cogent infotech

Case Study

Developing a Centralized Cyber Risk & Compliance Management Platform

The Client

A U.S.-based financial services enterprise operating across multiple states, supporting lending, payments, and investment services. The organization manages sensitive financial data and is subject to increasing regulatory scrutiny while facing a growing cyber threat landscape.

The Challenge

- Disparate cybersecurity tools used for risk management, compliance tracking, vulnerability management, and audits
- Manual tracking of regulatory controls (SOC 2, ISO 27001, PCI-DSS) through spreadsheets and siloed documentation
- Limited real-time visibility into the organization’s overall cyber risk posture
- Inefficient coordination between security, compliance, and IT teams during remediation efforts
- Delays in audit preparation, evidence collection, and remediation tracking
- Need for a scalable platform to support evolving regulatory and compliance requirements

About Cogent Infotech

Founded in 2003, Cogent Infotech is a trusted, award-winning firm with **23+ years** of experience**, 150+** government contracts, **10,000+** projects, and a **96% employee retention rate**. Recognized as an SBA Small Business and MBE-certified, we deliver excellence through diverse talent, AI-driven recruitment, and cooperative contracts like **NASPO Value Point and TIPS-USA.**

Babu V.
Chief Revenue Officer

babu@cogentinfo.com

972 – 439 - 0386

Solution and Process

- **Unified Risk Dashboard**
  Centralized visibility into enterprise cyber risks, vulnerabilities, and control status across business units

- **Compliance Mapping Engine**
  Automated mapping of controls across SOC 2, ISO 27001, PCI-DSS, and internal security policies

- **Remediation & Workflow Automation**
  Issue tracking, ownership assignment, SLA-based escalation, and remediation progress monitoring

- **Audit Readiness Module**
  Centralized evidence repository, audit trails, and real-time compliance reporting

- **Role-Based Security**
  Segregated access for auditors, security teams, compliance officers, and executive leadership

Outcome

- Established a **single source of truth** for cyber risk and compliance management

- Achieved a **40% reduction in audit preparation time**

- Improved regulatory confidence through real-time visibility into control status

- Accelerated remediation cycles using automated workflows and escalation

- Delivered a **scalable cybersecurity platform** ready to support future regulatory frameworks

Risk Analysis

- Regulatory compliance risk due to fragmented control tracking

- Audit readiness risk from manual evidence collection processes

- Data integrity and access control risk across multiple user roles

- Remediation delay risk without automated workflows and escalation

- Scalability risk as new regulations and frameworks are introduced

Best Practices

✓ Secure-by-design architecture with embedded identity and access controls
✓ Automated compliance mapping across multiple regulatory frameworks
✓ Centralized evidence management to support audit readiness
✓ SLA-driven remediation workflows to accelerate issue resolution
✓ Role-based access aligned to security, compliance, and executive needs
✓ Scalable platform design to support evolving regulatory requirements

TECHNOLOGIES

- **ARIA™ (Cogent AI Talent Intelligence Platform)**
- **Java, Spring Boot**
- **Microservices Architecture**
- **Angular (secure, role-based UI)**
- **Azure App Services**
- **Azure SQL & Azure Data Lake**
- **Microsoft Entra ID (Azure AD)**
- **Azure Monitor & Log Analytics**
- **Power BI**

Babu V.
Chief Revenue Officer | **babu@cogentinfo.com** | **972 – 439 - 0386**