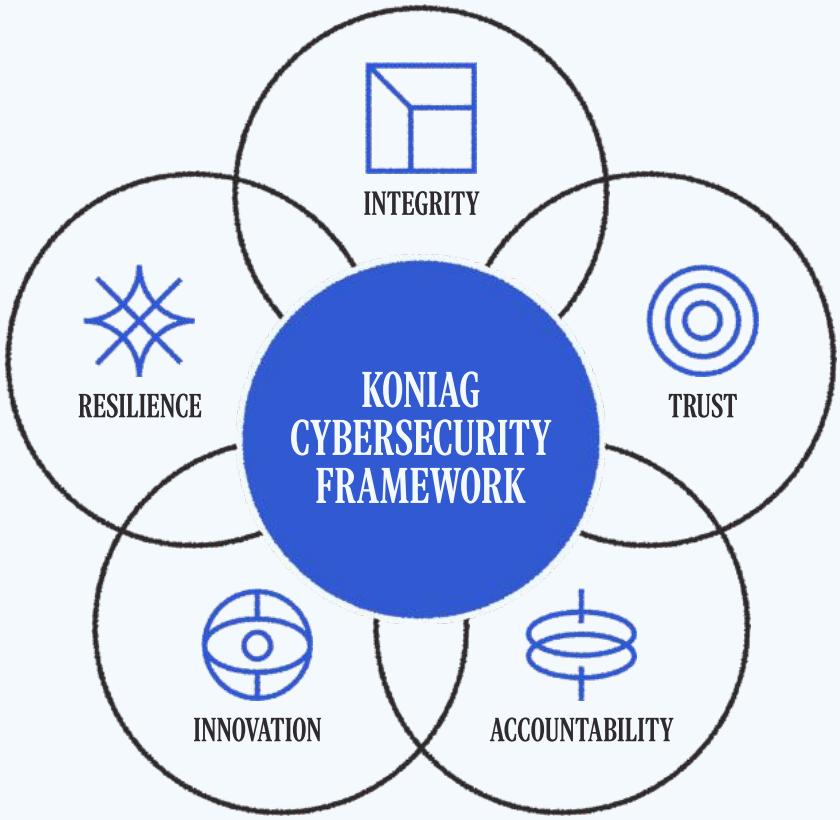
KONIAG CYBERSECURITY FRAMEWORK

Building Trust, Resilience, and Innovation

At Koniag Cyber, our cybersecurity framework is rooted in our core values: Integrity, Trust, Accountability, Innovation, and Resilience.

These principles shape how we protect our clients while aligning with our core service offerings — Assessment, Prevention, Detection, Response, Recovery, and Compliance. This integration ensures every engagement reflects our values while delivering measurable business outcomes.



INTEGRITY

We stand by our clients when it matters most.

VALUE CONNECTION

- Conduct IR readiness reviews, tabletop exercises, and develop tailored playbooks.
- Provide rapid containment, forensic investigation, and root cause analysis.
- Deliver trusted recovery through AD restoration, ransomware negotiation support, and continuity planning.

CORE SERVICE TIE-IN

- **Response:** Incident Response as a Service (IRaaS), ransomware negotiation, breach containment.
- **Recovery:** AD forest recovery, disaster recovery/business continuity planning.

FRAMEWORK OUTCOMES

Confidence in responding to and recovering from incidents.

TRUST

Trust begins with visibility. We provide clients with clear insight into their risks.

VALUE CONNECTION

- Identify and prioritize critical business assets.
- Map data flows, dependencies, and external exposure points.
- Model adversary tactics, techniques, and procedures (TTPs) to simulate real-world threats.

CORE SERVICE TIE-IN

- **Assessment:** Threat modeling, penetration testing, supply chain risk assessments.
- **Compliance Readiness:** Risk assessments aligned to NIST, ISO, HIPAA, and CMMC.

FRAMEWORK OUTCOMES

Clear visibility into risks and assurance of defenses.

ACCOUNTABILITY

Transparency and accountability are central to how we operate.

VALUE CONNECTION

- Implement continuous compliance monitoring (NIST, ISO, PCI, HIPAA, CMMC).
- Automate control validation with executive and regulatory dashboards.
- Perform supply chain and third-party risk assessments to extend accountability across the ecosystem.

CORE SERVICE TIE-IN

- **Compliance:** Continuous compliance monitoring, regulatory audits, SBOM validation.
- **Governance:** Security program development, secure configuration management, executive dashboards.

FRAMEWORK OUTCOMES

Transparent, measurable compliance posture.

INNOVATION

Innovation drives proactive defense and future-readiness.

VALUE CONNECTION

- Leverage AI-powered threat hunting and analytics for proactive detection.
- Integrate global and regional threat intelligence feeds.
- Adapt defenses to local environments (e.g., addressing elevated risks in China).

CORE SERVICE TIE-IN

- **Detection:** MDR, EDR/XDR deployment, SIEM tuning, and 24/7 SOC support.
- **Threat Intelligence:** Global and regional intelligence feeds, behavioral analytics, China-specific fraud detection.

FRAMEWORK OUTCOMES

Future-ready defenses against evolving cyber threats.

RESILIENCE

Resilience reflects our commitment to safeguard people and systems.

VALUE CONNECTION

- Harden infrastructure, applications, and identity systems (Zero Trust, AD, and cloud environments).
- Build human resilience with role-based awareness training, phishing simulations, and security culture initiatives.
- Ensure least-privilege access and continuous authentication.

CORE SERVICE TIE-IN

- **Prevention:** Zero Trust architecture design, IAM/PAM solutions, OT/ICS hardening, cloud security posture management.
- **Human Resilience:** Insider threat reduction and tailored security training

FRAMEWORK OUTCOMES

Strengthened security across people, processes, and technology.

We help our clients be foundationally prepared and ahead of next-generation threats

Let's get started at koniagcyber.com/contact