United Allied
Global Risks & Security Solutions

GRC & CYBERSECURITY SOLUTIONS OVERVIEW

Technology & FinTech

Compliance built to scale with your ambition — helping fintech startups and growth-stage technology firms build investor-ready security programs anchored in SOC 2, PCI DSS, ISO 27001, and responsible AI governance.

OUR VALUE PROPOSITION

SOC 2 TYPE II | PCI DSS | ISO 27001 | AI / ML GOVERNANCE

For fintech startups and growth-stage technology firms, compliance is not a back-office function — it is a growth enabler and a competitive weapon.

The regulatory environment for technology and fintech companies has never been more demanding or more consequential. Firms handling payment data, consumer financial information, and sensitive personal data face mandatory compliance obligations under PCI DSS, SOC 2, ISO 27001, and the California Privacy Rights Act (CPRA) frameworks that enterprise clients, institutional investors, and strategic partners increasingly require as a condition of doing business. A single compliance gap can cost a growth-stage company a critical enterprise contract, delay a funding round, or trigger a regulatory investigation that diverts leadership attention at the worst possible moment.

At the same time, fintech firms deploying artificial intelligence and machine learning in credit decisioning, fraud detection, risk scoring, and customer experience are operating in an environment where AI governance is rapidly moving from a best practice to a regulatory expectation. United Allied helps technology and fintech firms build compliance programs that are not just audit- ready today, but architecturally designed to scale with the business — eliminating the costly compliance rebuilds that typically occur at Series B, Series C, and enterprise market entry.

SOC 2 TYPE II | PCI DSS | ISO 27001 | CPRA | GDPR | NIST CSF | AI / ML GOVERNANCE | POPIA

01

Regulatory Compliance & Scalable Framework Alignment

Prove It to Investors. Prove It to Clients. Prove It to Regulators.

Fintech startups and technology firms operate in one of the most heavily scrutinized regulatory environments in the world. SOC 2 Type II has become the de facto standard for demonstrating security and operational integrity to enterprise buyers with most Fortune 500 procurement processes now requiring it as a baseline. PCI DSS compliance is mandatory for any organization that stores, processes, or transmits payment card data, with non-compliance exposing firms to significant fines, transaction processing suspension, and breach liability. ISO 27001 certification provides the internationally recognized Information Security Management System (ISMS) framework that satisfies regulatory bodies, institutional investors, and enterprise clients across global markets simultaneously.

The California Privacy Rights Act (CPRA) extends and strengthens CCPA protections — establishing new rights for California consumers around sensitive personal information, data minimization, and purpose limitation that apply to any fintech firm with California-based users regardless of where the company is headquartered. For firms with European users or operations, GDPR adds a further layer of data subject rights, consent management, and cross-border transfer obligations. Managing these overlapping frameworks independently is inefficient and expensive — United Allied designs unified compliance architectures that satisfy multiple regulatory regimes through a single, coherent control environment, eliminating duplication and dramatically reducing the ongoing cost of compliance.

Our approach is built for growth-stage firms specifically. We design compliance programs that are proportionate to your current size, architecturally ready for your next stage, and structured to accelerate — not obstruct — your enterprise sales motion and fundraising process.

CORE DELIVERABLES:

- SOC 2 Type II readiness & audit preparation
- PCI DSS gap analysis & compliance roadmap
- ISO 27001 certification readiness
- Regulatory gap assessments
- Compliance training programs
- CPRA compliance program development
- GDPR & cross-border data transfer advisory
- Multi-framework unified control environment
- Policy development & management
- Ongoing regulatory monitoring & change management

02

AI / ML Governance & Responsible Innovation

Build AI That Regulators, Investors, and Customers Can Trust.

Artificial intelligence and machine learning have become central to the fintech value proposition — powering credit scoring models, fraud detection systems, automated underwriting, customer risk profiling, and personalized financial products. But the same capabilities that create competitive advantage also create significant regulatory, reputational, and operational risk. Algorithmic bias in credit decisioning can constitute a violation of fair lending laws. Opaque AI models that cannot explain their outputs are increasingly incompatible with emerging regulatory frameworks across the U.S., EU, and global markets. A model failure in a high-stakes financial decision can cause material harm to consumers and expose the firm to class-action litigation, regulatory investigation, and lasting reputational damage.

The regulatory landscape for AI in financial services is moving quickly. The EU AI Act establishes a risk-based framework that classifies AI systems used in credit scoring, insurance, and financial services as high-risk — subject to mandatory conformity assessments, transparency requirements, human oversight obligations, and ongoing monitoring. In the U.S., the Consumer Financial Protection Bureau (CFPB) and Federal Trade Commission (FTC) have both issued guidance on algorithmic fairness and explainability requirements. NIST's AI Risk Management Framework (AI RMF) provides the governance structure that organizations can use to demonstrate responsible AI practices to regulators and investors alike.

United Allied's AI/ML governance practice helps fintech firms build the policies, processes, and technical controls needed to deploy AI responsibly and defensibly. We conduct model risk assessments, develop AI governance frameworks aligned to the NIST AI RMF and EU AI Act requirements, implement bias detection and fairness evaluation processes, and establish the documentation and audit trail that regulators and investors require. AI governance is rapidly becoming a diligence requirement in fundraising — firms that build it early turn it into a competitive differentiator rather than a remediation project.

CORE DELIVERABLES:

- AI / ML risk assessment & model inventory
- NIST AI RMF governance framework alignment
- AI governance policy development
- AI audit trail & evidence management
- Ongoing model monitoring framework
- EU AI Act readiness assessment
- Algorithmic bias & fairness evaluation
- Model explainability & transparency documentation
- Responsible AI training programs
- Investor-ready AI governance documentation

03

GRC Program Build-Out for Growth-Stage Fintechs

Compliance That Scales With Your Ambition.

Most fintech startups encounter compliance as a crisis rather than a strategy — scrambling to meet SOC 2 requirements ahead of an enterprise deal, rebuilding security programs before a Series B audit, or retroactively addressing regulatory gaps after an incident. The cost of reactive compliance is significant — not just financially, but in leadership time, engineering resources, and deal velocity. United Allied helps growth-stage fintech firms break this cycle by building GRC programs that are designed from the outset to scale with the business, satisfy multiple stakeholder requirements simultaneously, and eliminate the expensive compliance rebuilds that occur at every growth inflection point.

Our GRC program build-out practice embeds governance, risk management, and compliance architecture directly into your operating model — not as an overlay, but as an integrated capability. We establish the risk management frameworks, control libraries, audit management processes, and continuous monitoring capabilities that enterprise clients require in vendor due diligence and that institutional investors scrutinize in security diligence. For firms with vCISO needs, we provide senior security leadership on a fractional basis — bringing board-level cybersecurity strategy without the cost of a full- time executive hire.

For fintech firms with international ambitions — including expansion into African markets where mobile money, digital lending, and embedded finance are growing at extraordinary rates — we design compliance architectures that accommodate multi-jurisdictional regulatory requirements from the outset, satisfying POPIA, GDPR, and local central bank frameworks without requiring separate compliance programs for each market.

CORE DELIVERABLES:

- GRC program architecture & build-out
- vCISO advisory services
- Enterprise risk management planning
- Third-party & vendor risk management
- Incident response planning
- Business continuity & disaster recovery planning
- Security architecture review
- Audit management
- Security awareness training
- Continuous compliance monitoring dashboards
- Investor-ready security posture documentation
- Multi-jurisdictional compliance framework design

FRAMEWORKS & STANDARDS WE WORK WITH

SOC 2 Type II | PCI DSS | ISO 27001 | CPRA | GDPR | NIST AI RMF | EU AI Act | NIST CSF

Built to Scale. Designed to Last.

Contact United Allied to discuss how we can help your fintech or technology firm build a compliance program that accelerates growth, satisfies investors, and stays ahead of the regulatory curve.