vedapraxis
Indonesia - Vietnam - Malaysia

Dukungan *Security Governance,* Keamanan Siber yang Relevan dan Solutif

Di era digital saat ini, teknologi informasi menjadi aspek utama dalam aktivitas operasional Bank. Keamanan siber menjadi landasan yang krusial dalam mendukung kelangsungan bisnis, perlindungan aset, dan menjaga kepercayaan Nasabah. Tantangan keamanan, terutama dalam bentuk ancaman siber akan semakin kompleks. Dalam konteks ini, dukungan security governance dan keamanan siber bukan lagi sekadar pilihan, melainkan suatu kebutuhan mendesak yang memerlukan strategi holistik dan solutif untuk keberlangsungan bisnis, integritas, dan kepercayaan Nasabah.

Seiring dengan kemajuan teknologi, munculnya regulasi yang lebih ketat, dan ancaman siber yang semakin canggih, pelindungan terhadap informasi menjadi prioritas utama bagi para Stakeholder. Kelangsungan bisnis, reputasi, dan kepercayaan Nasabah bergantung pada kemampuan kita untuk melindungi informasi dari ancaman siber yang terus berkembang.

Pentingnya memiliki kerangka kerja security governance yang kokoh, kebijakan keamanan siber yang proaktif merupakan kunci utama untuk menciptakan pertahanan yang tangguh dan berkelanjutan terhadap ancaman yang dapat merugikan Bank. Namun, menghadapi lingkungan dari ancaman yang dinamis, diperlukan pendekatan yang relevan dan adaptif. Veda Praxis siap mendampingi Bank dalam strategi penerapan security governance, bukan hanya untuk memitigasi risiko keamanan yang ada, namun juga dapat menggali potensi inovasi dalam keamanan siber dan membangun kepercayaan dalam ekosistem digital.

Layanan Veda Praxis dalam Digital GRC:

Security Governance

1. **Penyusunan tata kelola Keamanan Siber dan Risiko TI (kerangka kerja, kebijakan dan prosedur)**
   Membantu penyusunan pedoman dan panduan operasi dalam penerapan keamanan siber dan pengelolaan risiko TI.
2. **Layanan Manajemen Keamanan TI (IT Security Managed Service, seperti SIEM, DLP, PAM, IAM, dll)**
   Membantu Bank untuk mengelola aspek-aspek keamanan TI Perusahaan. Layanan ini dapat mencakup aktivitas yang dirancang untuk melindungi, mendeteksi dan me-respon ancaman keamanan siber, serta memastikan kepatuhan terhadap regulasi, kebijakan dan prosedur yang berlaku.
3. **Manajemen Risiko Pihak Ketiga**
   Membantu Bank untuk mengidentifikasi, menilai dan mengelola risiko yang terkait dengan keterlibatan pihak ketiga.
4. **Review Kepatuhan Atas Regulasi yang Berlaku Terkait Keamanan Siber dan Risiko TI**
   Melakukan pemeriksaan/ audit secara menyeluruh atas kepatuhan penerapan keamanan siber.

Keamanan Siber

1. **Asesmen Teknologi dan Keamanan Siber *(penetration test, vulnerability assessment)***
   Penetration test - melakukan simulasi serangan siber untuk menguji sejauh mana sistem Bank dapat bertahan terhadap upaya peretasan.
   Vulnerability assessment – melakukan identifikasi kerentanan yang mungkin ada dalam sistem atau jaringan Bank.
2. ***Source code review***
   Melakukan pemeriksaan dan evaluasi secara sistematis terhadap source code aplikasi. Pemeriksaan dilakukan untuk mengidentifikasi dan memperbaiki kerentanan keamanan, kesalahan pemrograman, dan memastikan kepatuhan terhadap standar pengkodean.
3. ***Red Team Services***
   Mensimulasikan ancaman dan serangan siber terhadap sistem, jaringan maupun aplikasi yang digunakan oleh Bank. Tujuan dari layanan ini adalah untuk mengindentifikasi kerentanan, kelemahan dan potensi celah keamanan pada sistem Bank.
4. **Konsultansi terkait Manajemen Insiden dan Krisis Keamanan Siber**
   Membantu Bank dalam mengembangkan rencana tanggap darurat untuk menghadapi pelanggaran atau insiden keamanan informasi / keamanan siber. Menyusun panduan dalam menangani insiden keamanan informasi/ keamanan siber.
5. **Pelatihan Teknis Terkait Keamanan Siber**
   Memberikan pelatihan teknis mengenai pengelolaan keamanan siber.

AD Premier Office Park, 8th floor
Jl. TB. Simatupang No. 5 Ragunan Kec. Pasar Minggu, Jakarta 12540
Telp. 021 2270 8982, email: info@vedapraxis.com, website: www.vedapraxis.com