Manajemen Risiko pada Bank Syariah

Oleh M. Jusuf Wibisana
Ketua KASy IAI

Struktur Dasar	Dewan Komisaris dan Komite-komite
	Dewan Direksi
	Dewan Pengawas Syariah

Kategori Risiko

- Risiko Kredit
- Risiko investasi ekuitas
- Risiko pasar
- Risiko likuiditas
- Risiko tingkat imbalan
- Risiko operasi
- Risiko IT
- Risiko kepatuhan

Risiko Kredit

Risiko nasabah pembiayaan gagal memenuhi kewajibannya sesuai dengan akad - Institusi Bank Syariah (IBS) risiko kredit yang melekat pada pembiayaan dan investasi ekuitasnya untuk menghindari atau mitigasi kerugian karena penurunan kualitas pembiayaan dan default, dan penurunan bagi hasil. IBS juga merencanakan dan mengendalikan proses bagi hasil dan menghindari konsentrasi risiko

Risiko Kepatuhan pada Regulasi dan Ketentuan Syariah

IBS teregulasi secara ketat sebagai institusi perbankan dan sekaligus institusi syariah. Ke tidak patuhan pada regulasi dan ketentuan bisa berdampak pada sanksi dari regulator, berkurangnya kepercayaan nasabah, penurunan laba, dan penurunan reputasi IBS.

Risiko IT

- IT adalah *back bone* dari bank
- IT dependency akan semakin tinggi untuk memulai transaksi, otorisasi, pengendalian, processing dan pelaporan (*reporting*).
- IT Strategy dan IT Governance harus baik.

Risiko TI pada Bank Syariah

Bank syariah sangat bergantung pada infrastruktur, sistem, dan pengendalian TI untuk mendukung kegiatan operasional sehari-hari dan proses pelaporan keuangan. Lingkungan TI Bank merupakan sistem yang kompleks dikarenakan jumlah dan kompleksitas dari sistem yang digunakan dan adanya *interface* antar sistem. Sehingga pengoperasian dan kontrol atas teknologi informasi Bank merupakan hal yang sangat penting dalam manajemen risiko.

Pengendalian Umum TI

- Akses ke program dan data
- Perubahan program
- Pengembangan program
- Operasional TI

What can go wrong jika pengendalian TI tidak berjalan?

1. Kapasitas server tidak memadai menyebabkan transaksi terhambat
2. Serangan siber dari pihak luar
3. *Maintenance* data dan system tidak sesuai prosedur
4. Kapasitas SDM TI team tidak memadai
5. Penggunaan infrastruktur TI yang tidak update (contoh tidak update antivirus, penggunaan windows yang lama)

What should we do?

1. Analisis secara berkala volume transaksi dan kebutuhan kapasitas server dan perangkat pendukung TI lainnya.
2. Melakukan simulasi switch DC DRC secara regular.
3. Meningkatkan ketahanan siber dengan menggunakan software terbaru.
4. Melakukan simulasi serangan siber untuk mengetahui celah pada system TI yang dapat diserang.
5. Memastikan Bank memiliki catatan arsitektur TI yang mecatat *mapping* program, system, dan penyimpanan data
6. Memastkan infrastruktur TI telah update dengan teknologi terbaru.