

L4D.1 — Kustodi dan Regulasi Aset Digital

Kurikulum Invesmentpedia · Level 4 Profesional · Rumpun D (Aset Digital) · Modul 1

Invesmentpedia

2026

Daftar Isi

- L4D.1 — Kustodi dan Regulasi Aset Digital
 - - 1. Identitas Modul
 - 2. Capaian Pembelajaran Mata Kuliah (CPMK)
 - 3. Peta Konsep
 - 4. Materi
 - 5. Contoh Terhitung
 - 6. Lembar Kerja Peserta
 - 7. Bank Soal
 - 8. Rubrik Penilaian
 - 9. Panduan Fasilitator
 - 10. Penafian

L4D.1 — Kustodi dan Regulasi Aset Digital

1. Identitas Modul

1.1 Batas kompetensi — dibaca sebelum apa pun yang lain

Modul ini tidak memberikan nasihat hukum dan tidak melatih peserta untuk memberikannya.

Regulasi aset digital di Indonesia dan di hampir seluruh yurisdiksi lain **berubah cepat**. Kewenangan pengawasan, kewajiban perizinan, perlakuan pajak, dan status hukum kepemilikan aset digital telah berubah beberapa kali dalam beberapa tahun terakhir dan dapat berubah lagi sebelum peserta menyelesaikan modul ini.

Karena itu modul ini mengajarkan pertanyaan yang harus diajukan, bukan jawaban yang berlaku hari ini.

Yang diajarkan modul ini	Yang tidak diajarkan
Struktur risiko kustodi dan cara mengukurnya	Apakah penyedia tertentu aman atau patuh
Pertanyaan yang menentukan posisi hukum Anda	Jawaban atas pertanyaan itu
Mengapa segregasi menentukan pemulihan	Status hukum aset Anda pada penyedia tertentu
Cara memverifikasi klaim penyedia	Bahwa klaim penyedia tertentu benar

Aturan yang berlaku bagi peserta dan fasilitator:

Setiap pertanyaan tentang status hukum, kewajiban perizinan, perlakuan pajak, atau hak kepemilikan atas aset digital wajib dirujuk kepada penasihat hukum berizin di yurisdiksi yang relevan — termasuk pertanyaan yang tampak sederhana, dan termasuk permintaan “pendapat sementara”.

Batas ini identik dengan yang berlaku pada **L4A.2 §1.1**, dan berlaku dengan alasan yang sama: memberikan pendapat di luar kompetensi berizin merugikan penerimanya justru ketika ia paling mempercayainya.

1.2 Identitas

Atribut	Keterangan
Kode	L4D.1
Nama	Kustodi dan Regulasi Aset Digital
Jenjang	Level 4 — Profesional
Rumpun	D — Aset Digital
Beban	16 JP (13 jam 20 menit) — 5 JP teori, 7 JP praktik, 4 JP asesmen
Prasyarat	L4.2; L4Q.2; L2I.5
Pilar	P5 Risiko (dominan), P6 Operasional, P3 Etika & Kepatuhan
CPL terkait	CPL-5, CPL-6, CPL-7, CPL-8, CPL-9
Kanon	K-02, K-06, K-09, K-10, K-12

Tesis modul. Kriptografi yang mengamankan aset digital **tidak dapat ditembus dengan kekuatan komputasi** — menebak satu frasa pemulihan 12 kata memerlukan waktu $7,7 \times 10^8$ kali umur alam semesta.

Karena itu setiap kerugian nyata bersifat operasional atau hukum, bukan kriptografis.

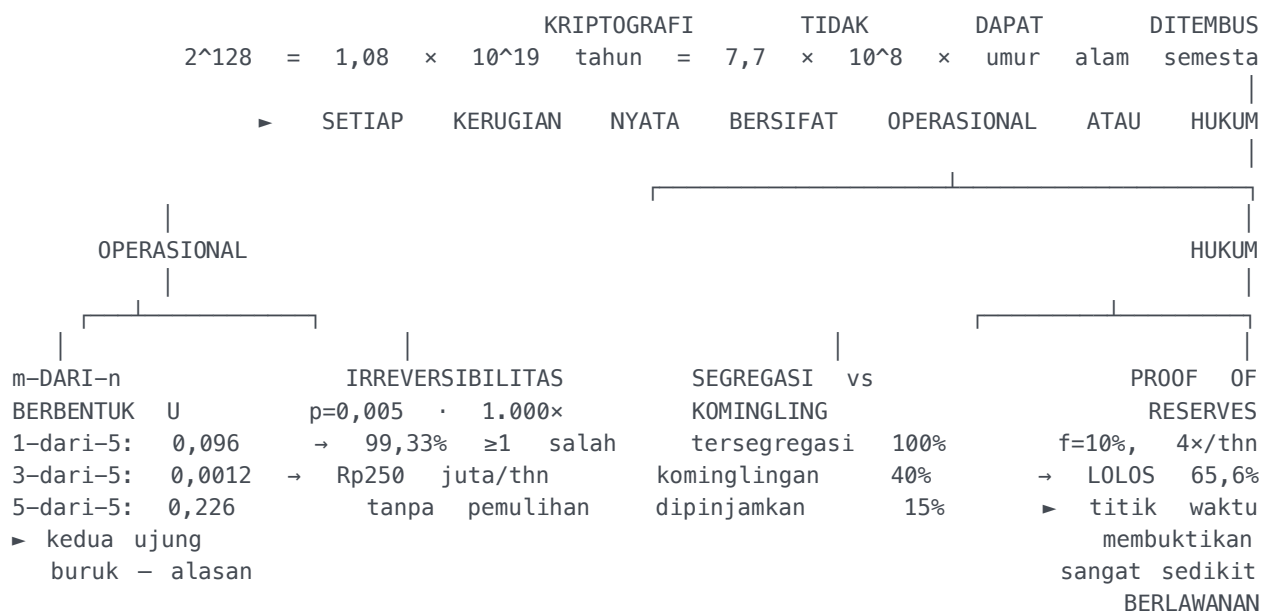
Modul ini adalah tentang dua sumber kerugian yang sebenarnya itu.

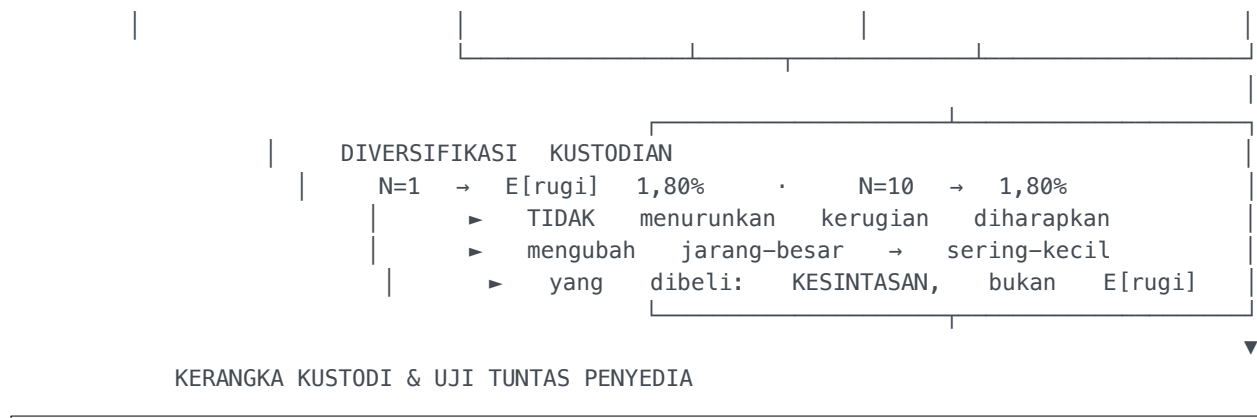
2. Capaian Pembelajaran Mata Kuliah (CPMK)

Kode	Rumusan CPMK	Bloom
CPMK-L4D.1.1	Menyatakan batas kompetensi dan	C3

Kode	Rumusan CPMK	Bloom
	merujuk pertanyaan hukum kepada pihak berizin	
CPMK-L4D.1.2	Menghitung peluang kehilangan dan pencurian pada skema <i>m</i> -dari- <i>n</i>	C4
CPMK-L4D.1.3	Menjelaskan mengapa kedua ujung spektrum <i>m</i> -dari- <i>n</i> buruk, dan mengapa karena alasan berlawanan	C5
CPMK-L4D.1.4	Menilai secara kritis apa yang dibuktikan dan tidak dibuktikan oleh <i>proof of reserves</i>	C5
CPMK-L4D.1.5	Membedakan segregasi dan kominglingan serta akibatnya pada pemulihan	C4
CPMK-L4D.1.6	Menghitung akibat diversifikasi kustodian secara benar	C5
CPMK-L4D.1.7	Menentukan alokasi <i>hot/cold</i> dari kerugian yang diharapkan	C5
CPMK-L4D.1.8	Menyusun Kerangka Kustodi dan Daftar Uji Tuntas Penyedia	C6

3. Peta Konsep





4. Materi

4.1 Mengapa kriptografi bukan mata rantai terlemah

Frasa pemulihan BIP39 dengan 12 kata memuat **128 bit entropi**:

$$2^{128} = 3,403 \times 10^{38} \text{ kemungkinan}$$

Pada laju penembakan **satu triliun per detik** — jauh melampaui yang tersedia bagi penyerang mana pun:

$$\frac{3,403 \times 10^{38}}{10^{12}} = 3,403 \times 10^{26} \text{ detik} = 1,08 \times 10^{19} \text{ tahun}$$

$$\frac{1,08 \times 10^{19}}{1,4 \times 10^{10}} = 7,7 \times 10^8 \text{ kali umur alam semesta}$$

Kesimpulannya bukan “aset digital aman”. Kesimpulannya jauh lebih berguna:

Karena kriptografinya tidak dapat ditembus, setiap kerugian nyata terjadi melalui jalur lain — kesalahan operasional, kegagalan penyimpanan kunci, penipuan, atau kegagalan hukum pihak yang memegang aset atas nama Anda.

Ini mengubah ke mana perhatian harus diarahkan. Perdebatan tentang kekuatan algoritma hampir selalu salah sasaran. Empat jalur di bawah inilah yang menghabiskan aset:

Jalur	Dibahas pada
Kunci hilang atau dicuri	§4.2
Transaksi salah yang tidak dapat dibatalkan	§4.3
Pihak yang memegang aset gagal	§4.4–4.5
Klaim cadangan yang tidak terverifikasi	§4.6

K-10 — jika kedengarannya terlalu bagus untuk jadi kenyataan. Penyedia yang menjual “keamanan tingkat militer” menjawab persoalan yang tidak pernah menjadi masalah, sambil tidak menjawab keempat jalur di atas.

4.2 Skema m -dari- n berbentuk U

Kunci tunggal menghadapi dua risiko yang **saling berlawanan arah**:

Risiko	Cara menguranginya
Kehilangan — kunci rusak, hilang, pemiliknya meninggal	Perbanyak salinan
Pencurian — kunci dikuasai penyerang	Kurangi salinan

Skema m -dari- n memisahkan kendali ke n kunci dan memerlukan m di antaranya untuk bertransaksi. Dengan peluang satu kunci **hilang** 5% per tahun dan satu kunci **dikuasai penyerang** 2% per tahun:

Skema	$P(\text{hilang})$	$P(\text{dicuri})$	Total
1-dari-1	0,050000	0,020000	0,070000
1-dari-2	0,002500	0,039600	0,042100
1-dari-3	0,000125	0,058808	0,058933
2-dari-2	0,097500	0,000400	0,097900
2-dari-3	0,007250	0,001184	0,008434
2-dari-4	0,000481	0,002336	0,002818
3-dari-3	0,142625	0,000008	0,142633
3-dari-5	0,001158	0,000078	0,001236
4-dari-5	0,022593	0,000001	0,022593
4-dari-7	0,000194	0,000005	0,000199

Dan inilah hasil yang paling penting. Naikkan m pada $n=5$ dan perhatikan bentuknya:

Skema	$P(\text{hilang})$	$P(\text{dicuri})$	Total
1-dari-5	0,0000003	0,0960792	0,0960795
2-dari-5	0,0000300	0,0038424	0,0038724
3-dari-5	0,0011581	0,0000776	0,0012357
4-dari-5	0,0225925	0,0000008	0,0225933
5-dari-5	0,2262191	0,0000000	0,2262191

Kurvanya berbentuk U. Kedua ujungnya buruk, dan karena alasan yang berlawanan.

Ujung	Masalah	Besarnya
1-dari-5	Lima kunci, masing-masing cukup untuk mencuri	$P(\text{dicuri})$ 9,6%

Ujung	Masalah	Besarnya
5-dari-5	Satu kunci hilang menghanguskan seluruh aset	<i>P</i>(hilang) 22,6%
3-dari-5	Seimbang	Total 0,12%

5-dari-5 adalah 183 kali lebih buruk daripada 3-dari-5 — meskipun terdengar “paling aman”.

K-02 — keamanan bukan satu dimensi. Menambah syarat tidak selalu menambah keamanan. Pada 5-dari-5, syarat tambahan itu **menciptakan** risiko yang lebih besar daripada yang dihilangkannya.

Dan perhatikan perbandingan yang paling berguna bagi pemula:

	1-dari-1	2-dari-3	Perubahan
<i>P</i> (hilang)	0,050000	0,007250	−85,5%
<i>P</i> (dicuri)	0,020000	0,001184	−94,1%

Beralih dari 1-dari-1 ke 2-dari-3 menurunkan KEDUA risiko sekaligus. Ini jarang terjadi — biasanya keamanan dan kemudahan dipertukarkan. Di sini tidak.

Dan atas sepuluh tahun:

Skema	<i>P</i> (selamat 10 tahun)	<i>P</i> (kejadian)
1-dari-1	0,4840	51,60%
2-dari-3	0,9188	8,12%
3-dari-5	0,9877	1,23%

Kunci tunggal yang dipegang sepuluh tahun adalah lemparan koin.

4.3 Irreversibilitas

Transaksi aset digital **tidak dapat dibatalkan**. Tidak ada pihak yang berwenang membalikkannya, dan tidak ada prosedur banding.

Peluang setidaknya satu kesalahan alamat:

Laju kesalahan <i>p</i>	50 transaksi	200 transaksi	1.000 transaksi
0,0001	0,50%	1,98%	9,52%
0,001	4,88%	18,14%	63,23%
0,005	22,17%	63,30%	99,33%
0,01	39,50%	86,60%	~100%

Dan nilainya, pada kerugian rata-rata Rp50.000.000 per kesalahan:

<i>p</i>	Transaksi/tahun	Kesalahan/tahun	Kerugian yang diharapkan
0,001	200	0,20	Rp10.000.000
0,001	1.000	1,00	Rp50.000.000
0,005	200	1,00	Rp50.000.000
0,005	1.000	5,00	Rp250.000.000

Bandingkan dengan L4Q.2 §4.7. Di sana laju kesalahan yang sama menghasilkan 252 kesalahan per tahun — yang **terdeteksi dan diperbaiki** oleh rekonsiliasi harian.

Di sini tidak ada yang dapat diperbaiki. Perbedaannya bukan pada laju kesalahan; perbedaannya adalah rekonsiliasi hanya memberi tahu Anda bahwa uang sudah hilang.

Konsekuensi yang tidak dapat ditawar:

Pada sistem yang tidak dapat dibalikkan, seluruh pengendalian harus berada SEBELUM transaksi dikirim. Pengendalian setelahnya tidak ada gunanya.

Lima pengendalian pra-transaksi:

#	Pengendalian	Apa yang dicegah
1	Daftar alamat yang disetujui (<i>allowlist</i>) dengan jeda waktu untuk penambahan	Alamat penyerang, kesalahan ketik
2	Transaksi uji bernilai kecil sebelum pengiriman penuh	Alamat salah
3	Verifikasi alamat pada perangkat penanda tangan, bukan pada layar yang dapat dikompromikan	Penggantian alamat oleh perangkat lunak jahat
4	Persetujuan kedua untuk nilai di atas ambang	Kesalahan dan penyalahgunaan satu orang
5	Jeda wajib antara penyusunan dan pengiriman	Keputusan tergesa dan tekanan sosial

Butir 1 dan 5 menangani serangan yang paling sering berhasil: bukan serangan teknis, melainkan **tekanan waktu** — “kirim sekarang atau kesempatan hilang”. Jeda wajib menghilangkan seluruh kelas serangan itu dengan satu aturan.

4.4 Segregasi dan kominglingan

Ketika pihak yang memegang aset Anda gagal, yang menentukan berapa yang Anda dapatkan kembali bukanlah teknologinya — melainkan struktur hukum penyimpanannya.

Struktur	Pemulihan	Dari Rp100.000.000	Hilang
Tersegregasi dan teridentifikasi sebagai milik Anda	100%	Rp100.000.000	Rp0
Tersegregasi, tetapi catatan cacat	85%	Rp85.000.000	Rp15.000.000
Dikominglingkan — Anda kreditur umum	40%	Rp40.000.000	Rp60.000.000
Dikominglingkan dan sudah dipinjamkan	15%	Rp15.000.000	Rp85.000.000

(Tingkat pemulihan bersifat ilustratif; hasil sebenarnya bergantung pada hukum kepailitan yurisdiksi yang berlaku dan fakta setiap kasus.)

Selisih antara baris pertama dan baris terakhir adalah 85% dari aset Anda — dan tidak satu pun ditentukan oleh kekuatan kriptografi.

Tiga pertanyaan yang menentukan baris mana yang berlaku bagi Anda:

#	Pertanyaan	Mengapa menentukan
1	Apakah aset saya tercatat atas nama saya, atau atas nama penyedia?	Menentukan apakah Anda pemilik atau kreditur
2	Apakah penyedia berhak meminjamkan atau menjaminkan aset saya?	Menentukan apakah aset masih ada saat gagal
3	Dalam kepailitan, apakah aset saya masuk harta pailit?	Menentukan urutan Anda dalam antrean

Ketiga pertanyaan ini dijawab oleh dokumen hukum, bukan oleh materi pemasaran — dan jawabannya wajib diverifikasi oleh penasihat hukum berizin (§1.1).

Yang dapat Anda lakukan sendiri adalah mengajukannya secara tertulis dan menyimpan jawabannya. Penyedia yang tidak bersedia menjawab ketiganya secara tertulis telah memberi Anda informasi yang berguna.

4.5 Diversifikasi kustodian — dan apa yang sebenarnya dibelinya

Nasihat “jangan simpan semuanya di satu tempat” benar, tetapi alasan yang biasa diberikan untuknya keliru.

Dengan peluang satu kustodian gagal 3% per tahun dan pemulihan 40%:

N kustodian	$P(\geq 1 \text{ gagal})$	Kerugian bila 1 gagal	$E[\text{kerugian}]$
1	3,00%	60,0% modal	1,80% modal
2	5,91%	30,0% modal	1,80% modal
3	8,73%	20,0% modal	1,80% modal
5	14,13%	12,0% modal	1,80% modal
10	26,26%	6,0% modal	1,80% modal

Baca kolom terakhir. Kerugian yang diharapkan sama persis — 1,80% — berapa pun jumlah kustodian.

Dan kolom kedua bergerak ke arah yang salah: peluang mengalami setidaknya satu kegagalan **naik** dari 3,00% menjadi 26,26%.

Jadi apa yang sebenarnya dibeli oleh diversifikasi?

Diversifikasi kustodian tidak menurunkan kerugian yang diharapkan. Ia mengubah kerugian yang jarang dan besar menjadi kerugian yang sering dan kecil. Yang dibeli adalah KESINTASAN.

Dan kesintasan adalah hal yang benar untuk **dibeli**, karena kerugian 60% modal dapat mengakhiri kemampuan Anda melanjutkan, sementara kerugian 6% tidak — persis asimetri pemulihan yang diukur pada L3.3 §4.1.

Dua peringatan yang harus menyertainya:

Pertama, kolom kedua nyata. Dengan sepuluh kustodian Anda akan **mengalami** kegagalan lebih sering. Organisasi yang tidak siap secara operasional untuk itu akan menemukan bahwa diversifikasi memperbanyak krisis yang harus dikelola.

Kedua, dan lebih penting: perhitungan ini mengasumsikan kegagalan independen. Bila sepuluh kustodian menyimpan aset pada pihak ketiga yang sama, menggunakan bank yang sama, atau tunduk pada yurisdiksi yang sama, **mereka bukan sepuluh taruhan** — persis kekeliruan *breadth* semu pada L4Q.1 §4.2.

Uji yang benar bukan “berapa banyak kustodian saya”, melainkan “apa yang mereka miliki bersama”.

4.6 Proof of Reserves: apa yang dibuktikanannya

Proof of reserves (PoR) adalah upaya penyedia membuktikan bahwa ia memegang aset yang cukup. **Ia berguna, dan ia membuktikan jauh lebih sedikit daripada yang umumnya dipahami.**

Tiga hal yang harus dipisahkan:

Klaim	Dapat dibuktikan secara kriptografis?
Aset — penyedia menguasai alamat tertentu	Ya (tanda tangan)
Liabilitas — jumlah yang dimiliki seluruh nasabah	Sebagian (pohon Merkle; nasabah hanya dapat

Klaim	Dapat dibuktikan secara kriptografis? memverifikasi saldonya sendiri)
Tidak ada liabilitas tersembunyi	Tidak

Dan ada persoalan yang lebih mendasar: PoR adalah potret pada satu titik waktu.

Bila kekurangan cadangan ada selama fraksi f dari waktu, dan attestasi dilakukan K kali per tahun pada waktu yang tidak dapat diprediksi:

$$P(\text{terdeteksi}) = 1 - (1 - f)^K$$

f	$K=1$	$K=4$	$K=12$	$K=52$	$K=365$
5%	5,0%	18,5%	46,0%	93,1%	100,0%
10%	10,0%	34,4%	71,8%	99,6%	100,0%
25%	25,0%	68,4%	96,8%	100,0%	100,0%
50%	50,0%	93,8%	100,0%	100,0%	100,0%

Dibaca dari sisi yang lebih jujur — peluang LOLOS:

Keadaan	Peluang tidak terdeteksi
Kekurangan ada 5% waktu, attestasi triwulanan	81,5%
Kekurangan ada 10% waktu, attestasi triwulanan	65,6%
Kekurangan ada 25% waktu, attestasi triwulanan	31,6%
Kekurangan ada 10% waktu, attestasi bulanan	28,2%

Attestasi triwulanan terhadap kekurangan yang ada sepersepuluh waktu gagal mendeteksinya pada 81,5% kasus — dan itu **sebelum** memperhitungkan bahwa waktu attestasi sering diketahui sebelumnya.

Bila waktunya diketahui, peluang deteksi bukan 34,4% melainkan mendekati nol, karena cadangan dapat dipinjam untuk potret itu saja.

Empat pertanyaan yang membuat PoR bermakna:

#	Pertanyaan	Mengapa
1	Apakah liabilitas ikut dibuktikan, bukan hanya aset?	Aset tanpa liabilitas tidak membuktikan solvabilitas
2	Seberapa sering, dan apakah waktunya tidak dapat diprediksi?	§4.6; potret terjadwal mudah dipenuhi

#	Pertanyaan	Mengapa
3	Apakah auditor independen dan apakah laporannya lengkap?	Attestasi terbatas bukan audit
4	Apakah aset yang ditunjukkan dipinjam?	Alamat dapat dikuasai sementara

PoR yang tidak menjawab pertanyaan 1 dan 2 tidak boleh diperlakukan sebagai bukti solvabilitas. Ia adalah bukti bahwa penyedia menguasai sejumlah alamat pada satu saat.

4.7 Alokasi hot dan cold

Aset yang dapat diakses cepat (*hot*) menghadapi risiko kompromi jauh lebih tinggi daripada aset yang disimpan luring (*cold*).

Dengan peluang kompromi *hot* 8% per tahun dan *cold* 0,3% per tahun:

Proporsi <i>hot</i>	$E[\text{kerugian}]/\text{tahun}$	Per Rp1 miliar
100%	8,0000%	Rp80.000.000
50%	4,1500%	Rp41.500.000
20%	1,8400%	Rp18.400.000
10%	1,0700%	Rp10.700.000
5%	0,6850%	Rp6.850.000
2%	0,4540%	Rp4.540.000

Menurunkan proporsi *hot* dari 20% ke 5% memotong kerugian yang diharapkan sebesar 62,8%.

Dan inilah cara menentukan angkanya — bukan dengan menebak:

Proporsi *hot* ditentukan oleh kebutuhan likuiditas operasional, bukan oleh kenyamanan. Hitung kebutuhan penarikan atau transaksi harian Anda, tambahkan cadangan yang wajar, dan **sisanya wajib berada di *cold*.**

Setiap rupiah di *hot* yang melampaui kebutuhan operasional adalah biaya **8% per tahun** yang dibayar untuk kemudahan yang tidak dipakai.

4.8 Kerangka Kustodi dan Uji Tuntas Penyedia

KERANGKA KUSTODI — Templat

Bagian 1 — Batas kompetensi (§1.1) 1.1 ☐ Saya memahami modul ini tidak memberikan nasihat hukum 1.2 Penasihat hukum berizin yang saya rujuk: ____ 1.3 Pertanyaan hukum yang sudah dirujuk dan dijawab: ____ 1.4 ☐ Saya tidak akan memberikan pendapat hukum kepada siapa pun, termasuk “pendapat sementara”

Bagian 2 — Skema kunci 2.1 Skema yang dipakai: ____-dari-____ 2.2 $P(\text{hilang}) = \text{____} \cdot P(\text{dicuri}) = \text{____} \cdot \text{Total} = \text{____}$ 2.3 Bandingkan dengan 2-dari-3 (0,008434) dan 3-dari-5 (0,001236): ____ 2.4 $P(\text{kejadian dalam 10 tahun}) = 1 - (1 - \text{total})^{10} = \text{____}\%$ 2.5 ☐ Saya tidak memakai 1-dari-1 untuk nilai yang tidak sanggup saya hilangkan 2.6 ☐ Saya tidak memakai n -dari- n (lihat 5-dari-5: 0,2262) 2.7 **Di mana masing-masing dari n kunci berada, dan siapa yang tahu?** ____ 2.8 **Apakah dua kunci pernah berada di lokasi yang sama?** ☐ Tidak ☐ Ya → bukan n kunci

Bagian 3 — Pengendalian pra-transaksi (tidak dapat dibalikkan — §4.3)

#	Pengendalian	Aktif?	Ambang
1	Daftar alamat + jeda disetujui + jeda penambahan	☐	
2	Transaksi uji bernilai kecil	☐	
3	Verifikasi alamat pada perangkat penanda tangan	☐	
4	Persetujuan kedua di atas ambang	☐	
5	Jeda wajib antara penyusunan dan pengiriman	☐	

3.1 Laju kesalahan yang diamati $p = \text{____} \cdot \text{Transaksi/tahun} = \text{____}$ 3.2 $**E[\text{kesalahan/tahun}] = \text{____} \cdot E[\text{kerugian}] = \text{Rp} \text{____} **$ 3.3 ☐ Saya memahami rekonsiliasi hanya memberi tahu bahwa uang sudah hilang

Bagian 4 — Alokasi hot/cold 4.1 Kebutuhan likuiditas operasional harian: Rp____ · Cadangan: Rp_ 4.2 **Proporsi hot yang dibenarkan kebutuhan:** ____% 4.3 **Proporsi hot aktual:** _% · **Selisih:** ____% 4.4 $E[\text{kerugian}]$ pada proporsi aktual: ____%/tahun = Rp_ 4.5 $E[\text{kerugian}]$ pada proporsi yang dibenarkan: _%/tahun = Rp____ 4.6 $**\text{Biaya kemudahan yang tidak dipakai: Rp____/tahun} **$

Bagian 5 — Uji tuntas penyedia (satu lembar per penyedia)

Nama penyedia: ____ · Yurisdiksi: ____ · Tanggal uji tuntas: ____

#	Pertanyaan	Jawaban tertulis?	Isi
1	Aset tercatat atas nama siapa?	☐	
2	Berhak meminjamkan/menjamin aset saya?	☐	
3	Dalam kepailitan, masuk harta pailit?	☐	

#	Pertanyaan	Jawaban tertulis?	Isi
4	PoR: liabilitas ikut dibuktikan?	☐	
5	PoR: frekuensi dan apakah waktunya tak terduga?	☐	
6	Auditor independen? Laporan lengkap?	☐	
7	Status perizinan dan otoritas pengawas?	☐	
8	Asuransi: apa yang ditanggung, apa yang tidak?	☐	

5.1 **Pertanyaan yang TIDAK dijawab secara tertulis:** ____ 5.2 ☐ Saya memahami penolakan menjawab adalah informasi 5.3 Struktur pemulihan yang berlaku (§4.4): ☐ 100% ☐ 85% ☐ 40% ☐ 15% ☐ **tidak diketahui** 5.4 ☐ Jawaban 1–3 sudah diverifikasi penasihat hukum berizin

Bagian 6 — Diversifikasi 6.1 Jumlah kustodian: ____ · Proporsi pada masing-masing: ____ 6.2 $P(\geq 1 \text{ gagal/tahun}) = \text{____\%} \cdot E[\text{kerugian}] = \text{____\%}$ 6.3 ☐ Saya memahami $E[\text{kerugian}]$ **tidak berubah** dengan jumlah kustodian 6.4 **Apa yang dimiliki bersama oleh para kustodian saya?**

Dimensi	Bersama?	Rincian
Sub-kustodian / pihak ketiga	☐	
Bank	☐	
Yurisdiksi	☐	
Perusahaan induk / pemilik	☐	
Penyedia teknologi	☐	

6.5 **Jumlah kustodian yang benar-benar independen:** ____ (*bukan 6.1*)

Bagian 7 — Kegagalan dan pemulihan 7.1 Bila satu kunci hilang hari ini, apa langkahnya? ____ 7.2 Bila pemegang kunci meninggal atau tidak dapat dihubungi? ____ 7.3 Bila kustodian menghentikan penarikan? ____ 7.4 **Kapan prosedur pemulihan terakhir DIUJI** (*bukan ditulis*)? ____ 7.5 ☐ Pengujian dilakukan tanpa memakai kunci utama

Tanda tangan dan tanggal: ____

5. Contoh Terhitung

Contoh 1 — Memilih skema kunci

Seorang peserta mengelola aset digital senilai Rp2.000.000.000 dan bertanya: “Skema apa yang paling aman? Saya berpikir 5-dari-5 supaya tidak ada satu orang pun yang bisa memindahkan aset sendirian.”

Langkah 1 — pisahkan dua risiko yang berlawanan.

Risiko	Diperkecil dengan
Kehilangan	Memperbanyak salinan
Pencurian	Mengurangi salinan

Langkah 2 — hitung skema yang diusulkan. Dengan $p_{\text{hilang}} = 0,05$ dan $p_{\text{curi}} = 0,02$ per kunci per tahun:

$$P(\text{hilang}) = P(\text{tersedia} < 5) = 1 - 0,95^5 = 0,2262$$

$$P(\text{dicuri}) = 0,02^5 \approx 0,0000000$$

$$\text{Total} = 0,2262$$

Langkah 3 — baca hasilnya. Skema yang diusulkan memberi peluang **22,62% per tahun** kehilangan seluruh aset — karena **satu** kunci yang hilang dari lima sudah cukup menghancurkan semuanya.

$$0,2262 \times \text{Rp } 2.000.000.000 = \text{Rp } 452.400.000 \text{ per tahun}$$

Langkah 4 — hitung 3-dari-5.

$$P(\text{hilang}) = 0,0011581 \quad P(\text{dicuri}) = 0,0000776$$

$$\text{Total} = 0,0012357$$

Langkah 5 — bandingkan.

$$\frac{0,2262}{0,0012357} = 183 \times \text{lebih buruk}$$

Langkah 6 — tunjukkan bentuk U-nya, agar pelajarannya dapat digeneralisasi:

Skema	Total	Yang mendominasi
1-dari-5	0,0960795	Pencurian (9,6%)
2-dari-5	0,0038724	Pencurian
3-dari-5	0,0012357	Seimbang
4-dari-5	0,0225933	Kehilangan
5-dari-5	0,2262191	Kehilangan (22,6%)

Kedua ujung buruk, dan karena alasan yang berlawanan.

Langkah 7 — jawab kekhawatiran aslinya. Peserta ingin memastikan tidak ada satu orang pun dapat memindahkan aset sendirian. **3-dari-5 sudah memenuhi itu** — satu orang tidak cukup, dua orang pun tidak. Syarat kelima tidak menambah perlindungan yang berarti; ia hanya menambah cara untuk kehilangan segalanya.

Langkah 8 — nyatakan prinsipnya.

Menambah syarat tidak selalu menambah keamanan. Pada n -dari- n , syarat terakhir menciptakan risiko yang jauh lebih besar daripada yang dihilangkannya.

Langkah 9 — dan pertanyaan yang lebih penting daripada angkanya.

Apakah dua dari lima kunci itu pernah berada di lokasi yang sama, atau diketahui oleh orang yang sama? Bila ya, itu bukan lima kunci, dan seluruh perhitungan di atas tidak berlaku.

Contoh 2 — Diversifikasi kustodian yang dihitung dengan benar

Sebuah keluarga menyimpan aset digital pada satu penyedia dan mempertimbangkan memecahnya ke sepuluh penyedia “*agar risikonya sepepersepuluh.*”

Langkah 1 — uji klaimnya. Dengan peluang gagal 3% per tahun per kustodian dan pemulihan 40%:

Satu kustodian:

$$E[\text{kerugian}] = 0,03 \times 0,60 = 1,80\% \text{ modal}$$

Sepuluh kustodian:

$$E[\text{kerugian}] = 10 \times 0,03 \times \frac{0,60}{10} = 1,80\% \text{ modal}$$

Langkah 2 — kerugian yang diharapkan identik.

N	$P(\geq 1 \text{ gagal})$	Kerugian bila gagal	$E[\text{kerugian}]$
1	3,00%	60,0%	1,80%
3	8,73%	20,0%	1,80%
10	26,26%	6,0%	1,80%

Langkah 3 — dan perhatikan kolom kedua bergerak ke arah yang salah. Peluang **mengalami** kegagalan naik dari 3,00% ke 26,26% — hampir sembilan kali lipat.

Langkah 4 — jadi apakah diversifikasi keliru? Tidak. Tetapi alasannya bukan yang dikemukakan.

Langkah 5 — hitung apa yang sebenarnya dibeli. Pada modal Rp1.000.000.000:

	Kerugian bila terjadi	Dapat dilanjutkan?
1 kustodian	Rp600.000.000	Sering tidak

	Kerugian bila terjadi	Dapat dilanjutkan?
10 kustodian	Rp60.000.000	Ya

Yang dibeli adalah kesintasan, bukan kerugian yang diharapkan.

Langkah 6 — hubungkan dengan L3.3. Kerugian 60% memerlukan kenaikan **150%** untuk pulih; kerugian 6% memerlukan **6,4%**. Asimetri itulah yang membenarkan diversifikasi — bukan pengurangan $E[\text{kerugian}]$ yang sebenarnya tidak terjadi.

Langkah 7 — dan peringatan yang menentukan. Seluruh perhitungan mengasumsikan **kegagalan independen**. Periksa:

Dimensi	Bersama?
Sub-kustodian yang sama	?
Bank yang sama	?
Yurisdiksi yang sama	?
Pemilik yang sama di belakang merek berbeda	?

Langkah 8 — bila sepuluh penyedia memakai satu sub-kustodian yang sama, mereka bukan sepuluh taruhan melainkan satu — dan hasilnya lebih buruk daripada satu kustodian, karena kini ada sepuluh lapisan operasional yang masing-masing dapat gagal.

Ini adalah kekeliruan *breadth* semu (L4Q.1 §4.2) dalam bentuk lain: menghitung jumlah, bukan jumlah yang independen.

Langkah 9 — nasihat akhir.

“Pecah ke beberapa penyedia — tetapi karena Anda ingin bertahan dari satu kegagalan, bukan karena kerugian yang diharapkan berkurang. Ia tidak berkurang. Dan periksa apa yang mereka miliki bersama sebelum menghitungnya sebagai penyedia yang terpisah.”

Contoh 3 — Membaca sebuah Proof of Reserves

Sebuah penyedia mengumumkan: “Kami menerbitkan *proof of reserves* triwulanan yang diverifikasi secara kriptografis. Cadangan kami 104% dari kewajiban.”

Langkah 1 — pisahkan tiga klaim.

Klaim	Dapat dibuktikan kriptografis?
Menguasai alamat tertentu	Ya
Total liabilitas nasabah	Sebagian
Tidak ada liabilitas tersembunyi	Tidak

Langkah 2 — tanyakan apakah liabilitas ikut dibuktikan. Bila hanya aset yang dibuktikan, **angka 104% tidak bermakna** — penyebutnya tidak diverifikasi.

Langkah 3 — hitung kekuatan attestasi triwulanan. Misalkan kekurangan cadangan ada selama 10% waktu:

$$P(\text{terdeteksi}) = 1 - (1 - 0,10)^4 = 34,4\%$$

$$P(\text{LOLOS}) = 0,90^4 = 65,6\%$$

Langkah 4 — baca angka kedua. Kekurangan yang ada sepersepuluh waktu **lolos pada 65,6% kasus** di bawah attestasi triwulanan.

Langkah 5 — dan itu masih terlalu optimistis. Perhitungan itu mengandaikan waktu attestasi **tidak dapat diprediksi**. Bila waktunya diketahui sebelumnya:

$$P(\text{terdeteksi}) \approx 0$$

karena cadangan dapat dipinjam untuk potret itu saja dan dikembalikan sesudahnya.

Langkah 6 — hitung apa yang diperlukan untuk deteksi yang berarti.

Frekuensi	$P(\text{deteksi}), f=10\%$
Triwulanan (4×)	34,4%
Bulanan (12×)	71,8%
Mingguan (52×)	99,6%
Harian (365×)	100,0%

Langkah 7 — susun pertanyaan yang benar kepada penyedia:

1. Apakah **liabilitas** ikut dibuktikan, atau hanya aset?
2. Apakah waktu attestasi **tidak dapat diprediksi** oleh penyedia?
3. Apakah auditor **independen**, dan apakah laporannya **lengkap** atau terbatas?
4. Apakah aset yang ditunjukkan **dipinjam** untuk keperluan attestasi?

Langkah 8 — nyatakan kesimpulannya dengan tepat.

“PoR triwulanan yang hanya membuktikan aset menunjukkan bahwa penyedia menguasai sejumlah alamat pada empat saat dalam setahun. Ia tidak membuktikan solvabilitas, dan terhadap kekurangan yang ada sepersepuluh waktu ia gagal mendeteksinya pada 65,6% kasus.”

Langkah 9 — dan apa yang tetap harus dilakukan. PoR — bahkan yang lemah — lebih baik daripada tidak ada. Tetapi **ia tidak menggantikan pertanyaan §4.4** tentang struktur hukum, yang menentukan pemulihan Anda **setelah** kegagalan terjadi.

Contoh 4 — Struktur hukum dan alokasi hot/cold

Bagian A — Struktur hukum

Dua penyedia menawarkan layanan yang **tampak identik**: aplikasi serupa, biaya serupa, klaim keamanan serupa.

Langkah 1 — ajukan tiga pertanyaan §4.4 secara tertulis.

#	Pertanyaan	Penyedia A	Penyedia B
1	Aset tercatat atas nama siapa?	Nasabah, terpisah	Penyedia
2	Berhak meminjamkan aset?	Tidak	Ya, dengan persetujuan syarat & ketentuan
3	Masuk harta pailit?	Tidak	Ya

Langkah 2 — terjemahkan ke pemulihan.

	Struktur	Pemulihan	Dari Rp100.000.000
A	Tersegregasi, teridentifikasi	100%	Rp100.000.000
B	Dikominglingkan dan dipinjamkan	15%	Rp15.000.000

Langkah 3 — hitung selisihnya.

$$\text{Rp } 100.000.000 - \text{Rp } 15.000.000 = \text{Rp } 85.000.000$$

Selisih 85% dari aset — antara dua layanan yang tampak identik, dan tidak satu pun ditentukan oleh kriptografi.

Langkah 4 — perhatikan di mana jawabannya berada. Ketiganya dijawab oleh dokumen hukum, bukan oleh halaman keamanan di situs penyedia.

Langkah 5 — dan inilah batasnya (§1.1). Menafsirkan dokumen itu — apakah klausul tertentu benar-benar menciptakan segregasi yang akan diakui pengadilan — adalah **pekerjaan penasihat hukum berizin**.

Yang dapat dan wajib dilakukan peserta: mengajukan ketiga pertanyaan **secara tertulis**, menyimpan jawabannya, dan membawanya kepada penasihat.

Langkah 6 — penyedia yang menolak menjawab. Penolakan menjawab ketiga pertanyaan itu secara tertulis adalah jawaban, dan ia harus dicatat sebagai demikian pada Bagian 5.2 templat.

Bagian B — Alokasi hot/cold

Langkah 7 — ukur kebutuhan operasional yang sebenarnya. Sebuah operasi dengan modal Rp1.000.000.000 menyimpan 20% di *hot* “untuk berjaga-jaga”, sementara kebutuhan transaksi nyatanya Rp50.000.000 per bulan.

Langkah 8 — hitung proporsi yang dibenarkan.

$$\frac{\text{Rp } 50.000.000 \times 1,0 \text{ bulan cadangan}}{\text{Rp } 1.000.000.000} = 5 \%$$

Langkah 9 — hitung biaya selisihnya.

Proporsi <i>hot</i>	$E[\text{kerugian}]/\text{tahun}$	Nilai
20% (aktual)	1,8400%	Rp18.400.000
5% (dibenarkan)	0,6850%	Rp6.850.000
Selisih	1,1550%	Rp11.550.000

$$\text{Pengurangan} = \frac{1,8400 - 0,6850}{1,8400} = 62,8 \%$$

Langkah 10 — nyatakan apa yang dibeli oleh selisih itu.

Rp11.550.000 per tahun dibayar untuk kemudahan yang tidak dipakai — karena kebutuhan nyata hanya 5%.

Langkah 11 — aturan yang dihasilkan.

Proporsi *hot* ditentukan oleh kebutuhan likuiditas operasional yang dihitung, bukan oleh perasaan aman. Setiap rupiah di atas kebutuhan itu berbiaya 8% per tahun.

Langkah 12 — dan uji terakhir.

Kapan prosedur pemulihan *cold* terakhir diuji? Alokasi *cold* yang benar tidak bernilai apa-apa bila prosedur untuk mengaksesnya belum pernah dijalankan. Uji itu wajib dilakukan **tanpa memakai kunci utama** — karena itulah keadaan yang sedang disimulasikan.

6. Lembar Kerja Peserta

Bagian A — Batas kompetensi

- ☐ Saya memahami modul ini tidak memberikan nasihat hukum
- Penasihat hukum berizin yang saya rujuk: _____
- Tiga pertanyaan §4.4 yang sudah saya ajukan **secara tertulis**: _____
- ☐ Saya tidak akan memberikan pendapat hukum, termasuk “pendapat sementara”

Bagian B — Skema kunci

- Skema saya: ____-dari-____
- $P(\text{hilang}) \cdot P(\text{dicuri}) \cdot \text{Total}$ ____
- Bandingkan: 2-dari-3 = 0,008434 · 3-dari-5 = 0,001236 · 5-dari-5 = 0,226219
- $P(\text{kejadian dalam 10 tahun}) = \text{____} \%$
- Skema saya didominasi oleh: ☐ kehilangan ☐ pencurian ☐ seimbang
- Apakah dua kunci pernah berada di lokasi yang sama? ☐ Tidak ☐ Ya → bukan n kunci

Bagian C — Irreversibilitas

- Transaksi/tahun: ____ · Laju kesalahan p : ____
- $P(\geq 1 \text{ kesalahan}) = \text{____} \% \cdot E[\text{kerugian}] = \text{Rp} \text{____}$
- Pengendalian pra-transaksi yang aktif: ____ dari 5
- Apakah jeda wajib (nomor 5) aktif? ☐ Ya ☐ Tidak
- ☐ Saya memahami rekonsiliasi hanya memberi tahu bahwa uang sudah hilang

Bagian D — Penyedia

Satu baris per penyedia:

Penyedia	Atas nama siapa	Boleh dipinjamkan	Harta pailit	Pemulihan
• Pertanyaan yang tidak dijawab tertulis: ____ • ☐ Saya mencatat penolakan menjawab sebagai informasi				

Bagian E — Diversifikasi

- Jumlah kustodian: ____ · $P(\geq 1 \text{ gagal}) = \text{____} \% \cdot E[\text{kerugian}] = \text{____} \%$
- ☐ Saya memahami $E[\text{kerugian}]$ tidak berubah dengan jumlah kustodian
- Yang dimiliki bersama: sub-kustodian ☐ · bank ☐ · yurisdiksi ☐ · pemilik ☐ · teknologi ☐
- Jumlah kustodian yang benar-benar independen: ____

Bagian F — PoR

- Penyedia saya menerbitkan PoR? ☐ Ya, ____×/tahun ☐ Tidak
- Liabilitas ikut dibuktikan? ☐ Ya ☐ Tidak → angka rasio tidak bermakna
- Waktu attestasi tidak dapat diprediksi? ☐ Ya ☐ Tidak
- $P(\text{lolos})$ bila kekurangan ada 10% waktu = ____%

Bagian G — Hot/cold

- Kebutuhan transaksi bulanan: Rp____ · Modal: Rp____
- Proporsi hot yang dibenarkan: ____% · Aktual: ____%

- $E[\text{kerugian}]$ aktual Rp_____ vs dibenarkan Rp_____
- **Biaya kemudahan yang tidak dipakai: Rp_____/tahun**
- Kapan prosedur pemulihan *cold* terakhir diuji? _____

Bagian H — Kerangka

Isi templat §4.8 lengkap. **Bagian 7 wajib memuat prosedur yang sudah diuji tanpa memakai kunci utama.** Dokumen ini menjadi lampiran **Capstone Level 4**.

7. Bank Soal

Butir disusun mengikuti urutan materi §4 agar dapat dipakai per sesi, bukan menaik menurut tingkat kognitif. **Setiap butir diberi label kognitif**, sehingga fasilitator dapat menyusun kuis pendek menurut bagian §4 yang sedang diajarkan, menurut tingkat kognitif, atau keduanya.

Sebaran modul ini: **C1** Mengingat 4 · **C2** Memahami 1 · **C3** Menerapkan 10 · **C4** Menganalisis 8 · **C5** Mengevaluasi 2.

1. Mengapa modul ini tidak menjawab pertanyaan hukum? (C2) (Kunci: di luar kompetensi berizin; regulasi berubah cepat; pendapat di luar kompetensi merugikan penerimanya justru ketika ia paling mempercayainya)
2. Hitung waktu menebak frasa 12 kata pada 10^{12} tebakan/detik. (C3) (Kunci: $2^{128}/10^{12} = 3,403 \times 10^{26}$ detik = $1,08 \times 10^{19}$ tahun = $7,7 \times 10^8 \times$ umur alam semesta)
3. Apa kesimpulan yang benar dari soal 2? (C4) (Kunci: bukan “aset digital aman” — melainkan setiap kerugian nyata bersifat operasional atau hukum, bukan kriptografis)
4. Sebutkan dua risiko berlawanan yang dihadapi kunci. (C1) (Kunci: kehilangan — dikurangi dengan memperbanyak salinan; pencurian — dikurangi dengan mengurangi salinan)
5. Hitung total risiko 1-dari-1 dan 2-dari-3. (C3) (Kunci: 0,070000 dan 0,008434)
6. Berapa penurunan kedua risiko dari 1-dari-1 ke 2-dari-3? (C3) (Kunci: hilang -85,5%; dicuri -94,1% — keduanya turun sekaligus)
7. Hitung P (hilang) untuk 5-dari-5 dengan $p=0,05$. (C3) (Kunci: $1 - 0,95^5 = 0,2262$)
8. Bandingkan 5-dari-5 dengan 3-dari-5. (C4) (Kunci: 0,2262 vs 0,0012357 = 183× lebih buruk)
9. Mengapa kurva m -dari-5 berbentuk U? (C4) (Kunci: 1-dari-5 didominasi pencurian 9,6%; 5-dari-5 didominasi kehilangan 22,6%; kedua ujung buruk karena alasan berlawanan)
10. Hitung P (kejadian dalam 10 tahun) untuk 1-dari-1. (C3) (Kunci: $1 - (1 - 0,07)^{10} = 51,60\%$ — lemparan koin)
11. $p=0,005$, 1.000 transaksi. Hitung $P(\geq 1 \text{ kesalahan})$ dan $E[\text{kerugian}]$ pada Rp50 juta/kesalahan. (C3) (Kunci: 99,33%; 5 kesalahan; Rp250.000.000)
12. Apa perbedaan mendasar dengan L4Q.2 §4.7? (C4) (Kunci: di sana kesalahan terdeteksi dan diperbaiki; di sini rekonsiliasi hanya memberi tahu bahwa uang sudah hilang)

13. Nyatakan konsekuensi irreversibilitas untuk desain pengendalian. (C4) (Kunci: seluruh pengendalian harus berada **SEBELUM** transaksi dikirim)
14. Sebutkan lima pengendalian pra-transaksi. (C1) (Kunci: allowlist + jeda; transaksi uji; verifikasi di perangkat penanda tangan; persetujuan kedua; jeda wajib)
15. Pengendalian mana yang menangani serangan tekanan waktu? (C4) (Kunci: allowlist dengan jeda penambahan, dan jeda wajib — menghilangkan seluruh kelas serangan dengan satu aturan)
16. Sebutkan empat struktur pemulihan dan tingkatnya. (C1) (Kunci: tersegregasi teridentifikasi 100%; tersegregasi catatan cacat 85%; dikominglingkan 40%; dikominglingkan & dipinjamkan 15%)
17. Sebutkan tiga pertanyaan yang menentukan struktur mana yang berlaku. (C1) (Kunci: atas nama siapa tercatat; boleh dipinjamkan/dijaminkan; masuk harta pailit)
18. Hitung $E[\text{kerugian}]$ untuk 1 dan 10 kustodian ($q=3\%$, pemulihan 40%). (C3) (Kunci: keduanya 1,80% modal)
19. Bagaimana $P(\geq 1 \text{ gagal})$ berubah dari $N=1$ ke $N=10$? (C3) (Kunci: naik dari 3,00% ke 26,26%)
20. Apa yang sebenarnya dibeli oleh diversifikasi kustodian? (C4) (Kunci: kesintasan — mengubah kerugian jarang-besar menjadi sering-kecil; bukan pengurangan $E[\text{kerugian}]$)
21. Mengapa perhitungan diversifikasi dapat gagal seluruhnya? (C5) (Kunci: mengasumsikan independensi; kustodian dengan sub-kustodian/bank/yurisdiksi/pemilik yang sama bukan taruhan terpisah — breadth semu, L4Q.1 §4.2)
22. Tiga klaim PoR: mana yang dapat dibuktikan kriptografis? (C4) (Kunci: aset ya; liabilitas sebagian; tidak ada liabilitas tersembunyi tidak)
23. Kekurangan ada 10% waktu, attestasi triwulanan. Hitung $P(\text{terdeteksi})$ dan $P(\text{lolos})$. (C3) (Kunci: $1 - 0,9^4 = 34,4\%$; lolos 65,6%)
24. Mengapa soal 23 masih terlalu optimistis? (C5) (Kunci: mengandaikan waktu attestasi tak terduga; bila diketahui sebelumnya, cadangan dapat dipinjam untuk potret itu → deteksi mendekati nol)
25. Hitung $E[\text{kerugian}]$ pada hot 20% dan 5%, dan penurunannya. (C3) (Kunci: 1,8400% dan 0,6850%; turun 62,8%)

8. Rubrik Penilaian

Dim	Aspek	4	3	2	1
D1	Penguasaan konsep	Menjelaskan bentuk U m -dari- n dan mengapa $E[\text{kerugian}]$ tak berubah dengan diversifikasi	Menguasai skema kunci dan struktur kustodi	Menguasai sebagian	Mengira keamanan adalah soal kriptografi
D2	Ketepatan kuantitatif	Peluang kunci, pemulihan, PoR, dan	Benar dengan kekeliruan kecil	Beberapa kekeliruan	Tidak dapat direproduksi

Dim	Aspek	4	3	2	1
		hot/cold benar dan diperiksa silang			
D3	Penalaran & kerangka	Kerangka utuh; kustodian dihitung dari independensi, bukan jumlah	Kerangka koheren	Komponen terpisah	Tidak ada kerangka
D4	Perlakuan risiko (knockout)	Pengendalian pra-transaksi lengkap; prosedur pemulihan sudah diuji tanpa kunci utama	Risiko dinilai memadai	Disebut tanpa angka	Memakai 1-dari-1 atau n-dari-n untuk nilai material, atau prosedur pemulihan belum pernah diuji → GAGAL
D5	Disiplin proses (knockout)	Tiga pertanyaan §4.4 diajukan tertulis dan diverifikasi penasihat berizin	Terdokumentas i	Sebagian	Batas kompetensi dilanggar — memberikan pendapat hukum, termasuk “sementara” → GAGAL
D6	Komunikasi & etika	Menyatakan apa yang PoR tidak buktikan; mencatat penolakan menjawab sebagai informasi	Jujur	Kurang lengkap	Menyajikan PoR sebagai bukti solvabilitas

Ambang lulus: rata-rata $\geq 3,0$ **dan** D4 ≥ 2 **dan** D5 ≥ 2 .

D4 (perlakuan risiko) dan D5 (disiplin proses) bersifat menggugurkan: nilai 1 pada salah satunya membuat tugas harus diulang, berapa pun nilai dimensi lain.

Catatan penilai. Pelanggaran batas kompetensi pada D5 adalah **kegagalan langsung tanpa mempertimbangkan dimensi lain**. Peserta yang menjawab pertanyaan hukum peserta lain — betapapun benar jawabannya — telah melakukan persis hal yang dilarang §1.1.

9. Panduan Fasilitator

Alokasi waktu (16 JP)

Sesi	Isi	JP
1	§1.1 Batas kompetensi — wajib, tidak boleh dipersingkat	1
2	§4.1 Entropi; §4.2 Skema <i>m</i> -dari- <i>n</i> ; Contoh 1 — sesi kunci	3,5
3	§4.3 Irreversibilitas dan pengendalian pra-transaksi	2,5
4	§4.4 Segregasi; Contoh 4 Bagian A	2,5
5	§4.5 Diversifikasi; Contoh 2 — sesi kunci	2,5
6	§4.6 PoR; Contoh 3	2
7	§4.7–4.8 Hot/cold dan Kerangka; Contoh 4 Bagian B	1
8	Asesmen	1

Urutan yang disarankan

Sesi 1 tidak boleh dipersingkat, betapapun peserta tampak ingin melewatinya. Rumpun D menarik pertanyaan hukum lebih banyak daripada rumpun mana pun, dan fasilitator yang belum menetapkan batasnya di awal akan diminta melewatinya sepanjang tujuh sesi berikutnya.

Sesi 2 dibuka dengan angka entropi, lalu segera dengan pertanyaannya: “*Kalau begitu, ke mana perginya aset yang hilang selama ini?*” Peserta menjawabnya sendiri, dan jawabannya adalah daftar isi modul ini.

Kemudian tanyakan skema mana yang paling aman. Sebagian besar peserta menjawab *n*-dari-*n*. Biarkan jawaban itu berdiri, lalu bangun tabel *m*-dari-5 bersama-sama sampai **0,2262** muncul.

Sesi 5 memuat hasil yang paling sering ditolak peserta pada awalnya. Tampilkan kolom *E*[kerugian] — 1,80% di setiap baris — dan biarkan hening. Peserta akan mencari kesalahan dalam perhitungan. Biarkan mereka mencari; perhitungannya benar, dan usaha mencarinya adalah bagian dari pembelajarannya.

Momen pengajaran kunci

Bentuk U pada Contoh 1 Langkah 6 adalah inti modul ini. Kedua ujung buruk karena alasan yang berlawanan — sebuah pola yang berulang di seluruh kurikulum: terlalu sedikit dan terlalu banyak sama-sama merugikan, dan titik tengahnya harus dihitung, bukan dirasakan.

Contoh 2 Langkah 5 memperbaiki alasan, bukan kesimpulannya. Peserta datang dengan nasihat yang benar (“jangan satu tempat”) dan alasan yang keliru (“risikonya sepersepuluh”). Nasihat yang benar dengan alasan yang keliru akan diterapkan secara keliru pada kasus berikutnya — persis persoalan yang diangkat L3I.3.

Contoh 3 Langkah 5 layak disampaikan dengan tenang. Attestasi yang waktunya diketahui sebelumnya memiliki peluang deteksi mendekati nol. Ini bukan tuduhan terhadap penyedia mana pun; ini sifat dari pengujian pada waktu yang dapat diprediksi.

Contoh 4 Langkah 3 — Rp85.000.000 dari Rp100.000.000 — adalah angka yang harus dibawa pulang peserta. Dua layanan yang tampak identik, selisih 85% dari aset, dan tidak satu pun ditentukan oleh teknologi.

Kesalahan umum peserta

Kesalahan	Koreksi
Mengira keamanan adalah soal kekuatan kriptografi	§4.1; $7,7 \times 10^8$ umur alam semesta — bukan di situ letaknya
Mengira n -dari- n paling aman	§4.2; 5-dari-5 = $183 \times$ lebih buruk daripada 3-dari-5
Menyimpan dua kunci di lokasi yang sama	Contoh 1 Langkah 9; itu bukan n kunci
Mengandalkan rekonsiliasi untuk menangkap kesalahan	§4.3; ia hanya memberi tahu uang sudah hilang
Mengira diversifikasi menurunkan E [kerugian]	§4.5; 1,80% di setiap baris
Menghitung jumlah kustodian, bukan yang independen	§4.5; breadth semu dalam bentuk lain
Memperlakukan PoR sebagai bukti solvabilitas	§4.6; lolos 65,6% pada attestasi triwulanan
Menilai penyedia dari halaman keamanannya	§4.4; jawabannya ada di dokumen hukum
Menyimpan <i>hot</i> berlebih “untuk berjaga-jaga”	§4.7; berbiaya 8%/tahun untuk kemudahan tak dipakai

Aturan keras bagi fasilitator

1. **Dilarang memberikan pendapat hukum, pajak, atau perizinan dalam bentuk apa pun** — termasuk pendapat yang diberi label “sementara”, “bukan nasihat”, atau “sekadar pandangan pribadi”. Rujuk kepada penasihat berizin. (§1.1)
2. **Dilarang menyatakan bahwa penyedia, bursa, dompet, atau kustodian tertentu aman, patuh, atau berizin** — termasuk sebagai contoh, dan termasuk bila peserta menyebutkannya lebih dahulu.
3. **Dilarang menyebutkan atau merekomendasikan produk, merek, atau platform tertentu.**

4. **Dilarang meminta, melihat, menyentuh, atau membantu menuliskan frasa pemulihan, kunci privat, atau kredensial peserta** dalam keadaan apa pun. Seluruh praktik memakai dompet uji tanpa nilai.
 5. **Dilarang membantu peserta memindahkan aset nyata** selama atau sesudah sesi.
 6. **Dilarang menerima imbalan, rujukan, atau fasilitas** dari bursa, kustodian, penerbit, atau penyedia dompet. Kepentingan finansial apa pun wajib diungkapkan di awal sesi. (L4.2)
 7. **Wajib menyampaikan** bahwa status regulasi aset digital berubah dan bahwa seluruh keterangan struktural dalam modul ini harus diverifikasi terhadap ketentuan yang berlaku pada saat dibaca.
 8. **Wajib menghentikan sesi** dan merujuk kepada pihak berwenang bila seorang peserta menyampaikan indikasi bahwa ia sedang menjadi korban penipuan atau pemerasan.
-

10. Penafian

Materi ini disusun untuk tujuan pendidikan dan peningkatan literasi keuangan. Materi ini **bukan** nasihat investasi, **bukan nasihat hukum**, bukan nasihat pajak, bukan rekomendasi penyedia atau produk, dan bukan ajakan untuk melakukan transaksi.

Modul ini tidak menyatakan bahwa penyedia, bursa, kustodian, atau dompet mana pun aman, patuh, atau berizin. Modul ini juga tidak menyatakan sebaliknya. Penilaian atas penyedia tertentu berada di luar cakupannya.

Seluruh peluang kehilangan, peluang pencurian, peluang kegagalan kustodian, tingkat pemulihan, laju kesalahan, dan nilai rupiah dalam modul ini bersifat **ilustratif dan dibuat untuk keperluan pengajaran**. Tidak satu pun diukur dari penyedia, peristiwa, atau data nyata mana pun. Tingkat pemulihan dalam kepailitan bergantung sepenuhnya pada hukum yang berlaku dan fakta setiap kasus.

Status regulasi aset digital berubah. Kewenangan pengawasan, kewajiban perizinan, perlakuan pajak, dan status hukum kepemilikan telah berubah beberapa kali dan dapat berubah lagi. Seluruh keterangan struktural dalam modul ini **wajib diverifikasi** terhadap ketentuan yang berlaku pada saat dibaca, oleh penasihat hukum berizin di yurisdiksi yang relevan.

Aset digital mengandung risiko kehilangan seluruh nilai, termasuk melalui kegagalan penyedia, kesalahan operasional yang tidak dapat dibalikkan, perubahan regulasi, dan penipuan. **Transaksi aset digital tidak dapat dibatalkan dan tidak memiliki mekanisme banding.**

Invesmentpedia dan fasilitatornya tidak memberikan nasihat investasi yang dipersonalisasi, tidak memberikan nasihat hukum, dan tidak berizin sebagai penasihat investasi maupun sebagai advokat.
