RISK DECK

START HERE: ONE PAGE TO YOUR FIRST ROUND

A co-op game for a mixed table: half read a threat as **Tech** (how likely?), half as **Business** (how much would it cost?). You win or lose together, and the goal is to speak each other's risk language.

WHO
3 to 6 people. Full game: an Incident Captain (reads prompts, runs the timer, no Lens), the rest split Tech and Business.

HOW LONG
60 to 75 minutes full game. Core 20 minutes (guide: 3 steps, no Captain, Triage or Boardroom; one player referees and runs the timer).

WHAT YOU BRING
An attack chain: Actor, Target, 3 to 4 steps, from a game or a real incident. None? Use Cold Start.

YOU NEED

- ☐ a d20
- ☐ 10 tokens
- ☐ a timer
- ☐ 3 tally marks (full game)
- ☐ Lens cards
- ☐ Clue cards
- ☐ 8 Control cards
- ☐ 4 Consequence cards
- ☐ Boardroom cards
- ☐ Board Brief
- ☐ Cold Start (only if no chain)

TOKENS AND ROLLS

One Risk Appetite pool of **10 tokens**, fixed (one Alignment swap adds 1). 1 unit = 10k; tokens are not money. A Control costs 1 token and **lands on a d20 of 8+** (a miss still spends it); a landed Control lowers what its card prints: Likelihood one rung, or Impact one tier (Backups, IR Plan). The board ask is priced in units by your own estimate (any number with a reason), not in tokens.

EACH STEP IS ONE ROUND OF FIVE PARTS

1. **Triage.** Ten seconds out loud: accept, mitigate or transfer? No numbers move.
2. **Estimate.** Everyone privately writes Likelihood and Impact plus a blind guess of another player's read; flip together and score Alignment (within one rung or tier = 1, exact = 2). Core skips this. Start at Strength and tier, clue moves one step. Say your clue, then re-commit: the Tech Lens sets Likelihood, the Business Lens Impact (higher stands). Full game: re-committing before every Lens player has said their clue (the Captain speaks no clue) earns a tally mark; the third raises Impact one tier (the one bump a row can get).
3. **Boardroom.** A card asks one question; the Lens printed on it answers in plain words, under the timer. Then read the fitting Consequence card; a yes bumps (once).
4. **Defend.** Full game: swap 3 Alignment for +1 token, once. Spend tokens on Controls that fit; roll the d20 (3 tries a card a row).
5. **Record.** One row on the Brief. Next step.

TIME BUDGET

FULL GAME	MINUTES	CORE (NO TRIAGE, BOARDROOM)	MINUTES
Per step: triage 1, estimate 5, Boardroom 2, defend 3, record 2	13	Per step: commit and flip 2, articulate 1, defend 1.5, record 0.5	5
Brief aloud, Verdict, debrief	11	Verdict and one closing question	2
3 steps / 4 steps	**60 / 73**	**3 steps**	**20**

HOW IT ENDS

After the last step, roll one d20 and add your posture: unspent tokens, minus 3 per high-residual row, plus 3 per landed Control that lowers a row. (High-residual: final row after Controls, Likelihood 4+, or 3+ with Impact T4+.)

15+ Funded
The board backs your plan: a win.

8-14 Deferred
Not yet. The board wants a better case.

7 or less Breached
The risk was not covered: a loss.

ONE WORKED ROW

Step 2: *a stolen password logs in to the remote-access portal.* Actor: organized crime. Target: internal pricing data, importance 6 (T3 to start).

ESTIMATE
Tech Lens says Likelihood 4: the Organized Crime clue says weaknesses are hit everywhere, and a password got in. Business Lens says Impact T3, about 60 units (600k). Consequence card on regulated data: no, no bump.

DEFEND
Spend 1 token on **Multi-Factor Authentication** (the way in was a password). d20 shows 13: it lands, Likelihood drops one rung, 4 to 3.

TELL THE BOARD
> *"A stolen password could expose our pricing data, about 600k. We ask for multi-factor login on remote access, 3 units (30k)."*

AT THE END
After 3 steps: 6 tokens unspent, one other row high-residual, 1 landed Control: posture 6 - 3 + 3 = 6. d20 10, total 16: **Funded**.

ANCHORS, CONTROLS AND WORDS

WHAT A LIKELIHOOD NUMBER MEANS

RUNG	YOU WOULD SAY THIS ABOUT THE STEP
1 Rare	Needs a top-tier attacker and a lot of luck against a well-kept target. Not seen in your sector in years.
2 Unlikely	Needs inside help, or a flaw that is hard to find. It could happen, but you would be surprised.
3 Possible	A known method works if one of your defences has lapsed. Others like you have been hit.
4 Likely	A common attack that works against ordinary slips (a reused password, a late patch). It happened in your sector this year.
5 Almost certain	The door is open now (a default password, an exposed login) or it is already happening.

WHAT AN IMPACT TIER MEANS (1 UNIT = 10K)

TIER	UNITS	PICTURE IT AS
T1 Minor	1-4	A team loses a day. A report has to be redone.
T2 Moderate	5-24	An hour of a key system down, or a small customer list exposed.
T3 Serious	25-99	A day of a key system down, a few thousand customers, a letter from a regulator.
T4 Severe	100-499	Days of lost sales, tens of thousands of customers, a public notice.
T5 Critical	500-2,500	The company cannot trade for a week, or regulated data of nearly everyone is out.

Start from your Target's importance (1-2 T1, 3-4 T2, 5-6 T3, 7-8 T4, 9-10 T5). The Consequence card may add one tier per row, no more.

WHICH CONTROL FITS WHICH STEP

CONTROL CARD	USE IT WHEN THE STEP IS...	WHAT IT BUYS YOU
Multi-Factor Authentication	a stolen or guessed password	A password alone no longer gets in.
Endpoint Detection & Response	code running or hiding on a computer	Someone sees it early enough to act.
Network Segmentation	moving from one system to another	The attacker is stuck in one zone.
Immutable Offline Backups	data destroyed, locked or changed	You recover without the attacker's help.
Security Awareness Training	a phishing or trick message	A person reports it instead of clicking.
Tested Incident Response Plan	any step after the first way in	The first hour is rehearsed, so the chain is cut sooner.
Encryption At Rest	reading or copying stored data	Reaching the storage is not reading it.
Third-Party Risk Assessment	a supplier or vendor access path	The supplier path is checked before it is abused.

WORDS ON THE TECH CARDS, IN PLAIN ENGLISH

WORD	MEANS
foothold	The attacker already has a way in, even a small one.
known-CVE, unpatched	A flaw the world already knows about, with a fix you have not installed.
commodity, off-the-shelf	Cheap, common tools and software that many firms use, so many attackers know them.
perimeter	The outer wall: firewalls and logins facing the internet.
least-privilege	People only have the access their job needs.
lateral movement, pivot	Hopping from one computer or system to the next.
persistence	The attacker sets things up to stay, even after a reboot.
C2 (command and control)	The channel the attacker uses to give orders to the hacked computer.
exfiltration	Copying data out of your network.
tableau	The row of face-up Control cards in the middle of the table.