

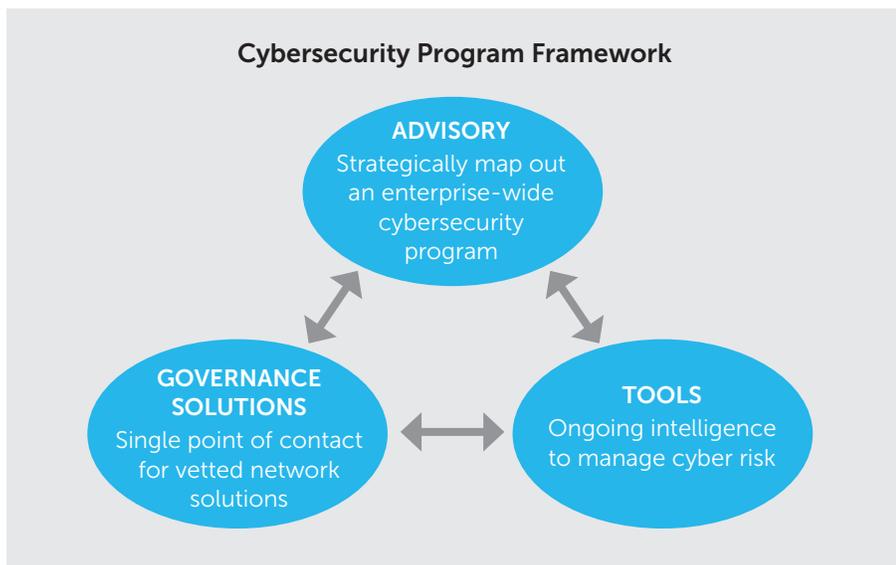
Cybersecurity Program

The increasing frequency of cyber incidents has significantly elevated the threats to companies, and as a result, solution providers are upping their game and regulators are sharpening their focus on cybersecurity preparedness.

But the cyber threat to companies is not a regulatory or technology issue — it's an enterprise-level **corporate governance** issue. As such, strong risk management controls are critical to ensuring that information about cyber risks and incidents reaches senior management, the board, and investors.

RANE's program includes:

- **Advisory services to map out and implement an enterprise-wide cybersecurity program**, with active and ongoing stewardship by RANE subject matter experts.
- **A range of cyber governance solutions**, with the ability to tap into a global network of credentialed cybersecurity service providers to save you time and effort.
- **Tools that provide ongoing intelligence to manage cyber risk** and keep pace with emerging threats, rapidly advancing technology, and the latest regulations.



The RANE Approach

RANE's comprehensive program leverages our in-house experience combined with access to a global network of cyber experts and service providers.

Cybersecurity as a corporate governance issue

Strategic analysis and recommendations to ensure up-to-date policies, procedures, and controls.

Focus on cyber resiliency and preparedness

Access to world-class cyber experts and information on cybersecurity risk, technology advancements, and regulatory trends.

Active and ongoing stewardship by RANE subject matter experts

A provider-agnostic partner to help you navigate the cybersecurity landscape.

Program Details

RANE’s modular approach provides you with the flexibility to customize a program specific to your needs.

Advisory	Governance Solutions	Tools
<ul style="list-style-type: none"> • Cyber Assessment, Gap Analysis, & Roadmap Comprehensive assessment and deployment plan covering legal, policy, and technical aspects of cybersecurity with roadmap for execution on where to invest time and resources. • Information Security Policy Review of current policies and written recommendations. Best practices on how to disseminate the policy to workforce and training techniques • Executive/Board Reporting & Briefings Develop a framework for presenting to senior leadership, including briefing and presentation support. 	<ul style="list-style-type: none"> • Data Management Perform data identification, mapping, compartmentalization, and classification. Assist in selecting products for data governance. • Incident Response Plan & Tabletop Exercise A written plan customized to your organizational priorities and needs and designed to synchronize all existing policies or playbooks. Tabletop exercise with customized scenario, RANE proctor, and written after action report. • Forensic Evaluation & Remediation Team On-demand incident response team to conduct forensics and remediate an incident at your site. 	<ul style="list-style-type: none"> • Regulatory Guidance State, federal, and international regulatory guidance, trend analysis, and interpretation related to cybersecurity, including suggestions for compliance. • Cyber Risk Monitoring & Analysis Ongoing source of relevant intelligence on cyber threat landscape, technology, and vendors and the implications to your organization. • Vendor Evaluation, Referral, & Response Provider-agnostic sourcing and vetting of cybersecurity and information technology vendors to get you the best solution for your needs.

SAMPLE PROGRAM: Year 1 Focuses on Building Out Your Program; Year 2 Focuses on Maintaining It



Ongoing: Information tying together implications of current and impending cyber regulations, cyber threat landscape, and technology. Ad-hoc research support on cybersecurity issues.