM-USA • www.tpcm-usa.com