CHARTA LEARNING · LESSON NOTES

Risk Identification

FRM Part II

1 A story: the risk that sat between two desks

- Payments and treasury each list their own risks
- A file passes between them; each thinks the other checked
- Duplicate payments go out: the risk sat in the handoff
- Op risk: inadequate or failed processes, people, systems
- Op risk also covers external events

IN THE LESSON

- Imagine Kestrel Bank, a mid sized lender with a payments unit and a treasury unit.
- Each unit keeps careful lists of its own risks, and each list looks complete.
- One morning a payment file passes from payments to treasury, and both teams assume the other has checked it.
- Nobody has.
- Duplicate payments go out, and money is lost before anyone notices.
- Neither list contained this risk, because it sat in the handoff between two units.
- Notice the lesson.
- Kestrel did not fail to measure this risk.
- It failed to see it at all.
- Operational risk is the risk of loss from inadequate or failed internal processes, people and systems, or from external events.
- Identification is the first step in managing it.

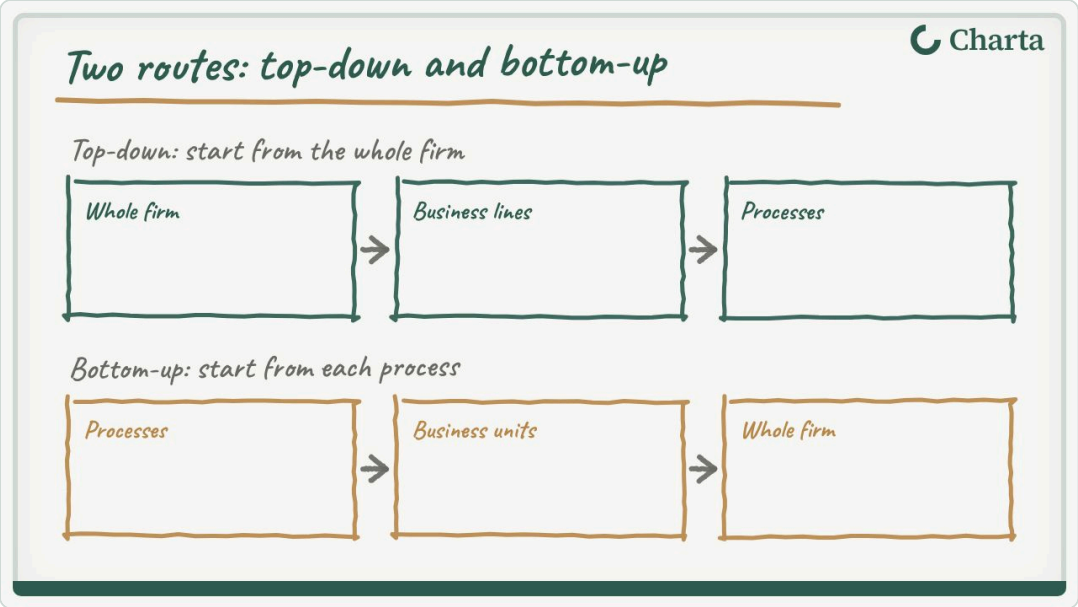
2 Identification is not measurement

- Identification: what could go wrong?
- Measurement: how large and how likely?
- A risk never identified is never measured or controlled
- A good model cannot fix a missing risk
- Two complementary routes to identification

IN THE LESSON

- Before we look at the tools, keep two jobs apart.
- Identification asks what could go wrong.
- It produces a list of risks, each with a description of how it could arise.
- Measurement asks how large and how likely.
- It puts numbers on the risks already found, such as a loss estimate or a frequency.
- The order matters, because a risk that is never identified is never measured, never controlled and never reported.
- It simply waits.
- An exam question may describe a bank with a sophisticated capital model and ask what is missing.
- If the model only covers risks the bank has listed, the gap is identification.
- Kestrel needs both, but identification comes first.
- There are two complementary routes to it.

3 Two routes: top-down and bottom-up



IN THE LESSON

- Here are the two routes.
- The top down route starts from the institution as a whole and works downward.
- Kestrel's senior managers look at the whole firm, then at its business lines, and then at the processes where the big risks could arise.
- The bottom up route goes the other way.
- It starts at the level of a single process, moves up to the business unit, and is then pulled together for the whole firm.
- Think of looking at a city from a plane, compared with walking its streets.
- From the plane you see the shape of the whole city and where a flood would spread, but not a broken step.
- On the street you see every broken step, but not the river rising.
- Each route sees what the other misses.

4 Top-down instruments

They start from the whole firm and look down

Instrument	What it gives Kestrel
Scenario workshops	Senior view of severe events
External loss data, benchmarks	What has hit peers
Aggregate loss, earnings swings	Signals at firm level
Emerging-risk scanning	New threats from outside

IN THE LESSON

- Now the instruments, starting with top down.
- First, senior management scenario workshops.
- Senior managers meet, with a facilitator, and ask what could seriously hurt the firm.
- Second, firm wide analysis of external loss data and industry benchmarks.
- External loss data are records of operational losses suffered by other firms, collected by industry groups or from public sources.
- They show Kestrel what has hit its peers.
- Third, review of aggregate loss and earnings volatility, meaning the firm's total operational losses and how much its earnings swing.
- A sudden change points to a risk worth chasing.
- Fourth, emerging risk scanning, which looks outward for new threats, such as a new kind of cyber attack or a new regulation.
- Notice that all four look at the firm from above.

5 Bottom-up instruments

They start at each process and add up

Instrument	What it gives Kestrel
RCSA	Units rate own risks and controls
Process mapping	Where each step can break
Internal losses and near misses	What has gone wrong, or nearly
KRIs and audit findings	Rising risk, weak controls
New-product reviews	Risks checked before launch

IN THE LESSON

- The bottom up instruments work at process or business unit level.
- First, risk and control self assessment, known as R C S A.
- Each unit lists its risks, rates them, and judges how well its controls work.
- Second, process mapping, which draws each step of a process to find where it can break.
- Third, internal loss and near miss collection.
- A near miss is an event that could have caused a loss but did not, perhaps because it was caught in time.
- Fourth, key risk indicators, or K R I s, which are metrics that warn that a risk is rising, such as failed trades a day.
- Fifth, audit findings, which flag control weaknesses.
- And last, new product reviews, which check the risks of a product before launch.

6 Strengths and weaknesses of each route

The weaknesses of one route are the strengths of the other

Feature	Top-down	Bottom-up
Speed	Quick	Slower
Best at	Strategy, tail events	Detail, action
Weakness	Coarse, judgement	Gaps between units
Never happened?	Can imagine it	Often missed

IN THE LESSON

- How do the two routes compare?
- Top down methods are quick, because a few senior people can cover the whole firm in a day.
- Bottom up methods are slower, because every unit has to take part.
- Top down methods are strategic and good at tail events, the rare and severe losses, because senior people think about what could threaten the firm.
- Bottom up methods are detailed and actionable, because a unit can fix the exact control that failed.
- The weaknesses mirror the strengths.
- Top down results are coarse and driven by judgement.
- Bottom up methods can miss risks that sit between units, like Kestrel's handoff, or that have never occurred, because each unit looks at its own patch and its own history.
- Top down workshops, by contrast, can imagine events that have never happened.

7 Example 1: what each route finds at Kestrel

Kestrel's register: risks found by each route, and by both

Found bottom-up	RCSA, KRIs, loss data	**40**
Found top-down	workshops, external data	**8**
Found by both	on both lists	**5**
Distinct risks	40 + 8 − 5	**43**
Found only top-down	8 − 5	**3**

Bottom-up alone misses 3 of 43 (7%): between units, never seen

IN THE LESSON

- Let us count, with made up numbers.
- Kestrel's bottom up work, through R C S A, K R I s and loss data, identifies forty risks.
- Its top down workshops and external data identify eight.
- Five of the eight were also on the bottom up list.
- So the number of distinct risks is forty plus eight minus five, which is forty three.
- Now look at the three risks that only the top down route found: eight minus five.
- They are the handoff between payments and treasury, a cloud vendor shared by several units, and a new form of cyber attack the bank has never suffered.
- Bottom up alone would miss three of forty three, about seven per cent.
- Few, but they are exactly the risks between units or never seen before.

8 Mistakes to avoid: one route is not enough

- Only bottom-up: 35, e.g. a weak branch reconciliation
- Good practice: combine both routes; each checks the other
- Trap 1: treating one route as sufficient
- Trap 2: confusing identification with measurement
- Identification: what could go wrong, not how big

IN THE LESSON

- Now look at the other side of the count.
- Thirty five risks were found only bottom up, such as a weak reconciliation in one branch.
- A senior workshop would rarely list those.
- So good practice combines both routes, and each checks the other.
- The first trap in exam questions is treating one route as sufficient.
- A bank that only runs R C S A will miss the risks between units and the risks it has never seen.
- A bank that only runs senior workshops will have a strategic list and no idea which control to fix.
- The second trap is confusing identification with measurement.
- Asking how likely a loss is, or how large, is measurement.
- Asking what could go wrong is identification.

9 Why extreme events are hard to find

- Extreme events: rare but severe
- Most firms have few or none in their own history
- Extrapolating past losses understates the tail
- Tail: the far end of the loss distribution
- Ten lucky years teach little about the worst case

IN THE LESSON

- Now the hardest part of identification: extreme events.
- These are operational losses that are rare but severe, the kind that can threaten a firm.
- A large rogue trading loss or a long outage of a critical system are examples.
- The trouble is that rare events are, by definition, rare.
- Most firms have few or none of them in their own loss history.
- So if Kestrel simply looks at its past losses and extrapolates, meaning it projects the pattern forward, it will understate the tail.
- The tail is the far end of the loss distribution, where the large losses live.
- A firm that has been lucky for ten years has learned very little about its worst case.
- Its own data cannot show it.

10 Example 2: the danger of anchoring on the past

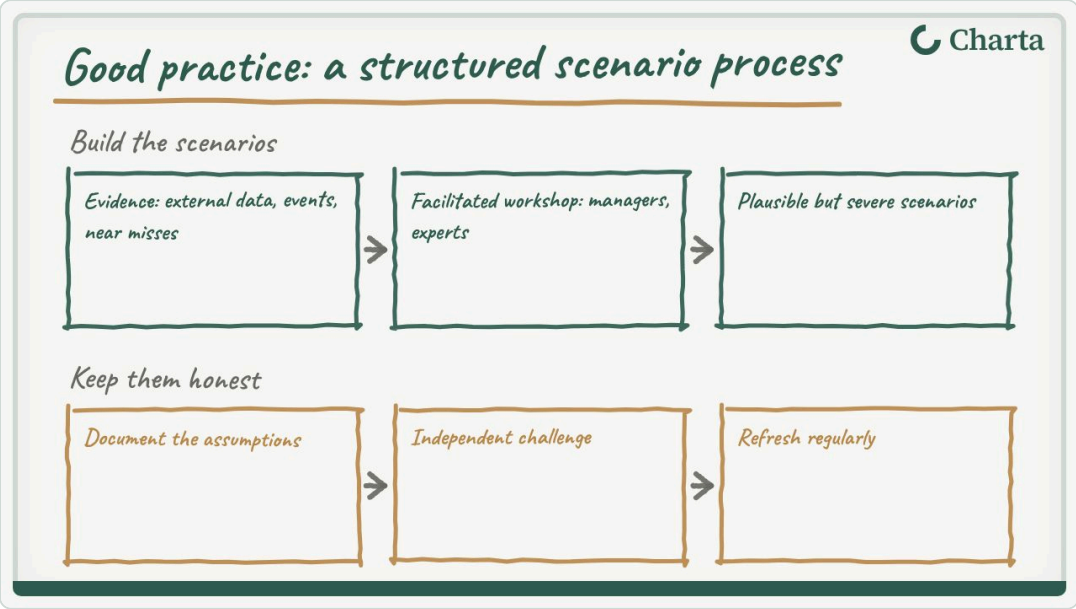
Kestrel: 10 years of internal loss data. Is the past a guide to the worst case?

Internal history	10 years, 1,250 events	**$60m in total**
Largest internal loss	in 10 years	**$4m**
Naive worst case	2 × largest	**$8m**
Peer's comparable event	external loss data	**$150m**
Understatement	150 ÷ 8	**18.75 times**

IN THE LESSON

- Here is that trap in numbers.
- Kestrel has ten years of internal loss data, with one thousand two hundred and fifty events and losses of sixty million dollars in total.
- Its largest single loss was four million.
- An analyst says the worst case is twice the largest loss seen, so eight million dollars.
- That is anchoring, which means fixing on a past number and adjusting too little from it.
- Now Kestrel checks external loss data, and finds that a peer bank of similar size suffered a comparable event, a payments failure, costing one hundred and fifty million dollars.
- The naive worst case understates that by a factor of one hundred and fifty divided by eight, eighteen point seven five times.
- The bank's own history was simply too short.

11 Good practice: a structured scenario process



IN THE LESSON

- So how should Kestrel find extreme events?
- Good practice is forward looking and structured.
- Look at the flow.
- The top row builds the scenarios.
- First, prepare the evidence: external loss data, public events at other firms, and internal near misses, which show how close the bank came to trouble.
- Second, run facilitated scenario analysis.
- Scenario analysis is a structured discussion of what could happen, how, and what it would cost.
- It is run by a facilitator with senior management and subject matter experts, the people who know each process best.
- Third, build scenarios that are plausible but severe.
- The bottom row keeps them honest.
- Document the assumptions, put the results through independent challenge by people outside the workshop, and refresh the scenarios regularly as the business changes.

12 Example 3: a severe scenario combines failures

Control breakdown + cloud vendor fails + market stress, on the same day ($m)

Client compensation	failed, late payments	**$35m**
Trades closed out	in a falling market	**$40m**
Regulatory penalty		**$15m**
Recovery and repair		**$10m**
Scenario total	35 + 40 + 15 + 10	**$100m**

25 times Kestrel's largest internal loss of $4m

IN THE LESSON

- Good scenarios combine several failures at once, because real disasters rarely have a single cause.
- Kestrel's workshop builds one.
- A control breakdown lets faulty payment files through.
- On the same day, its critical cloud vendor, a third party that runs the payments platform, fails.
- And markets are under stress.
- The experts size the pieces, with made up numbers.
- Compensating clients for failed and late payments costs thirty five million dollars.
- Trades that cannot settle are closed out in a falling market, losing forty million.
- A regulatory penalty adds fifteen million, and recovery and repair cost ten.
- The total is one hundred million dollars, twenty five times the largest loss in Kestrel's own history.
- Sizing is measurement, but the scenario itself was found by identification.

13 Look for interdependencies and concentrations

- Interdependency: one failure spreads to other units
- Concentration: one point that many activities rely on
- Kestrel: payments, custody, trading share one cloud vendor
- Each unit saw only its own contract: rated low risk
- Shared systems, data centres, key teams: look across

IN THE LESSON

- The cloud vendor in that scenario points to the next piece of good practice: examine interdependencies and concentrations.
- An interdependency is a link through which one failure spreads to other parts of the firm.
- A concentration is a single point that many activities rely on.
- When Kestrel maps its suppliers, it finds that payments, custody and trading all run on the same cloud vendor.
- Each unit had rated that vendor as a low risk, because each saw only its own contract.
- Seen together, one failure would stop three businesses at once.
- The same is true of a shared system, a single data centre or one key team.
- These links are invisible to unit level lists, which is why extreme event work must look across the whole firm.

14 Example 4: a reverse stress test

Start from the loss that would break Kestrel, then work back ($m)

Capital today		**$1,500m**
Minimum in the risk appetite		**$1,100m**
Viability-threatening loss	1,500 − 1,100	**$400m**
Worst scenario so far	combined failure	**$100m**
Share of the gap	100 ÷ 400	**25%**

Work back: what chain of failures could cost 4 times as much?

IN THE LESSON

- Another good practice tool is reverse stress testing.
- An ordinary stress test starts from a shock and asks how much it would cost.
- A reverse stress test starts from an outcome that threatens viability, meaning the firm's ability to carry on, and works back to its causes.
- Kestrel has capital of one thousand five hundred million dollars.
- Its risk appetite says capital must never fall below one thousand one hundred million.
- So a loss of four hundred million threatens viability.
- Kestrel's worst scenario so far, the one hundred million dollar combined failure, is only twenty five per cent of that gap.
- The reverse question is then: what chain of failures could cost four times as much?
- That forces the bank to imagine events no one had listed.

15 Working back, and the traps to avoid

- Work back: data corrupted, weeks of outage, clients leave
- Then judge plausibility and the controls that break it
- Trap: anchoring on past losses
- Trap: 'it has never happened', so it is not valid
- Trap: no documented assumptions, challenge or refresh

IN THE LESSON

- Working back, Kestrel's experts suggest a chain.
- A cyber attack corrupts the vendor's data, the outage lasts weeks rather than a day, and large clients move their business elsewhere.
- The bank then judges how plausible that chain is and what controls would break it.
- Now the traps.
- The first is anchoring on past losses, as we saw.
- The second is rejecting a scenario because it has never happened.
- A scenario is not invalid because it has never happened.
- Every extreme event at every firm was unprecedented at that firm once.
- The third is a scenario with no written assumptions and no challenge, which nobody can test.
- And the fourth is a scenario set once and never refreshed, while the business moves on.

16 What a risk taxonomy is

- Taxonomy: a structured, hierarchical list of categories
- Levels run from broad to granular
- Same labels for risks, events, losses and controls
- So they can be aggregated across the firm
- And compared across units and years

IN THE LESSON

- Once risks are found, they need names that everyone uses in the same way.
- That is the job of an operational risk taxonomy.
- A taxonomy is a structured, hierarchical list of defined risk categories.
- Hierarchical means it has levels, from a few broad categories at the top to many granular ones below.
- Why does Kestrel need one?
- Because its payments team might call an event a processing error, while treasury calls the same kind of event an operations failure.
- With one taxonomy, risks, events, losses and controls are all labelled the same way across the firm.
- Then they can be aggregated, meaning added up across units, and compared, from unit to unit and from year to year.
- Without shared labels, totals mean nothing.

17 Four ways to classify a risk

Each way of classifying answers a different question

Classify by	Question	Examples
Cause	Why?	People, process, systems, external
Event type	What happened?	Internal fraud, processing error
Effect or impact	What loss?	Legal liability, write-down, penalty
Business line	Where?	Retail banking, payments

IN THE LESSON

- Risks can be classified in several ways, and each answers a different question.
- The first is by cause, which asks why it happened.
- Typical causes are people, processes, systems and external events.
- The second is by event type, which asks what actually happened, such as internal fraud or a processing error.
- The third is by effect, or impact, which asks what kind of loss resulted, such as a legal liability, a write-down, meaning a reduction in the value of an asset, or a regulatory penalty.
- The fourth is by business line or process, which asks where it happened, such as retail banking or payments.
- The same event has an answer to all four questions, as our next example shows.

18 Example 5: one incident, four labels

A clerk keys a $2.4m payment twice; the duplicate cannot be recovered

Cause	why it happened	**People**
Event type	what happened	**Processing error**
Effect	what kind of loss	**Loss of recourse**
Business line	where it happened	**Payments**

Four facts about one $2.4m loss, not four losses

IN THE LESSON

- Take one incident at Kestrel.
- A clerk keys a payment of two point four million dollars twice, and the duplicate cannot be recovered from the receiving bank.
- Classify it four ways.
- The cause is people, a human error, and the process lacked a check that would have caught it.
- The event type is a processing error, the thing that actually happened.
- The effect is a loss of recourse, meaning money paid out in error that cannot be recovered.
- And the business line is payments.
- Notice that these are four different facts about one loss, not four losses.
- If Kestrel's taxonomy put all four kinds of label side by side on the same level, this one loss could end up counted more than once.

19 What makes a good taxonomy

- Mutually exclusive: no event fits two categories
- Collectively exhaustive: every event fits somewhere
- So each loss has one primary home
- Levels run from broad to granular
- Classic flaw: causes, events and effects on one level

IN THE LESSON

- So what makes a taxonomy good?
- First, it is mutually exclusive, which means no event fits two categories at the same level.
- Second, it is collectively exhaustive, which means every event fits somewhere.
- Together, these two properties mean each loss has one primary home.
- Third, it moves from broad to granular levels, so the board can see a few broad totals, and a unit manager can drill down to the detail.
- Now the classic flaw.
- It is mixing causes, events and effects at the same level, for example a category called people next to one called fraud and one called legal liability.
- These overlap.
- One fraud by an employee involves people, is a fraud and may create a legal liability.
- That causes double counting.

20 Example 6: how mixing levels double counts

Flawed level: People, Fraud, IT systems, Legal liability ($m)

Employee fraud, $3m	in People and in Fraud	**$6m**
System outage, $5m	in IT and in Legal	**$10m**
Processing error, $2m	in People only	**$2m**
Sum of the buckets	6 + 10 + 2	**$18m**
True total loss	3 + 5 + 2	**$10m**

Overstated by $8m, or 80%: one primary home per loss fixes it

IN THE LESSON

- Here is the flaw in numbers.
- An early version of Kestrel's taxonomy had four categories on one level: people, fraud, I T systems and legal liability.
- Three events happen in a year.
- An employee fraud loses three million dollars.
- It is tagged under people and under fraud, so six million appears in the buckets.
- A system outage loses five million, including compensation paid to clients.
- It is tagged under I T systems and under legal liability, adding ten million.
- A processing error loses two million and is tagged only under people.
- The buckets sum to eighteen million dollars, but the true total loss is three plus five plus two, ten million.
- The report overstates losses by eight million, which is eighty per cent.

21 The fix: event type first, cause as an attribute

- Classify loss data by event type: one primary home
- Record the cause as an attribute, not a category
- Effect and business line can be attributes too
- Kestrel: the totals now add to $10m
- Basel's taxonomy takes the same approach

IN THE LESSON

- The fix is the standard one.
- Loss data are usually classified by event type, which gives each loss its one primary home.
- The cause is then recorded as an attribute, meaning an extra field attached to the loss record, rather than as a competing category.
- The effect and the business line can be recorded as attributes too.
- In Kestrel's new system, the employee fraud lives only under internal fraud, with people recorded as its cause.
- The outage lives only under business disruption and system failures, with legal liability recorded as its effect.
- Now the totals add up to ten million dollars, and the bank can still ask how much of its loss was caused by people.
- That is the approach the Basel taxonomy takes.

22 The Basel taxonomy: Level 1, part one

Seven Level 1 event types. The first four:

Level 1 category	What it covers
Internal fraud	Deliberate act involving an insider
External fraud	Deliberate act by a third party
Employment, workplace safety	Employment, safety law; discrimination
Clients, products, practices	Failing clients, product flaws

IN THE LESSON

- The Basel operational risk taxonomy, set by the Basel Committee on Banking Supervision, classifies loss events by event type, in three levels.
- Level one has seven categories, and you should know all seven.
- Here are the first four.
- Internal fraud covers deliberate acts, such as fraud or unauthorised trading, involving at least one insider.
- External fraud covers deliberate acts by a third party, such as theft, forgery or hacking.
- Employment practices and workplace safety covers losses from breaches of employment, health or safety laws, and from discrimination.
- Clients, products and business practices covers failing in an obligation to clients, such as mis selling or a breach of fiduciary duty, and losses from the design of a product, known as product flaws.

23 The Basel taxonomy: Level 1, part two

The remaining three, seven in all

Level 1 category	What it covers
Damage to physical assets	Disasters and other events
Business disruption, systems	System and utility outages
Execution, delivery, process (EDPM)	Processing errors, vendors

IN THE LESSON

- Here are the other three.
- Damage to physical assets covers loss of or damage to buildings and equipment from natural disasters or other events, such as a flood or an act of terrorism.
- Business disruption and system failures covers outages of systems, such as a crash of the payments platform, and failures of utilities such as power or telecommunications.
- And execution, delivery and process management, which we will shorten to E D P M, covers failed transaction processing or process management, and disputes with trade counterparties and with vendors.
- This last category is the home of unintentional errors in processing.
- At Kestrel, it is where most loss events turn up.
- Seven categories in all.

24 Levels 2 and 3: from broad to specific

Each level is more specific; EDPM has six Level 2 groups

Level 1	Level 2	Level 3 example
Internal fraud	Unauthorised activity	Intentional mismarking
Internal fraud	Theft and fraud	Embezzlement
External fraud	Systems security	Hacking damage
EDPM	Transaction capture	Data entry error
EDPM	Vendors and suppliers	Vendor dispute

IN THE LESSON

- Level two divides each Level one category into sub categories, and Level three gives examples of activities.
- Take internal fraud.
- It splits into two Level two groups.
- The first is unauthorised activity.
- A Level three example is intentional mismarking of positions, where a trader values positions wrongly on purpose to hide losses.
- The second group is theft and fraud, with examples such as embezzlement by an employee.
- External fraud has a Level two group called systems security, with hacking damage as an example.
- And E D P M divides into six Level two groups.
- One is transaction capture, execution and maintenance, with a data entry error as an example.
- Another is vendors and suppliers, with a dispute with a vendor as an example.

25 The key discriminators: intent and who

Was it intended? Who was involved?

Event	Level 1 category
Deliberate act by an insider	Internal fraud
Deliberate act by a third party	External fraud
Unintentional processing error	Usually EDPM
Strategic, reputational risk	Excluded from definition

IN THE LESSON

- How do you place an event in the right Level one category?
- Two questions do most of the work: was it intended, and who was involved?
- A deliberate act by an insider is internal fraud.
- A deliberate act by a third party, with no insider involved, is external fraud.
- An unintentional error in processing usually falls in E D P M, even when an employee made it.
- That is the commonest exam trap: a careless employee is not committing fraud.
- Finally, remember what is outside the definition altogether.
- Strategic risk, the risk from poor business decisions, and reputational risk, the risk of damage to the firm's standing, are excluded from the definition of operational risk, so they have no Level one category.

26 Example 7: classifying Kestrel's events

Five events at Kestrel: was it intended, and who was involved?

Trader mismarks positions	deliberate, insider	**Internal fraud**
Hacker steals client funds	deliberate, third party	**External fraud**
Clerk mistypes a payment	unintentional error	**EDPM**
Flood damages a branch	natural disaster	**Physical assets**
Data centre crash	system failure	**Disruption**

Level 2: trader, unauthorised activity; clerk, transaction capture

IN THE LESSON

- Let us apply the discriminators to five of Kestrel's events.
- A trader hides losses by marking positions at false prices.
- That is deliberate, by an insider, so it is internal fraud.
- An outside hacker breaks in and steals client funds.
- Deliberate, third party, so external fraud.
- A clerk mistypes the amount on a payment.
- Unintentional, a processing error, so E D P M.
- A flood damages a branch, which is damage to physical assets.
- And the data centre crashes and payments stop for a day, which is business disruption and system failures.
- At Level two, the trader's case is unauthorised activity and the clerk's is transaction capture.
- Notice that the clerk and the trader are both employees.
- Intent, not job title, separates them.

27 Example 8: a year of losses by Level 1

Kestrel's losses for one year by Level 1 event type ($m)

EDPM	processing errors	**$2.6m**
Clients, products, practices	mis-selling, product flaws	**$1.4m**
External fraud	third parties	**$0.9m**
Other four categories	together	**$1.1m**
Total, each loss once	2.6 + 1.4 + 0.9 + 1.1	**$6m**

EDPM 2.6 ÷ 6 = 43.3%. Cause attribute: $1.8m of EDPM (69%) was people

IN THE LESSON

- Why does all this labelling matter?
- Because it lets Kestrel add up its losses.
- Here is a made up year, in line with the average of Kestrel's ten year history, labelled by Level one event type.
- E D P M losses are two point six million dollars.
- Clients, products and business practices are one point four million.
- External fraud is nine hundred thousand dollars.
- The other four categories together are one point one million.
- The total is six million dollars, and each loss is counted once.
- E D P M is two point six out of six, about forty three point three per cent of the year's losses, so that is where Kestrel looks first.
- And because cause is recorded as an attribute, Kestrel can also see that one point eight million of the E D P M losses, about sixty nine per cent, had people as their cause.

28 Recap: what you have learned

- Two routes, top-down and bottom-up: combine them
- Identification comes before measurement
- Extreme events: combined scenarios, reverse stress tests
- Taxonomy: one home per loss; cause as an attribute
- Seven Basel Level 1 types; intent and who separate fraud

IN THE LESSON

- Let us pull the lesson together.
- Operational risks are found by two complementary routes.
- Top down methods, such as scenario workshops and external data, are quick and good at tail events, but coarse.
- Bottom up methods, such as R C S A, K R I s and loss data, are detailed and actionable, but miss risks between units.
- Good practice combines them, and keeps identification separate from measurement.
- Extreme events need forward looking, structured scenarios that combine failures, examine concentrations, use reverse stress tests, and resist anchoring on the past.
- A taxonomy should give each loss one primary home, classifying by event type with cause as an attribute.
- And the Basel taxonomy has seven Level one categories, where intent and who was involved separate fraud from processing errors.

29 Try three quick questions

1. Employee takes cash from the vault and hides it. Level 1 and Level 2?
   Answer: Deliberate insider: internal fraud, theft and fraud.
2. People and Internal fraud on one level. $6m fraud in both, $4m outage in one. Totals?
   Answer: Buckets $16m; true loss $10m; overstated by $6m.
3. Severe scenario rejected: 'it has never happened here'. Sound?
   Answer: No. Use external data and reverse stress tests.

IN THE LESSON

- Now try three quick questions.
- Pause the video, think, then listen to the answers.
- Question one.
- An employee takes cash from a branch vault and hides the shortfall.
- Which Basel Level one category is it, and which Level two group?
- It is deliberate and done by an insider, so it is internal fraud, in the theft and fraud group.
- Question two.
- A taxonomy has people and internal fraud on the same level.
- A six million dollar employee fraud is tagged in both, and a four million dollar outage in one bucket.
- What do the buckets show, and what is the true loss?
- The buckets show sixteen million dollars, but the true loss is ten million, overstated by six.
- Question three.
- A manager rejects a severe scenario because nothing like it has happened at the bank.
- Is that sound?
- No.
- Having no precedent at the bank does not make a scenario invalid.
- Use external data and reverse stress testing instead.