CHARTA LEARNING · LESSON NOTES

# Data aggregation and risk reporting: the Basel principles

FRM Part I

## 1 A story: the question nobody could answer

- A key client fails on Monday morning
- Question: what is our total exposure to it?
- Loans, derivatives, trading, branches: separate systems
- Several different answers, and days of delay

IN THE LESSON

- Picture a large bank on a bad Monday morning.
- A big client has just failed.
- The chief risk officer asks a simple question: how much do we have at risk with this client, across the whole group?
- It sounds easy.
- But the loans sit in one system, the derivatives in another, the trading desk in a third, and the overseas branch keeps its own records.
- Each team replies with a different number, and none of them can say how the numbers fit together.
- Two days pass before anyone can give a firm answer.
- By then the market has moved.
- This is the problem our topic is about.

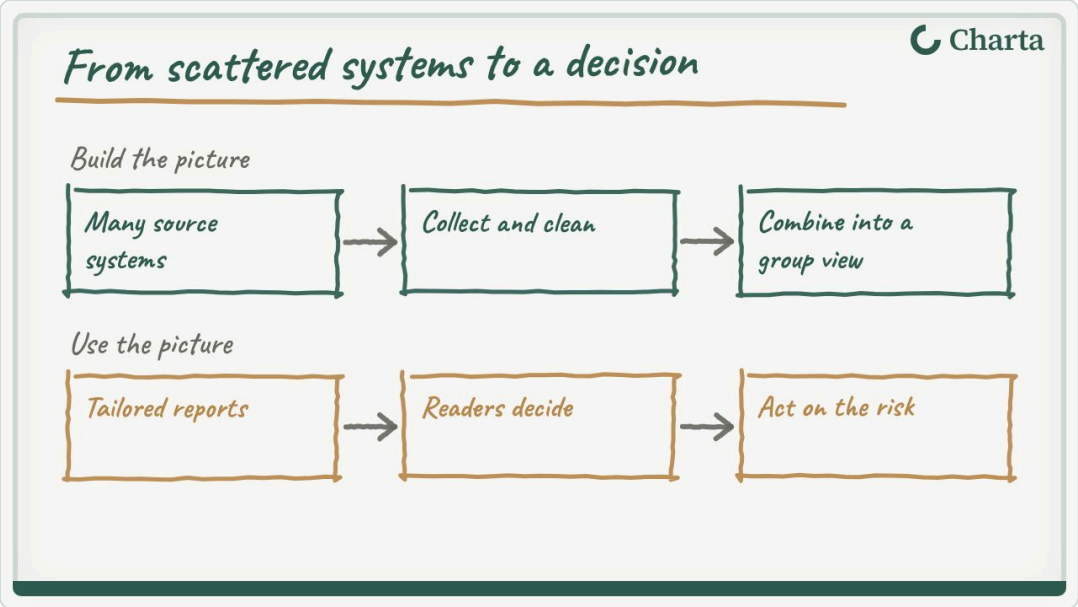
## 2 What the topic means in plain words

- Aggregation = gather exposures from all entities and risks
- Reporting = present the picture to those who must act
- Done well, reports are accurate, quick and usable
- A right number that arrives late is little use

IN THE LESSON

- Let's define the two ideas.
- Risk data aggregation means gathering a firm's risk figures from every legal entity, every business line and every type of risk, and putting them together into one reliable picture.
- Risk reporting is what happens next: presenting that picture to the people who must act on it, such as the board, senior managers, and the supervisors.
- A firm does both well when its reports are accurate, quick and usable.
- Notice that three words.
- Accurate means the numbers are right.
- Quick means they arrive while they still matter.
- Usable means the reader can understand them and act.

## 3 From scattered systems to a decision




IN THE LESSON

- Here is the path the data must travel.
- On the top row, the raw figures start in many places: trading books, loan systems, collateral records, and the separate legal entities of the group.
- They are first collected and cleaned, so that each exposure is counted once and in the same units.
- Then they are combined into a group view, by counterparty, by business line, by region, and by risk type.
- On the bottom row, that view becomes reports, tailored to each reader, and the readers decide: reduce a limit, hedge, raise more capital, or do nothing.
- Each step can fail, and a weak step spoils everything after it.

## 4 Where the principles come from

- Issued by the Basel Committee in 2013: B C B S 239
- Reaction to the 2008 crisis
- Many banks could not see total exposures quickly
- The data existed, but could not be assembled in time
- The principles describe what good capability looks like

IN THE LESSON

- The standard here comes from the Basel Committee on Banking Supervision, the international group of bank supervisors.
- It issued its principles for effective risk data aggregation and risk reporting in twenty thirteen.
- They are usually known by their document number, B C B S two thirty nine.
- The reason was the financial crisis of two thousand eight.
- When it struck, many banks discovered that they could not quickly identify their total exposures to particular borrowers or to each other.
- The information existed somewhere inside the firm, but it could not be assembled in time.
- The principles set out what good looks like, in a set of fourteen principles.

## 5 The advantages of effective aggregation and reporting

*Gains named in the principles*

| Advantage | What improves |
|---|---|
| Faster, better-informed decisions | Decision quality |
| Problems anticipated earlier | Early warning |
| Complete data quickly in stress | Resilience, resolution |
| Less manual reconciliation | Efficiency, fewer losses |
| Better risk and return view of deals | Strategy |

**IN THE LESSON**

- What does a firm gain?
- The principles list several advantages, and this table gathers them.
- First, management decides faster and on better information.
- Second, problems are anticipated earlier, because patterns show up before they become losses.
- Third, in a stress, complete information is available quickly, which supports crisis management and, if the worst happens, the orderly resolution of a failing bank.
- Fourth, manual reconciliation falls, so the firm is more efficient, and the probability and severity of losses fall too.
- Fifth, strategic planning improves, including the ability to judge the risk and return of new products, acquisitions and mergers.
- Remember them as better decisions, resilience and efficiency, with earlier warning and better strategy counted as part of better decisions.

## 6 Example 1: one counterparty, four entities

*Illustration: group limit on one client is $90m*

| | | |
|---|---|---|
| **Retail bank** | exposure | **$40m** |
| **Investment bank** | exposure | **$30m** |
| **Overseas branch** | exposure | **$20m** |
| **Derivatives desk** | exposure | **$20m** |
| **Group total** | 40 + 30 + 20 + 20, limit 90 | **$110m** |

**IN THE LESSON**

- Let's make the first gain concrete with made up numbers.
- A bank group has a limit of ninety million on its exposure to one client.
- The exposures sit in four places: the retail bank holds forty, the investment bank holds thirty, the overseas branch holds twenty, and a derivatives desk holds twenty more.
- No single entity is over the limit; each is far below ninety.
- A bank with weak aggregation sees only these four comfortable figures.
- A bank with strong aggregation adds them up on day one and sees one hundred and ten million, which is twenty million over the limit.
- The problem is caught early, while it can still be fixed cheaply.

## 7 Example 2: the efficiency gain

*Illustration: 40 reports a month*

| | | |
|---|---|---|
| **Before: manual** | 40 reports x 3 hours | **120 hours** |
| **After: automated** | 40 reports x 1 hour | **40 hours** |
| **Hours saved** | 120 − 40 | **80 hours** |
| **Share saved** | 80 ÷ 120 | **about 67%** |

**IN THE LESSON**

- The second gain is efficiency.
- Imagine a risk team that produces forty reports each month.
- With fragmented systems, each report needs three hours of copying, checking and matching numbers by hand.
- That is one hundred and twenty hours a month.
- After the firm builds one integrated source and automates the feeds, each report needs one hour, mostly for review.
- That is forty hours.
- The saving is eighty hours every month, and the freed analysts can study the risks instead of fixing spreadsheets.
- There is a quieter benefit too.
- Every manual step is a chance for a typing mistake, so fewer manual steps also means fewer errors, and fewer errors mean lower losses.

## 8 What the principles do not promise

- No promise of lower capital charges
- The gains: decision quality, resilience, efficiency
- It is not just a compliance cost
- It is not just an I T project: it is a business capability

**IN THE LESSON**

- Before moving on, two common misunderstandings.
- First, the principles do not promise lower capital charges.
- The benefits are decision quality, resilience and efficiency.
- A bank may well hold the same capital as before; it simply knows its risks better.
- Second, do not treat the topic as a compliance cost or a pure I T project.
- Compliance is part of it, and technology is a tool, but the real aim is a business one: better decisions and a firm that survives stress.
- A bank that sees it only as a box to tick will build the minimum, and will find the gaps again at the worst moment.

## 9 Why a robust process is hard to build

- Growth by acquisition leaves fragmented legacy systems
- Risk data sit in many places and countries
- Systems were never built to talk to each other
- Replacement is huge and slow, and the bank keeps running

**IN THE LESSON**

- Now the second question: if the gains are so clear, why do many banks still struggle?
- The first reason is history.
- Large banks have grown through acquisitions, and each acquired firm brought its own systems.
- The result is a patchwork of fragmented legacy systems that were never designed to talk to each other.
- The second reason is that risk data sit in many places at once, across business lines, legal entities and countries, each with its own habits and local rules.
- Replacing the patchwork is possible, but it is a huge, slow project, and while it runs the business must keep operating on the old systems.

## 10 Five reasons it is hard

*Obstacles to aggregation*

| Obstacle | Effect |
|---|---|
| Different data definitions | Numbers do not match |
| Different counterparty identifiers | Client seen many times |
| Manual processes, spreadsheets | Slow, error-prone |
| Unclear ownership of data quality | Nobody fixes it |
| Costly, slow investment | Loses to revenue |

**IN THE LESSON**

- Here are the five obstacles in one place.
- Definitions differ: one business counts an exposure before collateral, another after.
- Counterparty identifiers and taxonomies differ, so the same client may carry several names or codes.
- Much gets stitched together by manual processes and spreadsheets, which are slow and fragile.
- Ownership of firm wide data quality is often unclear, because each business optimises for its own needs and nobody owns the whole.
- And the investment is costly, slow, and competes with revenue projects, so it keeps being pushed down the list.
- Notice that only some of these are technical.
- Definitions, ownership and priorities are management problems.

## 11 Example 3: one client, three names

*Illustration: single-name limit $60m*

| | | |
|---|---|---|
| **Acme Holdings** | seen as borrower 1 | **$40m** |
| **Acme Holdings Limited** | seen as borrower 2 | **$35m** |
| **Acme International** | seen as borrower 3 | **$25m** |
| **True exposure to one group** | 40 + 35 + 25 | **$100m** |
| **Excess over the limit** | 100 − 60 | **$40m** |

IN THE LESSON

- Let's see an identifier problem with made up numbers.
- A client appears in three systems as Acme Holdings, Acme Holdings Limited, and Acme International.
- Because the names and codes differ, the systems treat them as three unrelated borrowers.
- The exposures are forty, thirty five, and twenty five million.
- The bank's single name limit is sixty million.
- Each record on its own is below the limit, and the largest looks like only forty.
- Once the identifiers are linked, the true exposure to this one group is one hundred million, forty million over the limit.
- The concentration was there all the time; the data simply could not show it.

## 12 Example 4: double counting

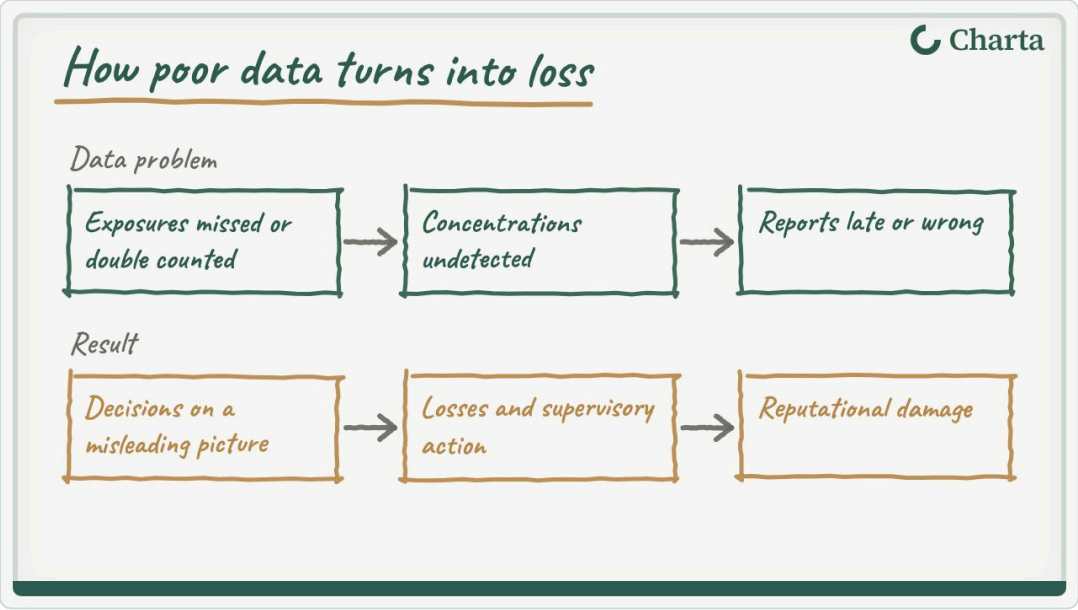
*Illustration: same trade in two systems*

| | | |
|---|---|---|
| **Trade in trading system** | exposure | **$30m** |
| **Same trade in credit system** | exposure | **$30m** |
| **Other exposures** | to the client | **$70m** |
| **Naive total** | 70 + 30 + 30 | **$130m** |
| **True total** | 70 + 30 | **$100m** |

IN THE LESSON

- The opposite error is just as harmful.
- Suppose a derivative trade with a client is booked in the trading system, and the same trade also appears in the credit system because both systems record the same trade.
- Each system reports thirty million for the trade.
- Other exposures to this client are seventy million.
- A careless sum of everything gives one hundred and thirty million, which is thirty million too high.
- The true figure is one hundred million.
- Overstating exposure can be costly too: the bank may refuse good business, or sell positions it did not need to sell.
- Aggregation needs the trade counted once, and counted in the right place.

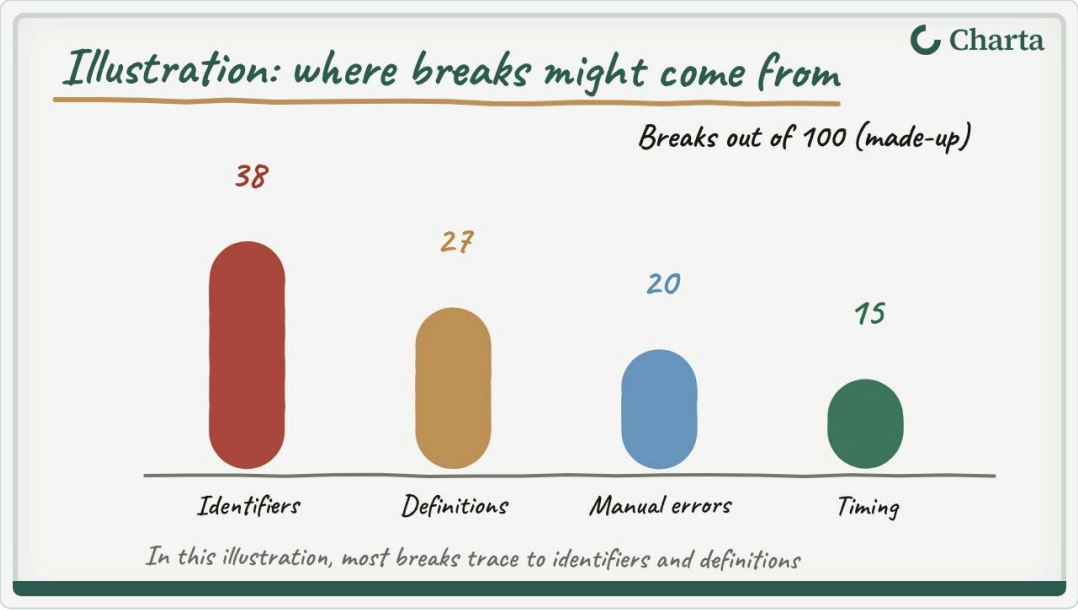
## 13 How poor data turns into loss




**IN THE LESSON**

- This chain shows the practical consequences.
- On the top row, poor data means exposures to the same counterparty are missed or double counted, and concentrations go undetected.
- The reports built on those data arrive late, or arrive wrong.
- On the bottom row, managers and the board then make decisions on a misleading picture.
- They lend too much to a name that is already too large, or they cut back where there was no need.
- The final links are real losses, action by supervisors, and damage to the reputation of the firm.
- Each link follows naturally from the one before, which is why the chain has to be broken at the start.

## 14 Illustration: where breaks might come from




IN THE LESSON

- Here is a made up picture of how reconciliation breaks might split in a bank.
- Suppose a team investigates one hundred breaks, which are cases where two systems disagree on the same exposure.
- They find thirty eight caused by differing counterparty identifiers, twenty seven by differing definitions, twenty by manual handling errors, and fifteen by timing, where one system was updated and the other was not.
- The shares add up to one hundred.
- In this illustration, most breaks come from identifiers and definitions, which are governance and design problems, rather than from faulty arithmetic.
- Fixing the roots removes many breaks at once, while chasing individual breaks never ends.

## 15 Poor data quality is a risk in itself

- Poor data quality is a risk in its own right
- It weakens control of credit, market and every other risk
- 2008: banks could not see total exposures quickly
- Result: losses, supervisory action, reputation hit

IN THE LESSON

- Let's draw the lesson of this section together.
- Poor data quality is not just a nuisance that makes reporting untidy; it is a risk in itself.
- It is a risk in its own right, and it weakens the control of credit risk, market risk and every other risk, because the firm cannot manage what it cannot see.
- This was the experience in two thousand eight, when banks were unable to see their total exposures quickly, at the moment when speed mattered most.
- Poor data can therefore lead to losses, to supervisory action, and to reputational damage, even when the underlying business is sound.
- That is why the Basel Committee wrote principles for it.

## 16 Governance: the first principle

- Principle 1: governance, the overarching principle
- Board and senior management are responsible
- Strong governance of aggregation and of reporting
- Not the I T department alone, and not the vendor

IN THE LESSON

- Now we turn to governance.
- In the Basel framework, governance is the first and overarching principle, and the others rest on it.
- It says that a bank's board and senior management are responsible for ensuring that its risk data aggregation capabilities and its risk reporting practices are subject to strong governance, consistent with all the other principles.
- The key word is responsible.
- Not the I T department alone, and not a software vendor.
- The people who run the bank and the people who oversee them must care about the quality of the information they use, because they are the ones who answer for the decisions made with it.

## 17 What the board and senior management must do

*Duties under the governance principle*

| Duty | In practice |
|---|---|
| Understand limitations | Know the limits |
| Approve remediation plans | Sign off the fixes |
| Provide adequate resources | Money, people, tools |
| Assign data ownership | Named accountable owners |
| Weigh strategic decisions | Mergers, I T changes |

IN THE LESSON

- So what does strong governance mean in practice?
- This table lists the duties.
- They must understand the limitations that prevent full aggregation, and approve plans to fix them.
- They must provide adequate resources, in money and in skilled people.
- They must assign data ownership, so that somebody is accountable for the quality of each data set.
- And they must consider the effect on aggregation of strategic decisions, such as acquisitions and changes to information technology, before taking those decisions rather than after.
- An acquisition that doubles the number of systems is a strategic decision with a data consequence, and the board should see that consequence in advance.

## 18 Documentation, validation and outsourcing

- Capabilities are fully documented
- High validation standards
- Independent validation, by non-producers of the data
- Outsourcing covered: the bank stays responsible

IN THE LESSON

- Governance also covers how the capabilities themselves are treated.
- They should be fully documented, and they should be subject to high standards of validation.
- That includes independent validation: review by people who do not produce the data, because producers tend to trust their own work.
- The principles extend to outsourced processes as well.
- If a bank hands part of its data work to a vendor, it keeps the responsibility.
- The vendor is a supplier, not a shield, and the bank must still be able to show that the outsourced work meets the same standards as work done in house.
- Responsibility cannot be passed to someone else by contract.

## 19 Classification exercise: who is responsible?

*Scenarios: where does responsibility sit?*

| | | |
|---|---|---|
| **Vendor loads data wrongly** | who is responsible? | **The bank** |
| **Desk certifies its own data** | is it independent? | **No** |
| **Acquisition adds six systems** | who weighs the effect? | **The board** |
| **Known gap blamed on I T** | who approves the fix? | **Management** |

IN THE LESSON

- Let's practise with four short scenarios, and decide where responsibility sits under the governance principle.
- In the first, an outsourced vendor loads data wrongly.
- Responsibility stays with the bank, not the vendor.
- In the second, the head of a trading desk checks her own data quality and certifies it.
- That is not independent validation; the check needs to be done by people who do not produce the data.
- In the third, a planned acquisition will add six incompatible systems.
- The board must weigh the aggregation effect before it approves the deal.
- In the fourth, a known data gap is blamed on the technology team.
- The board and senior management must understand the gap and approve a plan to close it.

## 20 Principle two: architecture and infrastructure

- Principle 2: architecture and I T infrastructure
- Must fully support aggregation and reporting
- In normal times and in times of stress or crisis
- Designing only for normal conditions is a mistake

IN THE LESSON

- Next, systems.
- The second principle requires data architecture and I T infrastructure that fully support risk data aggregation and reporting, both in normal times and in times of stress or crisis.
- Those last words are important.
- It is easy to build a system that works on a quiet Tuesday.
- The test is the day when markets are falling, volumes are huge, and every manager wants a new report at once.
- The principle says the infrastructure must still deliver.
- A design that only works in normal conditions fails the principle, because stress is exactly when the information is needed most.

## 21 Features of sound data architecture

*Principle 2: design features*

| Feature | Problem it addresses |
|---|---|
| Integrated taxonomies, group wide | Definitions, IDs differ |
| Documented definitions | Guesswork |
| Named data owners | Unclear ownership |
| Minimal manual intervention | Spreadsheet stitching |

IN THE LESSON

- What does sound design look like?
- There are four main features.
- First, integrated data taxonomies and architecture across the whole banking group, so that a word like exposure means the same thing everywhere.
- Second, documented definitions, so nobody has to guess.
- Third, named data owners, so that accountability is clear.
- Fourth, as little manual intervention as possible, because each manual step is slow and each is a chance for error.
- Think of these as answers to the obstacles we met earlier: different definitions and identifiers, guesswork, unclear ownership and heavy reliance on spreadsheets.
- Good architecture is the direct answer to each of them.

## 22 Accuracy and a single authoritative source

- Principle 3: accuracy and integrity
- Strive for one authoritative source for each type of risk
- Without it, systems disagree and people argue
- Other systems reconcile back to it

IN THE LESSON

- Principle three covers accuracy and integrity.
- Among its points is this: a bank should strive for a single authoritative source of risk data for each type of risk.
- Why?
- Because when two systems both claim to hold the number, they will sooner or later disagree, and then people argue about which is right instead of managing the risk.
- With one authoritative source, every report draws from the same place, so reports agree with each other.
- Other systems may still hold copies, but they are checked against the authoritative one.
- This is the idea behind reconciliation: comparing a figure with its authoritative source and explaining any difference.

## 23 Measuring a reconciliation break

**Break % = (System total − Authoritative total) ÷ Authoritative total**

| | |
|---|---|
| **Break %** | Gap as share of trusted figure |
| **System total** | Figure in the system checked |
| **Authoritative total** | Figure in the trusted source |
| **Break** | The gap to explain |

IN THE LESSON

- We can measure how far a system strays with a simple formula.
- The reconciliation break is the difference between the figure in a system and the authoritative figure.
- Dividing it by the authoritative total gives the break as a share, so that big and small portfolios can be compared on the same basis.
- A small share suggests the system is reliable, while a large one suggests a problem with definitions, timing or identifiers.
- The sign matters too.
- A positive break means the system shows more than the authoritative source, which may mean double counting.
- A negative break means it shows less, which may mean something was missed.

## 24 Example 5: reconciling three systems

*Illustration: authoritative total $400m*

| | | |
|---|---|---|
| **Credit system** | 415 − 400 = +15 | **+3.75%** |
| **Trading system** | 410 − 400 = +10 | **+2.5%** |
| **Finance ledger** | 396 − 400 = −4 | **−1.0%** |
| **Largest break to explain** | credit system | **$15m** |

IN THE LESSON

- Let's reconcile with made up numbers.
- The authoritative source says that total derivative exposure for a client group is four hundred million.
- The credit system shows four hundred and fifteen million, the trading system shows four hundred and ten, and the finance ledger shows three hundred and ninety six.
- The breaks are plus fifteen, plus ten, and minus four.
- As shares of four hundred, these are three point seven five per cent, two point five per cent, and minus one per cent.
- The credit system is the worst.
- Its excess is likely double counting, while the finance ledger being low suggests something was missed.
- Each break must be investigated and explained, not simply averaged away.

## 25 Good practice in risk reporting: five features

*Principles for risk reporting*

| Feature | Meaning |
|---|---|
| Accurate and precise | Numbers can be trusted |
| Comprehensive | All material risks, forward looking, stress |
| Clear and useful | Data, analysis and commentary |
| Frequency fits the need | More often in stress |
| Right people, confidential | Distribution controlled |

IN THE LESSON

- Now the other half of the topic: the reports themselves.
- Good practice has five features.
- First, reports are accurate and precise, so decisions rest on solid numbers.
- Second, they are comprehensive across all material risk areas, including forward looking information and stress results, not only the past.
- Third, they are clear and useful to each recipient, balancing data, analysis and commentary.
- Fourth, their frequency matches the need, and rises in stress, so the board may want daily figures in a crisis.
- Fifth, they go to the right people, with confidentiality preserved.
- If you can remember accurate, comprehensive, clear, timely and well distributed, you have all five.

## 26 Example: one data set, four readers

*Illustration: one data set, four readers*

| | | |
|---|---|---|
| **Board** | summary and stress | **Weekly/monthly** |
| **Desk head** | positions, limit use | **Daily** |
| **Supervisor** | comprehensive, confidential | **As required** |
| **Board in a crisis** | key exposures, liquidity | **Daily+** |

IN THE LESSON

- A common mistake is to send the same report to everyone.
- Let's tailor four.
- The board needs a short summary of the largest risks against its appetite, with forward looking and stress results, and commentary explaining what matters, perhaps weekly or monthly in normal times.
- A desk head needs detailed positions and limit use, every day.
- The supervisor needs the comprehensive picture, with confidentiality respected, as required.
- In a crisis, all of the frequencies rise, and the board may now want a daily view of liquidity and key exposures.
- The same data feed all four reports, but each reader gets a different cut, at a different pace.
- A report that is perfectly accurate but unreadable to its recipient has failed.

## 27 Five mistakes to avoid

- Treating it as only a compliance cost or an I T project
- Expecting lower capital charges from the principles
- Putting responsibility on I T or the vendor
- Designing only for calm times
- Sending one report to all readers

IN THE LESSON

- Let's collect the common errors.
- The first mistake is to treat the topic as a compliance cost or a pure I T project, when it is about decision quality, resilience and efficiency.
- The second is to believe the principles promise lower capital charges; they do not.
- The third is to put responsibility on I T or on a vendor, when it sits with the board and senior management, even for outsourced work.
- The fourth is to design only for normal conditions, when infrastructure must work under stress.
- The fifth is to send the same report to everyone, when reports must suit each user.
- Keep these five in mind, and you will avoid the common errors.

## 28 Recap: the whole topic in one page

- Gains: decisions, early warning, resilience, efficiency
- Hard: legacy systems, definitions, ownership, cost
- Poor data: missed exposures, late reports, losses
- Governance: board and senior management are responsible
- Good design works in stress; reports suit each reader

**IN THE LESSON**

- Let's pull the whole topic together.
- Effective aggregation and reporting give faster, better decisions, earlier warning, complete information in stress, less manual work and fewer losses, and better strategic planning.
- It is hard to achieve because of legacy systems, differing definitions and identifiers, manual spreadsheets, unclear ownership and costly investment.
- Poor data lead to missed or double counted exposures, late or wrong reports, and losses, supervisory action and reputational damage.
- Governance puts responsibility on the board and senior management, with independent validation.
- Sound architecture works under stress with one authoritative source.
- And good reports are accurate, comprehensive, clear, timely and well targeted.

## 29 Try three quick questions

1. Do the principles promise lower capital charges?
   **Answer:** No. The gains are decision quality, resilience and efficiency.
2. A client shows $30m, $25m and $15m in three systems. A $10m trade is in two of them, so counted twice. True exposure?
   **Answer:** $60m (30 + 25 + 15 = 70, less 10 double counted).
3. A vendor handles part of the data process. Who stays responsible?
   **Answer:** The bank: its board and senior management.

**IN THE LESSON**

- Now try three quick questions yourself.
- Pause after each one.
- Question one.
- Do the principles promise lower capital charges?
- No.
- The gains are better decisions, resilience in stress and efficiency.
- Question two.
- A client shows thirty million in one system, twenty five million in a second and fifteen million in a third, but a ten million trade appears in two of the systems, so it is counted twice in the total of seventy.
- What is the true exposure?
- Sixty million: the three systems add up to seventy, less ten that was double counted.
- Question three.
- A vendor handles part of the data process.
- Who stays responsible?
- The bank.
- Its board and senior management cannot hand the responsibility to a vendor, so they must still oversee and validate the work.