United Allied
Global Risks & Security Solutions

GRC & CYBERSECURITY SOLUTIONS OVERVIEW

Critical Infrastructure

Securing the systems society depends on — from energy grids and telecommunications networks to industrial control systems — through institutional-grade GRC and cybersecurity advisory built for Africa's infrastructure transformation.

OUR VALUE PROPOSITION

NIS2 ALIGNED | ISO 27001 | OT / ICS SECURITY | AFRICA INFRASTRUCTURE

Africa's critical infrastructure is at a pivotal moment — and the consequences of getting security wrong extend far beyond financial loss.

With Africa's cybersecurity market expanding at 13.5% CAGR through 2030 and 80% of businesses already facing active cyber threats, the continent's energy grids, telecommunications networks, financial systems, and industrial facilities require comprehensive, sector-specific risk and compliance strategies. Nation-state actors, ransomware syndicates, and sophisticated threat groups are actively targeting operational technology environments — systems that were never designed with cybersecurity in mind and cannot be easily patched without disrupting critical services.

United Allied delivers integrated GRC and cybersecurity solutions purpose-built for critical infrastructure operators combining deep regulatory expertise across NIS2, ISO 27001, NERC CIP, and Africa-specific frameworks with proven advisory capabilities that protect both the operational technology that runs these systems and the governance structures that oversee them.

NIS2 DIRECTIVE | ISO 27001 | ISO 27011 | NERC CIP | NIST 800-82 | ISA/IEC 62443 | POPIA | SARB / CBN

01

Regulatory Compliance & NIS2 / ISO 27001 Framework Alignment

Know the Rules. Validate Your Readiness.

Critical infrastructure operators across energy, telecommunications, banking, and digital infrastructure face an increasingly complex and rapidly evolving regulatory landscape. The NIS2 Directive raises the bar significantly for organizations operating essential services — establishing mandatory risk management measures, incident reporting obligations, and supply chain security requirements with significant penalties for non-compliance. For organizations seeking to validate their readiness, ISO 27001 certification provides the foundational Information Security Management System (ISMS) framework that maps directly to NIS2's core control requirements.

United Allied helps critical infrastructure organizations assess their current controls against NIS2 and ISO 27001 simultaneously — identifying gaps, building a prioritized remediation roadmap, and guiding the organization through certification. For telecommunications operators, ISO 27011 provides the sector-specific security controls that address the unique demands of network infrastructure protection. Across African markets, we layer these global frameworks against local regulatory requirements — SARB directives for banking, national telecommunications authority mandates, and energy sector compliance obligations — ensuring organizations satisfy both international standards and the jurisdictional frameworks that govern their operations.

Compliance with these frameworks is not simply a regulatory checkbox. It is a proactive measure that creates a more secure operating environment, improves internal processes, and demonstrates to clients, partners, and regulators that your organization takes infrastructure security seriously.

CORE DELIVERABLES:

- NIS2 Directive readiness assessment
- ISO 27001 certification readiness & gap analysis
- NIS2 + ISO 27001 unified compliance roadmap
- Policy development & management
- Compliance training programs
- ISO 27011 telecommunications security alignment
- Africa regulatory framework mapping (SARB, CBN, sector regulators)
- Regulatory change monitoring & impact assessment
- Audit management & certification preparation
- Supply chain & third-party compliance requirements

02

OT / ICS & Critical Asset Cybersecurity

Protect the Systems That Cannot Afford to Fail.

Operational technology environments — SCADA systems, industrial control systems, smart grids, and 5G network infrastructure — present a fundamentally different cybersecurity challenge than traditional IT environments. These systems were built for availability and reliability, not security. They often run legacy software that cannot be patched without operational disruption, operate on specialized industrial protocols, and increasingly converge with corporate IT networks in ways that create new and complex attack surfaces. Industrial downtime costs up to $125,000 per hour — and in critical infrastructure, the consequences extend far beyond financial loss to public safety and national security.

United Allied's OT and critical asset cybersecurity practice addresses these challenges through passive, non-disruptive assessment methodologies that provide full visibility into your operational technology environment without risking system availability. We evaluate your industrial control systems against NIST 800-82, ISA/IEC 62443, and NERC CIP standards identifying vulnerabilities, assessing network segmentation, reviewing access controls, and developing incident response capabilities specifically designed for OT environments. For telecommunications operators, we build security frameworks for 5G infrastructure, IoT device management, and network resilience. For energy and utility operators, we address smart grid cybersecurity, SCADA hardening, and the cyber-physical risks unique to power generation and distribution systems.

Beyond the technical assessment, we integrate findings into your broader compliance program — ensuring that operational technology security is not treated as a separate discipline but as a core component of your organization's enterprise risk posture.

CORE DELIVERABLES:

- OT / ICS vulnerability assessment (passive methods)
- SCADA hardening & anomaly detection advisory
- IT/OT convergence risk assessment
- Network segmentation & architecture review
- NERC CIP / NIST 800-82 / ISA IEC 62443 gap analysis
- 5G & network infrastructure security review
- IoT security governance framework
- Penetration testing & vulnerability management
- OT-specific incident response planning
- Smart grid cyber-physical security advisory

03

Africa Critical Infrastructure GRC & Resilience Advisory

Governance Built for Africa's Infrastructure Transformation.

Africa's critical infrastructure is undergoing its most significant transformation in a generation. With $4 trillion in domestic capital available for infrastructure development, the Mission 300 initiative targeting universal energy access by 2030, accelerating 5G rollout across the continent, and the rapid digitization of banking and financial services, the governance and risk management demands on infrastructure operators have never been greater. Regulatory bodies across energy, telecommunications, and financial services are raising their compliance expectations — and organizations that build robust GRC programs now will be best positioned to access capital, secure partnerships, and operate without regulatory disruption.

United Allied's GRC advisory practice provides the enterprise-wide governance framework that connects your operational technology security, regulatory compliance obligations, and organizational risk appetite into a coherent, board-level risk management program. We develop integrated risk management strategies, build executive dashboards and regulatory reporting capabilities, and establish the governance structures — policies, procedures, risk registers, and audit frameworks that enable your organization to demonstrate compliance to regulators, investors, and partners across multiple jurisdictions simultaneously.

With operational expertise across South Africa, Nigeria, Kenya, and broader African markets, we bring both the global standards fluency and the local regulatory knowledge required to build GRC programs that work in practice — not just on paper. Our Africa-U.S. corridor positioning means we understand the cross-border compliance obligations that face organizations operating across these markets, and we help clients build resilience programs that satisfy both local mandates and international investor expectations.

CORE DELIVERABLES:

- GRC program architecture & build-out
- Enterprise risk management planning
- Board-level risk reporting & executive dashboards
- Africa market regulatory compliance strategy
- Business continuity & resilience planning
- Security architecture review
- vCISO advisory services
- Audit management
- Security awareness training
- Continuous compliance monitoring dashboards
- Investor-ready security posture documentation
- Cross-border compliance framework advisory

FRAMEWORKS & STANDARDS WE WORK WITH

NIS2 | ISO 27001 | ISO 27011 | NERC CIP | NIST 800-82 | IEC 62443 | NIST CSF | POPIA

Empowering Resilience. Securing Africa's Future.

Contact United Allied to discuss how we can strengthen your critical infrastructure security posture and compliance program across global and emerging markets.