CHARTA LEARNING · LESSON NOTES

Risk Reporting

FRM Part II

1 A story: one report for everyone

- A bad quarter: payments fail for a day
- One 60-page pack goes to every committee
- The one decision is buried on page 40
- Accurate, but it fits nobody
- Start from the audience

IN THE LESSON

- Imagine Ashcombe Bank at the end of a bad quarter.
- Its payments system went down for a day, and its risk team worked hard on a sixty page report.
- The same pack went to the board, to the audit committee, to the management operational risk committee and to every business head.
- The board read the first pages, saw long tables of incidents, and moved on.
- Buried on page forty was the one point that needed a decision: whether to pay for a new payments platform.
- Nobody made it.
- The report was accurate.
- It simply did not fit anyone.
- Risk reporting starts from the audience, because each body decides different things, so each needs a different report.

2 Who decides what

Four audiences, four kinds of decision

Body	What it decides or oversees
Board and risk committee	Risk appetite and strategy
Audit committee	Internal audit and controls
OR committee	OR across the business lines
Business line managers	Their own area, day to day

IN THE LESSON

- So let us map the audiences.
- The board and its risk committee set the risk appetite, meaning how much risk the bank is willing to take, and the strategy.
- The audit committee oversees internal audit and the control environment, that is, whether the bank's controls are designed well and actually work.
- The management operational risk committee is made up of business heads and risk staff.
- It runs operational risk across the business lines, week to week.
- On the board we call it the O R committee, O R for operational risk.
- And business line managers run their own area, day to day.
- Four audiences, four kinds of decision.
- Keep this table in mind, because every report we design next follows from it.

3 What each audience needs to see

Content follows the decision each body makes

Audience	What its report shows
Board and risk committee	Exposure vs appetite; decisions
Audit committee	Control gaps, findings, overdue
OR committee	Losses, breaches, actions, owners
Business line managers	Granular, actionable, own area

IN THE LESSON

- Now match the content to the audience.
- The board and its risk committee need short, aggregated and forward looking reports.
- They compare exposure with appetite and flag the few issues that need a decision.
- The audit committee wants control weaknesses, audit findings, and whether the fixes, called remediation, are overdue.
- The management committee needs more detail, by business line: the loss events, the breaches of indicators, the action plans and the named owners of each action.
- And business line managers need frequent, granular and actionable data on their own area.
- Notice how the detail grows as we go down the table, from a few lines for the board to the full picture for the person who runs the desk.

4 Detail and frequency

The higher the body, the shorter and less frequent its report

Audience	Detail | How often
Board and risk committee	Aggregated | e.g. quarterly
Audit committee	Controls | each meeting
OR committee	By business line | e.g. monthly
Business line managers	Granular | frequent, even daily

IN THE LESSON

- Content is one dial.
- Two more are granularity, meaning how much detail, and frequency, meaning how often.
- The board gets the least detail, summarised and aggregated, and the least often, typically each quarter, in line with its meetings.
- The audit committee gets a report focused on controls and findings, for each of its meetings.
- The management committee gets detail by business line, more often, for example monthly.
- Business line managers get the most detail and the most often, sometimes daily, because they act on it at once.
- The exact timetable is a choice each bank makes, so remember the pattern, not the calendar: the higher the body, the shorter and less frequent its report.

5 Example 1: one quarter, four reports

Ashcombe's quarter: net loss $9.0m; appetite $12.0m a quarter

Board and risk committee	9.0 ÷ 12.0 of appetite	**75% used**
Audit committee	3 of 14 findings overdue	**21%**
OR committee	Payments, Retail, Markets	**3.0 / 3.9 / 2.1**
Payments line manager	outage cost $2.4m	**daily outage KRI**

IN THE LESSON

- Let us rebuild Ashcombe's quarter for each audience.
- Net operational losses were nine million dollars, against a quarterly appetite of twelve million.
- The board report says that nine over twelve, seventy five per cent of appetite, is used, and asks for one decision, on the payments platform.
- The audit committee sees that three of its fourteen open audit findings are overdue, about twenty one per cent.
- The management committee sees losses by business line: three million in payments, three point nine in retail and two point one in markets, which add up to the same nine million.
- The payments manager, whose outage cost two point four million, sees a daily indicator: minutes of outage.

6 One data source, and the mistakes to avoid

- Every report used the same $9.0m
- One consistent data source underneath
- Mistake: sending everyone the same report
- Mistake: burying decisions in detail
- Match content, detail, frequency to the body

IN THE LESSON

- Notice something in that example.
- Every report used the same nine million dollars.
- The board's total, the committee's split by business line and the manager's detail all came from one consistent data source underneath.
- If each report were built from its own spreadsheet, the numbers would disagree, and the meetings would argue about the data instead of the risk.
- Now the two usual mistakes.
- The first is sending everyone the same report, as Ashcombe did in our story.
- The second is burying decisions in detail, so the board never sees the question it must answer.
- For the exam, match content, granularity and frequency to the committee, all from that single source.

7 A story: the report that only looked back

- Every past loss listed, nothing else
- Board: what may go wrong next quarter?
- Rising turnover and failed trades were missing
- Classic weakness: a report of past losses only
- Combine backward- and forward-looking

IN THE LESSON

- Ashcombe's next report fixed the audience problem, but it had another flaw.
- It listed every loss of the past quarter in careful detail, and nothing else.
- A board member asked a simple question: what is likely to go wrong next quarter?
- The report could not say.
- Staff turnover in operations had been climbing for months, and failed trades were rising, but neither appeared anywhere.
- A report that only lists past losses is the classic weakness, because by the time a loss is booked, it is too late to prevent it.
- A good operational risk report combines backward looking information, about what has happened, with forward looking information, about what may happen.

8 Backward-looking items

What has already happened

Item	What it shows
Internal loss events	Gross, recoveries and net loss
Trends by event type	Which kinds of loss are rising
Trends by business line	Where losses are rising
External loss events	Losses at other firms

IN THE LESSON

- Start with the backward looking items.
- First, internal loss events, each with three figures.
- The gross loss is the full loss before anything is recovered.
- Recoveries are amounts got back, for example from insurance or from the other party.
- The net loss is gross minus recoveries.
- Second, trends, by event type, such as fraud or processing errors, and by business line, so the reader sees which way losses are moving and where.
- Third, relevant external loss events, meaning losses suffered at other firms that could happen here too.
- They show risks that the bank's own history has not yet revealed.

9 Example 2: gross, recoveries and net

Ashcombe's quarter by event type, $m: gross minus recoveries gives net

External fraud	3.2 − 0.8	**2.4**
Processing errors	4.5 − 0.9	**3.6**
System failures	3.0 − 0.0	**3.0**
Total gross and recoveries	3.2 + 4.5 + 3.0; 0.8 + 0.9	**10.7 and 1.7**
Total net loss	10.7 − 1.7	**$9.0m**

IN THE LESSON

- Here are Ashcombe's losses for the quarter by event type.
- External fraud caused a gross loss of three point two million dollars, of which point eight million was recovered, for a net loss of two point four million.
- Processing errors cost four point five million gross, with point nine recovered, so three point six net.
- System failures, including the payments outage, cost three million, with nothing recovered, so the net loss is also three million.
- In total, gross losses were ten point seven million, recoveries one point seven, and net losses nine million, the same figure the board saw.
- Showing all three figures matters, because a reader must know which basis a number is on.

10 Forward-looking items

What may happen next

Item	What it shows
Key risk indicators (KRIs)	Thresholds: green, amber, red
Self-assessments (RCSA)	Managers score risks, controls
Scenario analysis	Cost of severe, plausible events
Emerging risks, near misses	Warnings not yet in loss data
Operational risk capital	Capital held against the risk

IN THE LESSON

- Now the forward looking items.
- First, key risk indicators, or K R I s.
- These are metrics tracked regularly, such as failed trades or staff turnover, each with thresholds, often shown as green, amber and red.
- Second, the results of risk and control self-assessments, or R C S A, where managers score their own risks and controls.
- Third, scenario analysis, where experts estimate the cost of severe but plausible events.
- Fourth, emerging risks, which are new threats that are not yet in the data, and near misses, which are events that could have caused a loss but did not.
- Fifth, the capital held against operational risk.

11 Example 3: reading the indicators

Green below the first threshold, red above the second, amber between

Failed trades a day	green < 20, red > 40	**46: red**
Staff turnover a year	green < 10%, red > 15%	**12%: amber**
Downtime hours a month	green < 2, red > 6	**1.5: green**
Action on the red	owner, date, escalate	**to OR committee**

IN THE LESSON

- Here are three of Ashcombe's key risk indicators, each with its thresholds.
- Below the first threshold is green, above the second is red, and in between is amber.
- A reading exactly on a threshold counts as amber.
- Failed trades: green below twenty a day, red above forty.
- Today's reading is forty six, so red.
- Staff turnover: green below ten per cent a year, red above fifteen.
- The reading is twelve per cent, so amber, a warning to watch.
- System downtime: green below two hours a month, red above six.
- The reading is one and a half hours, so green.
- The red indicator needs action: a named owner, a date for the fix, and escalation to the management operational risk committee.

12 Good practice in reporting

- Link each item to risk appetite
- Show trends over time
- Give root causes, not just costs
- Name owners and remediation dates
- Escalate breaches clearly

IN THE LESSON

- What turns a list of items into a good report?
- First, link each item to risk appetite, so the reader sees not just a number but how close it is to the limit.
- Second, show trends over time, because one quarter's figure means little on its own.
- Third, give root causes, meaning why the loss happened and not just what it cost.
- Fourth, name an owner for each problem, with a date by which it will be fixed, called a remediation date.
- Fifth, escalate breaches clearly, so that a red indicator or an appetite breach reaches the right committee quickly and is not lost in the detail.
- Each of these turns information into action.

13 Example 4: a trend against appetite

Ashcombe's net losses, $m a quarter, against an appetite of $12.0m

Quarter 1	5.0 ÷ 12.0	**41.7% used**
Quarter 2	6.5 ÷ 12.0	**54.2% used**
Quarter 3	7.8 ÷ 12.0	**65.0% used**
Quarter 4	9.0 ÷ 12.0	**75.0% used**
If the last rise repeats	9.0 + 1.2 = 10.2	**85.0% used**

Up 80% in a year: every quarter is inside appetite, but the trend warns

IN THE LESSON

- Here is why trends matter.
- Ashcombe's net losses over four quarters were five million, six point five, seven point eight and nine million dollars, against an appetite of twelve million a quarter.
- Each quarter alone is inside appetite: forty one point seven, fifty four point two, sixty five and seventy five per cent used.
- A report showing only the latest quarter would say all is well.
- But losses have risen by eighty per cent in a year.
- If the latest rise of one point two million were repeated, next quarter would reach ten point two million, eighty five per cent of appetite.
- Shown as a trend, the same data gives early warning.

14 The qualities of a good report

- Accurate and timely
- Concise and comprehensible
- Same definitions each period
- Weakness: a report of past losses only
- Exam favours action and early warning

IN THE LESSON

- Finally, the qualities a report must have.
- It must be accurate, because a wrong number can drive a wrong decision.
- It must be timely, because a warning that arrives after the loss is useless.
- It must be concise and comprehensible, so a busy reader can understand it quickly and act.
- And it must use the same definitions each period, so that this quarter can be compared with the last.
- If the bank changes how it counts a loss, the trend breaks.
- Remember the classic weakness: a report that only lists past losses.
- The exam favours reports that support action and early warning, combining what has happened with what may happen.

15 Why operational risk is hard to report

- Market risk: one headline metric, VaR
- Market prices are observed every day
- Operational risk has no single metric
- Its information is heterogeneous
- And the loss data are awkward

IN THE LESSON

- Ashcombe's head of risk now tries to put operational risk on one page, the way the market risk team does.
- For market risk there is a single headline number, value at risk, or V a R: the loss the bank should not exceed on a given share of days.
- Prices are observed every day, so the data are plentiful.
- Operational risk has neither.
- Its information is heterogeneous, meaning made of different kinds: loss amounts, indicator readings, scores from self-assessments and expert scenarios.
- And the loss data themselves are awkward, as we will see.
- Operational risk reporting faces obstacles that market risk reporting largely avoids.

16 Five obstacles and their remedies

Exams pair each obstacle with its remedy

Obstacle	Remedy
Scarce data in the tail	External data, scenario analysis
Under-reporting, fear of blame	No-blame culture, ledger checks
Losses booked long after	Record all three dates
Optimistic self-assessments	Independent challenge, evidence
No single metric	Common taxonomies, rating scales

IN THE LESSON

- Here are the five obstacles, each paired with its remedy.
- First, loss data are scarce in the tail, because severe events are rare.
- The remedy is to add external data and scenario analysis.
- Second, events are under-reported when staff fear blame.
- The remedies are a no-blame culture and reconciling loss records to the general ledger.
- Third, losses are discovered and booked long after they occur, so the bank records all three dates.
- Fourth, self-assessments are subjective and optimistic, so they need independent challenge and comparison with evidence.
- Fifth, there is no single metric, so the bank uses common taxonomies and rating scales.
- Expect exam questions that pair an obstacle with its remedy.

17 Example 5: the empty tail

Ashcombe, ten years of internal loss data

Internal events, 10 years	all sizes	**2,400**
Events above $5m	1 of 2,400	**0.04%**
Largest internal loss	the tail is almost empty	**$6.2m**
Peer events above $20m	external database	**38**
Scenario: rogue trading	expert workshop estimate	**$45m**

IN THE LESSON

- Let us see how thin the tail is.
- Over ten years Ashcombe has recorded two thousand four hundred loss events of all sizes.
- Only one was above five million dollars, about four hundredths of one per cent of all events.
- The largest internal loss was six point two million.
- Yet the losses that threaten a bank are far larger and far rarer, and ten years of its own history says little about them.
- So Ashcombe adds external data: a shared database records thirty eight events above twenty million at peer banks.
- And it runs scenario analysis: a workshop estimates that a rogue trading event could cost forty five million.
- Together they fill the tail that internal data leave empty.

18 Under-reporting and the ledger check

- Staff who fear blame hide errors
- The database looks better than reality
- Remedy 1: a no-blame culture
- Remedy 2: reconcile to the general ledger
- Near misses depend on culture alone

IN THE LESSON

- The second obstacle is human.
- If staff fear blame, they hide small errors, and the loss database misses events.
- The losses still happen, and the money still leaves the bank, so the database looks better than reality.
- Two remedies work together.
- The first is a no-blame culture, where reporting a mistake is expected and even rewarded, and the punishment is for hiding one.
- The second is a mechanical check: reconcile the loss records to the general ledger, the bank's main accounting records.
- A loss that reached the accounts but not the loss database is a sign of under-reporting.
- Near misses depend on the same culture, because no ledger records them.

19 Example 6: reconciling to the ledger

One quarter two years ago: general ledger vs loss database, $m

General ledger: op losses	write-offs, compensation	**$8.2m**
Loss database	events recorded	**$6.7m**
Unrecorded gap	8.2 − 6.7	**$1.5m**
Share never reported	1.5 ÷ 8.2	**18.3%**
Action	trace each item to an event	**record, ask why**

IN THE LESSON

- Here is a reconciliation Ashcombe ran for one quarter two years ago, before it worked on its culture.
- The general ledger accounts that collect operational losses, such as write-offs of errors and compensation paid to clients, show eight point two million dollars.
- The loss database shows only six point seven million.
- The gap is one point five million dollars.
- One point five over eight point two means about eighteen point three per cent of the ledger losses never reached the loss database.
- The remedy is to trace each unmatched ledger item back to an event, record it, and ask why it was missed.
- If one team keeps appearing, the problem may be a culture of blame in that team, not a gap in the system.

20 Three dates for every loss

- Occurrence: when the event happened
- Discovery: when someone noticed it
- Booking: when it reached the accounts
- Trend by booking date understates recent risk
- Remedy: record all three dates

IN THE LESSON

- The third obstacle is timing.
- An operational loss has three dates.
- The occurrence date is when the event happened.
- The discovery date is when someone noticed it.
- The booking date, or accounting date, is when the loss was recorded in the accounts.
- These can be months or even years apart, for example when a fraud runs quietly before it is found.
- If the bank shows its trend by accounting date only, recent quarters look better than they are, because their losses have not yet been found or booked.
- So a trend by accounting date understates recent risk.
- The remedy is to record all three dates for every event.

21 Example 7: when did the loss happen?

One event: a $3.0m pricing error. Where does it fall?

Occurred	the error begins	**Feb: quarter 1**
Discovered	found in a review	**Jul: quarter 3**
Booked	loss recorded in accounts	**Oct: quarter 4**
Q1 by booking date	nothing from this event	**$0**
Q1 by occurrence date	once the event is found	**$3.0m**

IN THE LESSON

- Take one Ashcombe event.
- A pricing error in a retail product began in February, in quarter one.
- It was discovered in a review in July, in quarter three.
- The loss of three million dollars was booked in October, in quarter four.
- Now look at the quarter one figure.
- Built by booking date, quarter one shows nothing from this event, and the report for quarter one looked clean.
- Built by occurrence date, quarter one carries the full three million once the event is found.
- The risk was present in quarter one, and only the occurrence date shows it.
- The discovery date adds a separate lesson: a five month gap from start to discovery suggests weak detection, and a further three months to booking shows slow recording.

22 Optimistic self-assessments

- Managers score their own risks and controls
- Scores are subjective and optimistic
- Remedy 1: second-line challenge
- Remedy 2: compare with loss data and KRIs
- When they disagree, the evidence wins

IN THE LESSON

- The fourth obstacle is opinion.
- In a risk and control self-assessment, managers score their own risks and controls.
- The scores are subjective, and they tend to be optimistic: no manager likes to report that their own controls are weak.
- Left alone, the R C S A gives a reassuring picture that may not be true.
- The remedy has two parts.
- First, independent challenge, usually by the second line, meaning the independent risk function, which questions the scores.
- Second, comparison with harder evidence: the loss data and the key risk indicators.
- When a control is rated strong but the losses and indicators say otherwise, the evidence wins.

23 Example 8: challenging a self-assessment

Markets desk rates its settlement risk 1 = low, on a scale of 1 to 4

Desk's own rating	self-assessment	**1 = low**
Failed trades KRI	red in 3 of the last 4 months	**red**
Losses vs tolerance	2.1 ÷ 0.5	**4.2 times**
After second-line challenge	evidence over opinion	**3 = high**

IN THE LESSON

- Ashcombe's markets desk rates its trade settlement risk as low, a score of one on a scale from one to four, where four is the worst.
- Now the evidence.
- The failed trades indicator has been red in three of the last four months.
- Losses from settlement errors this year are two point one million dollars, against a tolerance of half a million, which is four point two times the tolerance.
- The second line challenges the rating.
- With the evidence on the table, the risk is rated three, high, and an action plan with an owner follows.
- The point is not that managers lie.
- Their view needs testing against data.

24 No single metric: speaking one language

- No single metric like VaR
- Losses, KRIs, scores, scenarios: different units
- Common taxonomy: one list of types
- Common rating scales: e.g. 1 to 4
- Then the whole bank fits on one page

IN THE LESSON

- The last obstacle is the one we began with.
- There is no single metric like V a R, so the report must combine dollars of loss, indicator readings, self-assessment scores and scenario estimates.
- Mixed carelessly, they cannot be added up or compared.
- The remedy is a common language.
- A common taxonomy means one agreed list of risk and event types, used by every business line, so a processing error in retail is filed the same way as one in markets.
- Common rating scales, such as one to four for likelihood and impact, let scores from different teams be compared and combined.
- Then the board can see the whole bank on one page.

25 Who outside the bank reads the reports

Each outside reader gets a different depth

Reader	What it gets
Supervisors	Detailed and confidential
Investors	Public disclosure, summarised
Rating agencies	Disclosures, plus meetings
External auditors	The figures and controls

IN THE LESSON

- Now we look outside the bank.
- External reporting serves regulators and other outside stakeholders, and each gets a different depth.
- Supervisors, meaning the regulators who oversee the bank, receive detailed and confidential information.
- Investors read the public disclosures, to judge whether the bank is sound and fairly priced.
- Rating agencies use the same disclosures, together with their own meetings with management, to rate the bank's debt.
- And the external auditors examine the figures and the controls behind them.
- The deepest view goes to the supervisor, and the public sees a summary.
- The rest of this part looks at the two main channels: the supervisor and public disclosure.

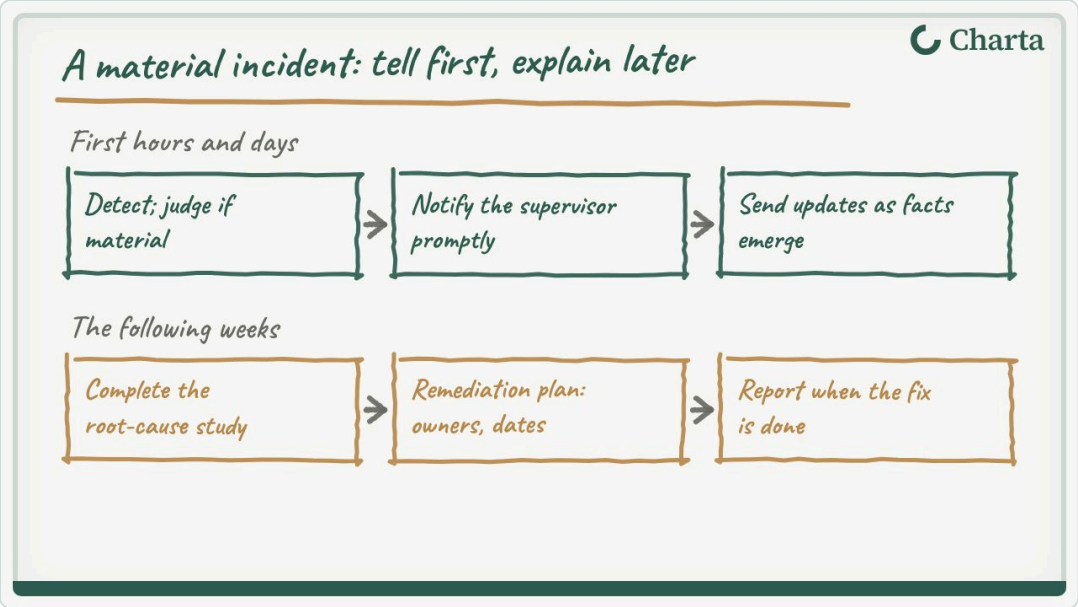
26 What the supervisor receives

- Event-level loss data
- Capital calculations
- Remediation plans with owners and dates
- Prompt notice of material incidents
- Do not wait for a full root-cause study

IN THE LESSON

- What does a supervisor receive?
- First, event level data, meaning the individual loss events, not just the totals.
- Second, the capital calculations, so the supervisor can check how much capital the bank holds against operational risk and how it got there.
- Third, remediation plans, showing what the bank is doing to fix its weaknesses, with owners and dates.
- Fourth, and most urgent, prompt notice of material incidents.
- A material incident, such as a major outage or a large fraud, must be reported quickly, without waiting for a full root cause study.
- The exact deadline varies by jurisdiction, so remember the principle: tell the supervisor promptly, then follow up.

27 A material incident: tell first, explain later



IN THE LESSON

- Here is how Ashcombe handles a material incident, such as its payments outage.
- Look at the boxes.
- The top row is the first hours and days.
- The incident is detected, and the bank judges whether it is material.
- If it is, the bank notifies the supervisor promptly, with what it knows so far.
- Then it sends updates as the facts become clear.
- The bottom row is the following weeks.
- The bank completes its root cause study, sets out a remediation plan with owners and dates, and finally reports to the supervisor when the fix is done.
- The common error is to reverse the order, waiting for the full story before saying anything at all.

28 Public disclosure under Pillar 3

- Purpose: market discipline
- Clear, comprehensive, meaningful
- Consistent over time, comparable across banks
- Governance, loss history, capital, summarised
- No client names or sensitive internal detail

IN THE LESSON

- Public disclosure follows a different logic.
- Under Pillar three of the Basel framework, banks publish information so that markets can judge their risk, which is called market discipline: investors and lenders reward sound banks and charge more to risky ones.
- For that to work, disclosure should be clear, comprehensive and meaningful, consistent over time and comparable across banks.
- On operational risk it covers governance, loss history and capital, in summarised form.
- Client names and sensitive internal detail are not disclosed.
- A public document that named the client in a fraud, or explained exactly which control failed, could harm clients and invite new attacks.

29 Example 9: gross, net and one set of figures

Ashcombe's year, $m. Two reports show different totals

Gross loss for the year	before recoveries	**$34.8m**
Recoveries	mainly insurance	**$6.5m**
Net loss	34.8 − 6.5	**$28.3m**
Gap between the reports	basis, not error	**$6.5m**

State the basis: gross or net of recoveries

IN THE LESSON

- Figures given to the regulator, the public and the board must reconcile, meaning they can be traced back to each other.
- Suppose Ashcombe's gross operational losses for the year were thirty four point eight million dollars, and recoveries, mainly insurance, were six and a half million.
- Net losses were therefore twenty eight point three million, the sum of the four quarters we saw earlier.
- Now suppose one report states thirty four point eight million and another states twenty eight point three.
- An analyst might cry inconsistency.
- But the gap is exactly the six and a half million of recoveries: one figure is gross, the other net.
- There is no error, provided each report states its basis.
- That is why the basis must always be stated.

30 Mistakes to avoid in external reporting

- Treating a difference in basis as inconsistency
- Concealing an exposure because it is uncertain
- Waiting for root cause before notifying
- Client names in public
- Each outside reader gets the depth it needs

IN THE LESSON

- Four mistakes to avoid.
- First, treating a difference in basis as an inconsistency, as in the example: gross and net figures differ by the recoveries, and that is not an error.
- Second, concealing a material exposure because the outcome is uncertain.
- A bank facing a large legal claim may hope to win, but the uncertainty is a reason to disclose with care, not to stay silent.
- Third, waiting for a full root cause study before notifying the supervisor.
- Fourth, giving the public sensitive detail, such as client names, that belongs only in confidential reports.
- Each audience outside the bank, like each committee inside it, gets the depth it needs.

31 Recap: the main ideas

- Start from the audience; one data source
- Backward- and forward-looking items
- Link to appetite; trends, owners, dates
- Five obstacles, five remedies
- Supervisors: detail. Public: summary

IN THE LESSON

- Let us pull it together.
- Reporting starts from the audience.
- The board wants exposure against appetite and the decisions it must take, the audit committee wants control findings and overdue fixes, the management committee wants detail by business line, and line managers want granular, frequent data, all from one data source.
- A good report combines backward looking losses with forward looking indicators, self-assessments, scenarios and capital, linked to appetite, with trends, owners and dates.
- The obstacles are scarce tail data, under-reporting, late booking, optimistic self-assessments and no single metric, and each has a remedy.
- Outside, supervisors get detail and prompt notice, and the public gets a summary on a stated basis.

32 Try three quick questions

1. Gross loss $5.0m; insurance recovers $1.2m. Net loss?
   Answer: 5.0 − 1.2 = $3.8m.
2. Ledger shows $4.0m of op losses; database $3.4m. Share unrecorded? Obstacle?
   Answer: 0.6 ÷ 4.0 = 15%: under-reporting. Fix: no-blame, ledger checks.
3. Which committee most wants overdue audit remediation?
   Answer: The audit committee.

IN THE LESSON

- Now try three quick questions.
- Pause the video, think, then listen to the answers.
- Question one.
- An internal fraud causes a gross loss of five million dollars, and insurance recovers one point two million.
- What is the net loss?
- Five minus one point two, which is three point eight million dollars.
- Question two.
- The general ledger shows four million dollars of operational losses, but the loss database shows three point four million.
- What share went unrecorded, and which obstacle does it point to?
- Point six over four is fifteen per cent, which points to under-reporting, so a no-blame culture and regular ledger checks are needed.
- Question three.
- Which committee most wants to know that remediation of audit findings is overdue?
- The audit committee.