KGMM

PRACTICE BRIEF

STRATEGIC ADVISORY & EXECUTION

Cybersecurity Core

Security strategy, testing, and readiness aligned with what matters most to your business.

THE BUSINESS CHALLENGE

Security priorities compete for attention while technology, threats, and business expectations change. Leaders need a clear view of risk and a practical path from decisions to delivery.

OUR APPROACH

Clarify critical assets and business priorities. Assess relevant controls, test agreed scenarios, and translate findings into an owned, sequenced improvement plan.

SERVICES IN THIS PRACTICE

Incident Response & Readiness

Prepare escalation paths, exercise response plans, and coordinate recovery responsibilities.

AI Security & Governance

Connect AI use cases, access, oversight, and practical security controls.

Targeted Attack Testing

Use authorized adversary simulations to evaluate how important defenses work together.

Cyber Risk Management

Connect risk scenarios and uncertainty to leadership and investment decisions.

Cybersecurity Transformation

Define the operating model, roadmap, ownership, and measures for security change.

Cloud Security & Posture

Align cloud configuration, identity, data protection, and operational ownership.

TYPICAL ENGAGEMENT OUTPUTS

- Prioritized risk and control findings
- Response plans and exercise outcomes
- Security roadmap with accountable owners
- Agreed governance and operating controls

Request a consultation

Explore this practice online

Incident response availability and service levels are agreed directly; the website is not an emergency hotline.