

# Security Beyond Standards

## SOC Compliance for Secure Utility Operations

### System and Organizational Controls (SOC 2) Compliance

CUSI has built a comprehensive cybersecurity strategy centered on SOC 2 compliance to safeguard sensitive utility data and operations. SOC 2 certification, provided by the American Institute of CPAs (AICPA), demands rigorous standards based on the Trust Services Criteria: security, availability, processing integrity, confidentiality, and privacy. CUSI has achieved SOC 2 Type II, reinforcing our dedication to data security and operational integrity.

### Why SOC?

Partnering with a SOC 2 compliant vendor means utilities gain protection through independently verified, industry-leading security standards, extending beyond basic measures. CUSI's SOC 2 compliance covers stringent controls over data handling—from data conversion and implementation to ongoing service delivery—ensuring essential protection in today's cyber landscape.

- **Enhanced Data Security:** SOC 2 compliance ensures CUSI enforces rigorous controls to protect customer and operational data, reducing the risk of breaches.
- **Operational Resilience:** With SOC 2 certified measures to ensure availability and continuity, utilities experience minimal downtime, ensuring uninterrupted service.
- **Risk Mitigation:** SOC 2 compliance verifies proactive risk management, supported by internal controls, audits, and monitoring to minimize costly security incidents.
- **Independent Verification:** SOC 2 compliance requires independent audits, providing third-party assurance that CUSI meets high standards for security, availability, and data integrity.
- **Clear Accountability:** SOC 2 certification ensures transparency in CUSI's security processes, supporting clear accountability for data protection.
- **Alignment with Best Practices:** SOC 2 compliance guarantees that CUSI follows industry best practices, giving utilities peace of mind with a trusted provider.

## CUSI's Dual-Layered Assurance with Azure's SOC Certification

While Microsoft Azure's SOC 2 compliance secures foundational infrastructure, **CUSI's independent SOC 2 certification** adds an essential layer of protection for our applications and data management practices. Unlike competitors who rely solely on their hosting partner's SOC 2 certification, CUSI's SOC 2 compliance verifies that we, as a software vendor, meet stringent security, availability, and privacy standards directly within our software and processes.

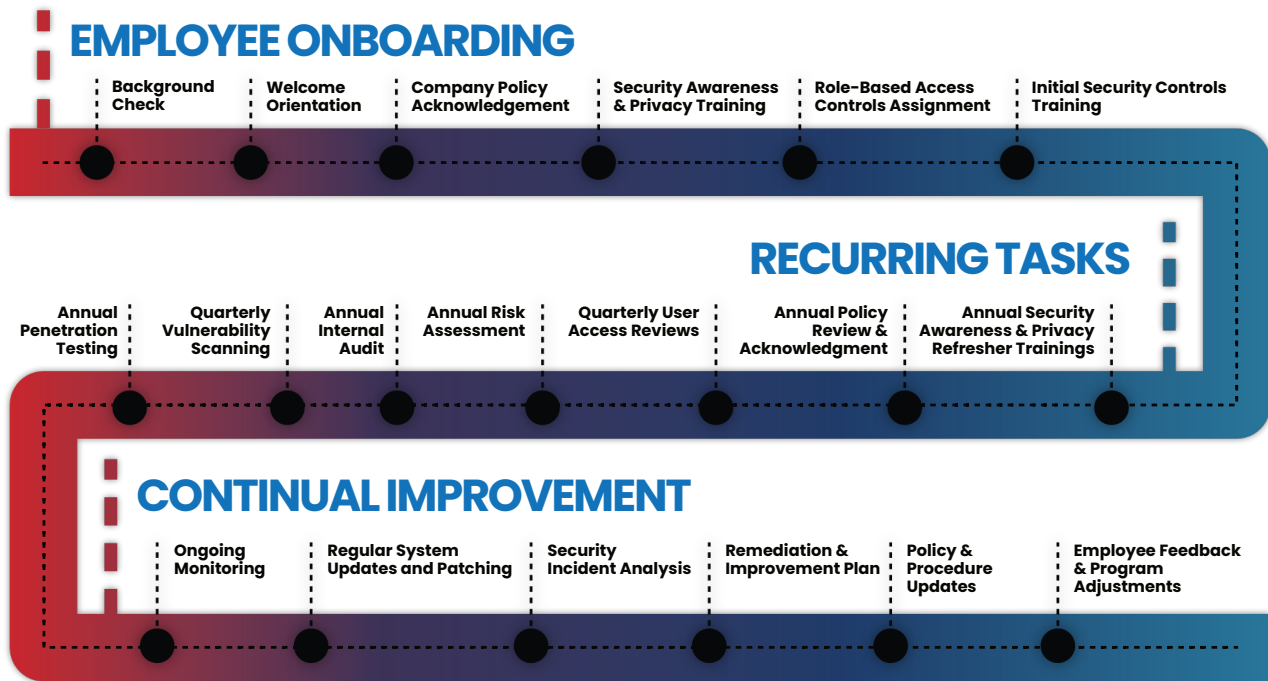
This dual-layered approach protects our clients with both Azure's SOC 2 certified infrastructure and CUSI's independently validated application security. With CUSI, utilities partner with an organization that doesn't simply inherit security standards but actively upholds and enforces them across every level—ensuring compliance, accountability, and operational resilience from end to end.

## Independent Verification of CUSI's Security Standards

SOC 2 compliance offers third-party verification of CUSI's security practices, with regular audits ensuring our internal controls meet stringent standards. This independent assessment means utilities can trust CUSI's dedication to protecting data integrity and privacy.

## Continuous Improvement and Resilience

The SOC 2 compliance process at CUSI is not a one-time audit, it's an ongoing commitment to excellence. With continual assessments and a culture of improvement, we adapt our security practices as new threats emerge. Starting from employee onboarding and through recurring training and evaluation, our SOC 2 framework ensure that CUSI's security posture is always evolving to meet current standards.



# SOC 2 Compliance: The Gold Standard of Security and Trust

For utilities, SOC 2 compliance is more than a certification; it's a standard of reliability, security, and trust. With SOC 2 Type II compliance, demonstrates CUSI's commitment to the highest levels of security across our operations. CUSI meets the Trust Services Criteria for security, availability, processing integrity, confidentiality, and privacy. This dual approach—combining CUSI's SOC 2 compliance with Microsoft Azure's SOC 2 certified infrastructure—ensures that utilities can trust us to safeguard sensitive data and support operational resilience.

## Key Benefits for Utilities:

- **Verified Data Protection:** Independent SOC 2 certification affirms our commitment to secure data management.
- **Operational Continuity:** SOC 2 focused standards and Azure's infrastructure guarantee high availability and secure data recovery.
- **Reduced Compliance Burden:** Partnering with a SOC 2 compliant vendor helps utilities meet regulatory standards.
- **Proactive Threat Defense:** SOC 2 compliance includes continuous monitoring and threat response, safeguarding utilities from emerging risks.
- **Enhanced Customer Trust:** Working with a SOC 2 compliant provider reinforces utilities' commitment to data security.

Choosing CUSI means choosing a partner dedicated to industry-leading solutions with robust, verified data security.

### SOC 2 Trust Services Criteria List

- ✓ Detailed Organizational Chart
- ✓ Comprehensive Employee Handbook
- ✓ Company Code of Conduct
- ✓ Board of Directors
- ✓ Internal & External Assessments
- ✓ Roles, Responsibilities, Authority, Job Descriptions
- ✓ Job Requirements & Competency Evaluations
- ✓ Criminal Background Checks
- ✓ Security Awareness Training
- ✓ Secure Code Development Training
- ✓ Annual Performance Reviews
- ✓ Company Policy Assignments
- ✓ Internal Control Evaluation
- ✓ Ongoing Policy, Key Personnel, Responsibilities, Processes & Product Updates
- ✓ Code of Conduct Violation Process
- ✓ Customer Support Line Process
- ✓ Security and Availability Commitments
- ✓ Quarterly Review of Firewall Rule Sets and Security Groups
- ✓ Required Utilization of Test Data
- ✓ Required Baseline Configuration for Production Resources.
- ✓ Required Updates Change Management Process
- ✓ Restricted Code Deployment & Configuration Changes
- ✓ Required Cyber Security Insurance
- ✓ IT Inventory of Service Providers Risk Weighted
- ✓ New IT Vendor Review and Assessment
- ✓ Annual Monitoring of Critical Service Providers
- ✓ Incident Response Procedures
- ✓ Security Incident Handling Process
- ✓ Annual Testing of Incident Response Plan
- ✓ Weekly Review of Performance Metrics
- ✓ Utilization of Autoscaling Technology
- ✓ System Logging and Monitoring
- ✓ Daily Back Up Monitoring
- ✓ Daily Database Snapshots
- ✓ Continual Replication of Production Database
- ✓ Disaster Recovery Plan
- ✓ Annual Validation of Backup Integrity
- ✓ Encrypted Encryption Keys
- ✓ Passwords & API Keys Salted & Hashed
- ✓ Restricted Access To Production Cloud Environment
- ✓ Restricted Access to Production Servers
- ✓ I2+ & Secure APIs Customer Data Encryption
- ✓ Computer Hard drive Encryption
- ✓ Security Center Monitoring Software Systems
- ✓ Required Anti-Virus Software
- ✓ Data Classification & Destruction Procedures
- ✓ Production Server Configuration Monitoring
- ✓ Web Application Firewalls
- ✓ Software Development Life Cycle Procedures
- ✓ Documentation of Code, Configuration, & Infrastructure Changes
- ✓ Version Control Software
- ✓ Developer Code Peer Reviews
- ✓ Quality Assurance Testing
- ✓ Integration and Regression Testing
- ✓ Development Code Merging Tracking
- ✓ Testing and Deployment Approvals
- ✓ Division of Development, Testing, & Production Environments
- ✓ Segment Network Traffic Using Public/Private Subnets
- ✓ Software License Agreement Posting
- ✓ Risk Policy
- ✓ Risk Mitigation Register Reporting
- ✓ Annual Third Party Assessment
- ✓ Quarterly External Vulnerability Scans
- ✓ Annual Third Party Penetration Test
- ✓ Visitor Sign In, Tracking, Escort
- ✓ Immediately Disable Access Terminated Employees and Contractors
- ✓ Access Approval of New or Modified Users
- ✓ Notification of Terminated Employees and Contractors
- ✓ Quarterly Review of User Access
- ✓ Customer Security Administrator Account
- ✓ Annual Review of User Matrix Access & Privileges
- ✓ Annual Review of Information Assets
- ✓ Authenticate Internal Applications User ID & Password Requirements
- ✓ Authenticate Production Servers & Databases User ID & Password Requirements
- ✓ Authenticate UB4 & CWP User ID & Password Requirements
- ✓ Require Multifactor Authentication
- ✓ Secure Production Resources
- ✓ Managed Customer Databases Encryption