B | RILEY Advisory Services

COMPLIANCE, RISK & RESILIENCE:

SERVICES & CAPABILITIES

PRACTICE LEADER
Duane Lohn
dlohn@brileyfin.com
(602) 321-9818

SUMMARY

Disruption and crisis risk is a sustained and predictable operating condition facing all organizations. Regulatory enforcement actions for compliance shortfalls are now more punitive and consequential. Stakeholders are increasingly unforgiving when organizations perform poorly in crisis. We advise clients' enterprise resilience efforts at the board and C-suite level.

DEMAND DRIVERS

- Recent breach, loss, claim disruption (pandemic, cyber, climate-related, e.g.)
- Regulatory obligation
- Audit finding
- Governance, risk and compliance (GRC) initiative
- Commercial condition required by a customer

Business Continuity Planning (BCP)

Assuring operational continuity after disruption and crisis is a hallmark of prepared organizations, a widespread regulatory requirement, a pillar of risk management, and an essential risk control.

- Current state assessments
- Business impact analysis
- Business continuity plans
- Simulations and exercises

IT Disaster Recovery (ITDR)

Business recovery requires technology to support organizational recovery priorities. ITDR plans supply the re- sources (hardware, communications, and software applications) required in the business continuity plan.

- Minimum equipment configuration
- Critical application inventory
- Data restoration procedures
- Disaster recovery plans

Enterprise Risk Management (ERM)

Risk-managed organizations have a process for identifying, assessing and managing risks so leaders can understand, prioritize and make decisions. ERM enables companies to prioritize and address risks based on objectives and risk appetite. We help clients implement a process that:

- Generates value
- Supports strategy
- Enhances enterprise value
- Creates a risk-aware culture

Cybersecurity Risk Management

Cybersecurity risk is a ubiquitous, high-profile enterprise issue that universally affects organizations as the leading cause of data loss and operational downtime. As the complexity and vulnerability of information systems evolve, so should cybersecurity risk management.

- Compliance assessments against standards, frameworks and regulations
- Optimizing DFARS and CMMC compliance
- Cybersecurity maturity, strategy and policy
- Network, mobile and web application security

Emergency & Crisis Management

With crisis situations seemingly inevitable, all organizations should have the ability for their global response teams to collaborate – crisis management, response coordination and resolution – as a fundamental risk management capability. We provide a unique crisis management platform that:

- Enables secure team interaction in 60 languages
- Delivers situational awareness and automated escalation paths
- Expedites crisis response and recovery
- Geo-targets impacted staff and sites