Operational Risk Governance

FRM Part II

1 A story: the outage nobody owned

- Kestrel's payments system fails for a whole day
- Technology blames operations; operations blames technology
- The board had never approved any framework
- Everyone assumed the risk team was in charge
- Governance answers: who decides, who does, who checks

IN THE LESSON

- One morning at Kestrel Bank, a mid sized bank, the payments system fails, and for a whole day customers cannot send money.
- When the board asks what happened, the technology team blames operations, and operations blames the technology team.
- It then emerges that the board had never approved any framework for operational risk, so nobody had clear responsibility for preventing an outage like this.
- Everyone had simply assumed that the small operational risk team was in charge.
- Nothing here needs a careless person, only a bank where nobody knows who decides, who does the work and who checks it.
- Governance answers those three questions.

2 Operational risk and its framework

- Op risk: failed processes, people, systems; external events
- Examples: outages, staff fraud, input errors, floods
- Framework: policies, tools, roles, reports to manage it
- Governance: who approves it, runs it, checks it
- Kestrel: outage is op risk; nobody in charge is governance

IN THE LESSON

- First, some words.
- Operational risk is the risk of loss from inadequate or failed internal processes, people and systems, or from external events.
- Examples are a system outage, a fraud by an employee, a data entry error or a flood in a data centre.
- An operational risk management framework is the bank's set of policies, tools, roles and reports for managing that risk.
- Governance is how that framework is directed and checked: who approves it, who runs it and who makes sure it works.
- So Kestrel's outage, a failure of a system, was an operational risk event.
- The fact that nobody was in charge of preventing it was a failure of governance.

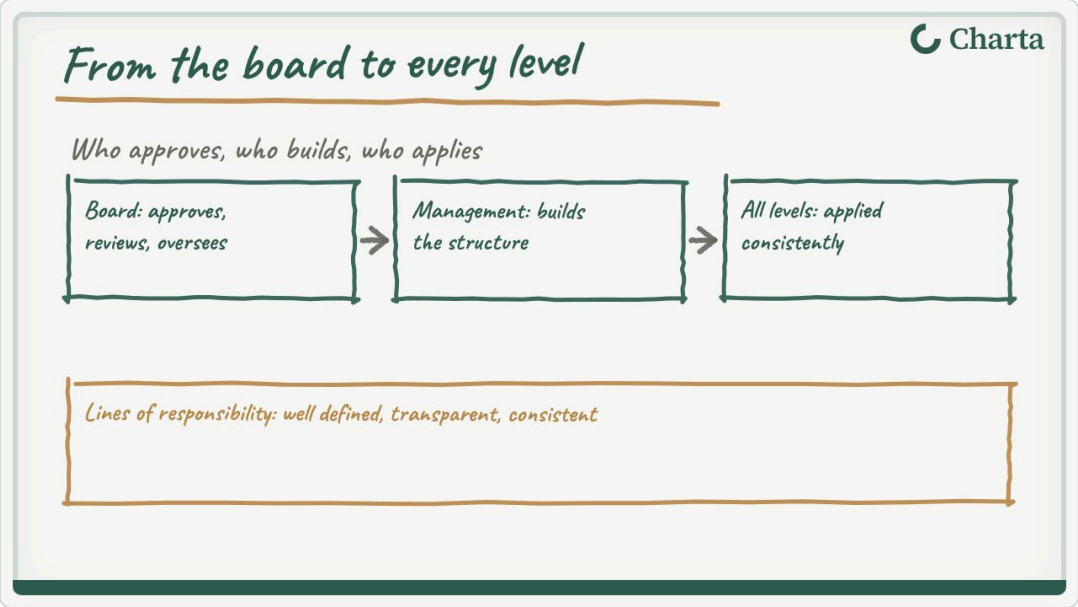
3 What Basel expects: the big picture

- Principles for the Sound Management of Operational Risk
- One framework, fully integrated into overall risk
- Board approves, reviews periodically, oversees management
- Senior management builds the structure and implements it
- Documented; proportionate to size, complexity, risk profile

IN THE LESSON

- The Basel Committee on Banking Supervision, which sets global standards for banks, sets out its expectations in its Principles for the Sound Management of Operational Risk.
- The main ideas are these.
- First, the bank runs one operational risk management framework, fully integrated into the bank's overall risk management.
- It is not a stand alone exercise run in a corner by specialists.
- Second, the board of directors approves the framework, reviews it periodically, and oversees senior management.
- Third, senior management builds a clear governance structure and implements the framework.
- Fourth, the framework is documented, which means written down, and the principles apply to every bank, but in proportion to its size, complexity and risk profile.

4 From the board to every level



IN THE LESSON

- Here is how responsibility flows at Kestrel, from the top down: who approves, who builds, and who applies.
- In the first box, the board approves the framework, reviews it periodically, and oversees senior management, holding it to account.
- In the second box, senior management, meaning the chief executive and the executives who report to them, develops the governance structure.
- That structure says who is accountable for each risk, and management submits it to the board.
- In the third box, management makes sure the framework is applied consistently at every level of the organisation, from head office to the smallest branch.
- Underneath all three boxes sits Basel's requirement: lines of responsibility that are well defined, transparent and consistent.

5 What the written framework covers

Kestrel's framework document: four things it must define

Element	At Kestrel
Definitions	What counts as operational risk
Roles	Who owns, challenges, assures
Tools	Self-assessment, KRIs, loss data
Reporting	Reports to management and board

IN THE LESSON

- Basel expects the framework to be documented.
- Kestrel's framework document covers four things.
- First, definitions: what counts as operational risk, so that everyone uses the same language.
- Second, roles: who owns each risk, who challenges, and who assures, which is the three lines of defence we meet later.
- Third, tools: the methods used to find and measure risk.
- These include risk and control self assessments, where a team reviews its own risks and controls, key risk indicators, which are measures that warn when a risk is rising, and a database of losses.
- Fourth, reporting: what information goes to senior management and the board, and how often.

6 Proportionality: same principles, other scale

Kestrel against Millbrook Savings, a small bank, for illustration

Feature	Kestrel (large)	Millbrook (small)
Risk function	Dedicated team	One risk officer
Committees	Several, specialised	One, combined
Indicators	Many KRIs	A few simple KRIs
Principles	Apply in full	Apply in full

IN THE LESSON

- The principles apply to all banks, but in proportion to each bank's size, complexity and risk profile.
- Compare Kestrel with a made up small lender, Millbrook Savings Bank, which lends in one town.
- For illustration, Kestrel has a dedicated operational risk team, while Millbrook may have a single risk officer.
- Kestrel runs several specialised committees, while Millbrook may combine them into one.
- Kestrel tracks many key risk indicators across many businesses, while Millbrook watches a few simple ones.
- But look at the last row.
- At both banks, the principles themselves apply in full: the board approves and oversees, management implements, and the framework is written down.
- Proportionality changes how much machinery a bank needs.
- It never excuses a bank from the principles.

7 Example 1: approve or implement?

Kestrel after the outage: who does each governance task?

Approves the new framework	at the start, then at intervals	**Board**
Reviews it each year	and oversees management	**Board**
Designs lines of responsibility	submits them to the board	**Management**
Rolls it out to every branch	consistently, every level	**Management**

IN THE LESSON

- After the outage, Kestrel sorts its governance tasks.
- Approving the new framework is the board's job, done once at the start and then again at intervals.
- Reviewing the framework each year, and overseeing the executives who run it, is also the board's job.
- Designing the lines of responsibility, so that every risk has a named owner, is a senior management task, and management submits the design to the board.
- Rolling the framework out consistently to every branch and every level is also senior management's task.
- Notice the two circled rows: the board approves the framework, and management rolls it out.
- That is the pattern in the right hand column.
- The board approves and oversees.
- Management implements.
- A management that approved its own framework would be marking its own homework.

8 Mistakes to avoid: not one team's job

- Treating governance as the op risk team's job alone
- A stand-alone framework outside overall risk management
- Board running the framework; management approving it
- Written at head office, not applied at every level
- Exam: board approves, oversees; management implements

IN THE LESSON

- Four mistakes to avoid.
- The first, and the most common, is to treat governance as the operational risk function's job alone.
- That is what happened at Kestrel.
- The risk team can design tools, but the board and senior management carry the responsibility.
- The second is a stand alone framework that sits outside the bank's overall risk management, with its own language and reports.
- The third is to swap the roles, so that the board runs the framework or management approves it.
- The fourth is a framework that is written down at head office but not applied consistently in every branch.
- And the exam point to remember is short: the board approves and oversees, and management implements.

9 A story: the board cannot do everything

- Kestrel's board meets only a few times a year
- Too little time to study every risk in depth
- So it delegates detailed work to committees
- It can delegate work, but not responsibility

IN THE LESSON

- Kestrel's board meets only a few times a year, and its directors have many subjects to cover: strategy, capital, credit, markets, and now operational risk.
- There is not enough time in a board meeting to study every risk in depth.
- So the board delegates detailed work to committees, which are smaller groups of directors who meet more often and focus on one area.
- Delegation is sensible, but it has a limit, and the exam tests it.
- The board can delegate work.
- It cannot delegate responsibility.
- If Kestrel's payments system fails again, the board as a whole is still ultimately responsible for how operational risk was governed.
- Let us look first at what the board itself does, and then at each of its committees in turn.

10 What the board itself does

The board holds ultimate responsibility, even when it delegates

Board task	What it means
Approve, review framework	Sets how op risk is managed
Approve appetite, tolerance	How much op risk to accept
Oversee senior management	Holds executives to account
Delegate to committees	Work moves; responsibility stays

IN THE LESSON

- The board has four tasks.
- It approves the operational risk management framework and reviews it periodically, which sets how operational risk is managed across the bank.
- It approves the risk appetite and tolerance statement, which says how much operational risk the bank is willing to accept.
- We return to that statement at the end of the lesson.
- It oversees senior management, holding the executives to account for running the framework.
- And it may delegate work to committees.
- Notice what happens when it delegates: the work moves to the committee, but the responsibility stays with the board.
- Next we look at the three board committees that matter most for operational risk.

11 Three board committees, side by side

Each committee is made up of directors and reports to the full board

Committee	Role in operational risk
Risk committee	Advises on appetite; monitors
Audit committee	Audit, reporting, controls
Remuneration committee	Pay rewards risk-aware conduct

IN THE LESSON

- Three committees of the board matter most.
- Each is made up of directors, and each reports back to the full board.
- The board risk committee advises the board on the risk appetite, and it monitors two things: how senior management is implementing the framework, and what the bank's operational risk profile looks like, meaning the risks it is actually running.
- The audit committee oversees internal audit.
- It makes sure that audit's review of the operational risk framework is independent, and it watches over the integrity of financial reporting and of internal controls.
- The remuneration committee makes sure that pay and incentives reward risk aware, compliant behaviour, rather than raw revenue.

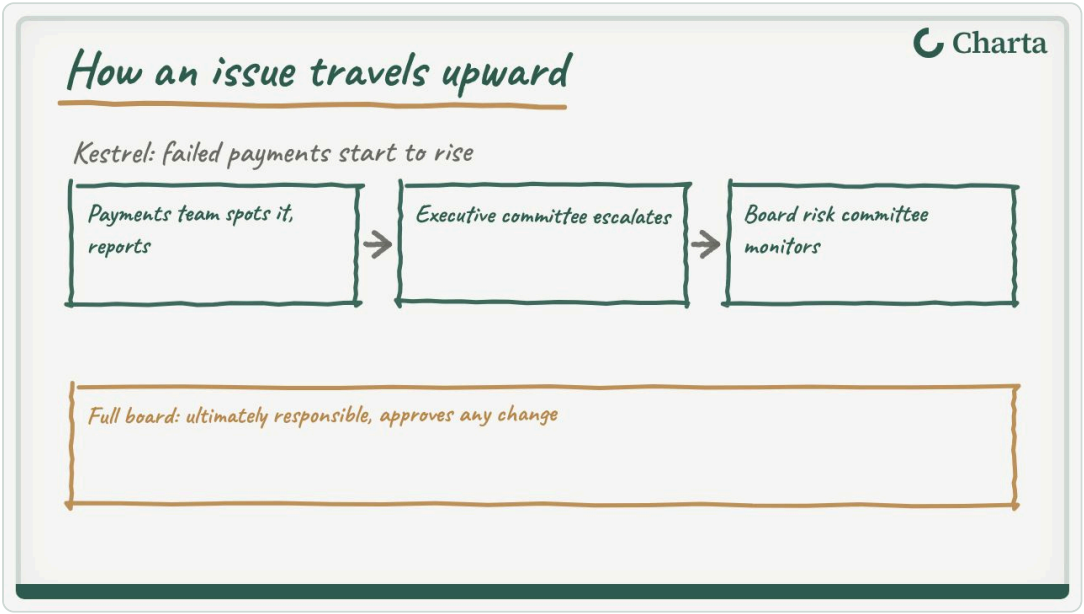
12 The executive operational risk committee

- Below the board: a committee of senior managers
- Reviews the risk profile, key risk indicators, losses
- Escalates material issues upward to the board
- A management body, not a board committee
- At Kestrel: meets monthly, sees problems first

IN THE LESSON

- Below the board sits a different kind of committee, the executive operational risk committee.
- Its members are senior managers, not directors.
- It reviews the operational risk profile, the key risk indicators, such as the number of failed payments a day, and the losses the bank has suffered.
- When it finds something material, such as an indicator in the red or a large loss, it escalates it upward, through senior management to the board and its risk committee.
- Notice its place.
- It is a management body, part of how senior management implements the framework.
- It is not a committee of the board, and it does not approve the framework or the appetite.
- At Kestrel it meets monthly, so it sees problems first.

13 How an issue travels upward



IN THE LESSON

- Let us follow one issue up the chain at Kestrel.
- Failed payments start to rise.
- In the first box, the payments team, which runs the process, spots the trend in its daily figures and reports it.
- In the second box, the executive operational risk committee reviews the report at its monthly meeting, sees that the trend is serious, and escalates it.
- In the third box, the board risk committee monitors the issue, asking senior management what is being done and whether the bank is still inside its risk appetite.
- In the bottom row, the full board, which keeps ultimate responsibility, receives the committee's report, and if the appetite or the framework needs to change, it is the board that approves the change.

14 Example 2: which body does it?

Five governance tasks at Kestrel: board, committee or management?

Approves the appetite statement	ultimate responsibility	**Board**
Monitors the risk profile	and advises on appetite	**Risk committee**
Checks audit's independence	and financial reporting	**Audit committee**
Ties bonuses to good conduct	not to raw revenue	**Remuneration**
Reviews monthly KRIs, losses	senior managers	**Exec committee**

IN THE LESSON

- Let us place five tasks.
- Approving the operational risk appetite statement is the board's job, because it carries ultimate responsibility.
- Monitoring the operational risk profile, and advising the board on appetite, belongs to the board risk committee.
- Checking that internal audit's review is independent, and that financial reporting is sound, is the audit committee's job.
- Changing Kestrel's bonus plan so that it rewards good conduct, not raw revenue, belongs to the remuneration committee.
- And reviewing the monthly key risk indicators and loss reports is the work of the executive operational risk committee, made up of senior managers.
- That highlighted last row is the one candidates get wrong: the detailed monthly review is done by management, which then escalates.

15 Mistakes to avoid: approve, monitor, assure

Remember who approves, who monitors and who assures

Question	Answer
Who approves?	The board
Who monitors?	Risk committee; exec committee
Who assures?	Audit committee, internal audit
Who aligns pay?	Remuneration committee

IN THE LESSON

- Here is the common error, and a way to avoid it.
- Candidates confuse the executive operational risk committee with the board committees.
- So keep four questions in mind.
- Who approves?
- The board, which approves the framework and the appetite.
- Who monitors?
- The board risk committee monitors at board level, and the executive committee of senior managers monitors in detail at management level, and escalates.
- Who assures?
- The audit committee, through internal audit's independent review.
- And who aligns pay with all of this?
- The remuneration committee.
- An answer saying the executive committee approves the appetite is wrong.
- A committee of managers can recommend, but only the board approves.

16 A story: the team that graded itself

- Payments team rates its own risks as low
- Nobody independent challenges the rating
- Nobody checks whether the controls really work
- Three lines of defence: own, challenge, assure

IN THE LESSON

- Before the outage, Kestrel's payments team filled in its yearly risk assessment.
- It rated the risk of a system failure as low, and its own controls as strong.
- No one independent challenged the rating, and no one checked whether the controls really worked.
- Some months later the system failed for a whole day.
- The lesson is not that the payments team was dishonest.
- It is that the people who take a risk should not be the only ones judging it.
- The three lines of defence divide operational risk responsibilities between three groups, so that owning a risk, challenging it and giving assurance about it sit with different people.

17 The three lines of defence

Own it. Challenge it. Assure it.

Line	Responsibility
1st: business lines	Own the risks and controls
2nd: op risk function	Design, challenge, monitor
3rd: internal audit	Independent assurance

IN THE LESSON

- Here is the model in one table.
- The first line is business line management, together with its support functions.
- It owns the risks and the controls.
- The second line is the independent corporate operational risk management function.
- It designs the framework, challenges the first line and monitors the risk profile.
- The third line is internal audit, which gives independent assurance that the whole system works.
- The three verbs to remember are on the top line: the first line owns, the second line challenges, and the third line assures.
- The next slides take each line in turn.

18 The first line: owns the risk

- Business line management and its support functions
- Identifies and assesses its own risks
- Runs the controls day to day
- Fixes weaknesses: remediation
- Reports its risks, events and losses

IN THE LESSON

- The first line is business line management and its support functions.
- At Kestrel, that means the head of payments and her team, along with the technology and operations staff who support them.
- The first line owns the risk because it takes the risk, every day, in the course of doing business.
- So it identifies and assesses its own risks, for example through the yearly self assessment.
- It runs the controls day to day, such as checking that payments over a certain size have a second approval.
- When a control is weak, it fixes it, which is called remediation.
- And it reports its risks, events and losses upward.
- It knows the risk best, which is why it owns it, and why someone independent must challenge it.

19 The second line: challenges the first

- Independent corporate op risk management function
- Designs the framework, tools and methodology
- Challenges the first line's assessments
- Monitors the risk profile; reports to management, board
- Does not do the first line's assessments

IN THE LESSON

- Now the second line, the independent corporate operational risk management function at head office.
- Independent means it does not report to the business lines it oversees, and is not paid for their results.
- It designs the framework, the tools and the methodology, such as the self assessment template.
- It challenges the first line's assessments.
- If the payments team rates outage risk as low, the second line asks for the evidence, compares it with past losses and incidents, and pushes back.
- It monitors the operational risk profile of the whole bank.
- And it reports to senior management and the board.
- Note what the second line does not do.
- It does not carry out the first line's assessments for it, because then it would be challenging its own work.

20 The third line: assures the board

- Internal audit: independent assurance
- Tests that the framework and lines one and two work
- Does not design or run the framework or controls
- Overseen by the board's audit committee

IN THE LESSON

- The third line is internal audit.
- Its job is to give independent assurance.
- Assurance means an objective opinion, based on testing, that something does what it is meant to do.
- Internal audit tests that the framework, and the first two lines, work as intended.
- At Kestrel, it might test a sample of large payments to see whether the second approval was really given, and review whether the second line's challenge was real or just a box ticked.
- Audit does not design the framework, and it does not run controls, because it could not then test them objectively.
- It is overseen by the board's audit committee, which we met earlier and which protects its independence.

21 Example 3: one self-assessment, three lines

Kestrel's payments self-assessment: who does each step?

Sets the template and method	op risk function	**2nd line**
Rates its risks and controls	payments team	**1st line**
Questions the low rating	op risk function	**2nd line**
Fixes the weak control	payments team	**1st line**
Tests the whole process	internal audit	**3rd line**

IN THE LESSON

- Let us run this year's self assessment at Kestrel through the three lines.
- First, the operational risk function sets the template and the method.
- That is second line work, because the second line designs the tools.
- Second, the payments team rates its own risks and controls.
- That is the first line, the owner.
- Third, the operational risk function questions the rating.
- The payments team again says outage risk is low, but the day long failure says otherwise, so the second line challenges and the rating is raised.
- Fourth, the payments team fixes the weak control by adding a backup system, because remediation belongs to the owner.
- Fifth, internal audit tests the whole process, including whether the challenge really happened.
- That is the third line.
- The two circled steps are the independent ones: the second line's challenge and the third line's assurance.
- Nobody judges their own work.

22 Mistakes to avoid: blurring the lines

Each blur takes away an owner or an independent view

Blur	What is lost
2nd line does the assessments	Independent challenge
Audit designs the framework	Independent assurance
1st line hands risk to 2nd	Ownership

IN THE LESSON

- Two mistakes come up again and again, and both blur independence.
- The first is letting the second line do the first line's assessments.
- If the operational risk function fills in the payments team's self assessment, there is nobody left to challenge it, so independent challenge is lost.
- The second is giving internal audit a design role.
- If audit designs the framework, it later audits its own design, so independent assurance is lost.
- A third, related error runs the other way.
- A business line that treats risk as the risk function's problem has handed its risk to the second line and stopped owning it, so ownership is lost.

23 Risk appetite and risk tolerance

- Board approves and periodically reviews the statement
- Appetite: types and levels of op risk taken for strategy
- Tolerance: acceptable variation or limit around appetite
- Kestrel: appetite about $20m of losses a year
- Tolerance: outer limit $24m

IN THE LESSON

- Now the last outcome: risk appetite and risk culture.
- The board approves and periodically reviews an operational risk appetite and tolerance statement.
- Appetite sets the nature, types and levels of operational risk that the bank is willing to assume in pursuit of its strategy.
- Tolerance sets the acceptable variation, or limit, around that appetite.
- Think of a long drive.
- Your appetite is the speed you plan to travel at, and your tolerance is the most you would accept on a downhill stretch before you brake.
- At Kestrel, the board's appetite is operational losses of about twenty million dollars a year, and its tolerance sets an outer limit of twenty four million dollars.
- Beyond twenty four million, the limit is breached.

24 Why operational risk appetite looks different

- Op risk earns no direct return
- So appetite is often set by risk type, not one number
- Very low or zero tolerance for fraud and conduct breaches
- Mix: qualitative statements and quantitative metrics
- Metrics: KRIs, loss limits, escalation triggers

IN THE LESSON

- Operational risk appetite looks different from appetite for credit or market risk.
- A bank takes credit risk to earn interest.
- Operational risk earns no direct return.
- So the appetite is often expressed by risk type, rather than as one number for the whole bank.
- For some types, the bank accepts a small, steady level of loss, such as minor processing errors.
- For others, it sets very low or zero tolerance, notably for fraud and for conduct breaches, meaning harm to customers or markets from how staff behave.
- The statement mixes qualitative statements, written in words, with quantitative metrics, in numbers.
- The metrics are typically key risk indicators, loss limits and escalation triggers, which are the levels at which an issue must be passed upward.

25 Kestrel's appetite statement, by risk type

Words and numbers together, risk type by risk type

Risk type	Appetite or metric
Internal fraud	Zero: every case escalated
Conduct, mis-selling	Zero for known breaches
Processing errors	Losses under $5m a year
System outages	Critical systems back in 2 hours
All operational risk	Appetite $20m; limit $24m

IN THE LESSON

- Here is Kestrel's statement, with made up figures.
- For internal fraud, the tolerance is zero, and every case is escalated, however small.
- For conduct breaches such as mis selling, which means selling customers products that do not suit them, the tolerance is also zero for known breaches.
- For processing errors, the bank accepts losses under five million dollars a year.
- For system outages, critical systems must be back within two hours, a lesson from the day long failure.
- And for operational risk as a whole, the appetite is losses of about twenty million dollars a year, with a limit of twenty four million.
- Words and numbers sit side by side.

26 Example 4: how much appetite is used?

Appetite $20m a year, limit $24m. Early warning at 80% of appetite

Early-warning trigger	80% × 20m	**$16m**
Losses so far this year	January to September	**$17.5m**
Appetite used	17.5 ÷ 20	**87.5%**
Room before the limit	24 − 17.5	**$6.5m**
Action	above the $16m trigger	**Escalate**

IN THE LESSON

- Now measure Kestrel's position.
- The appetite is twenty million dollars a year, and the limit twenty four million.
- The statement sets an early warning trigger at eighty per cent of appetite.
- Eighty per cent of twenty million is sixteen million dollars.
- Losses from January to September total seventeen and a half million.
- The appetite used is seventeen point five divided by twenty, which is eighty seven and a half per cent.
- The room left before the limit is twenty four minus seventeen point five, which is six and a half million dollars.
- So Kestrel is still inside its appetite, and well inside its limit.
- But it has passed the sixteen million trigger, so the action is to escalate: the executive committee reviews it and reports to the board risk committee, as the statement requires for this trigger, and explains what is being done.

27 Example 5: key risk indicators

Kestrel's monthly report: amber and red thresholds set in the statement

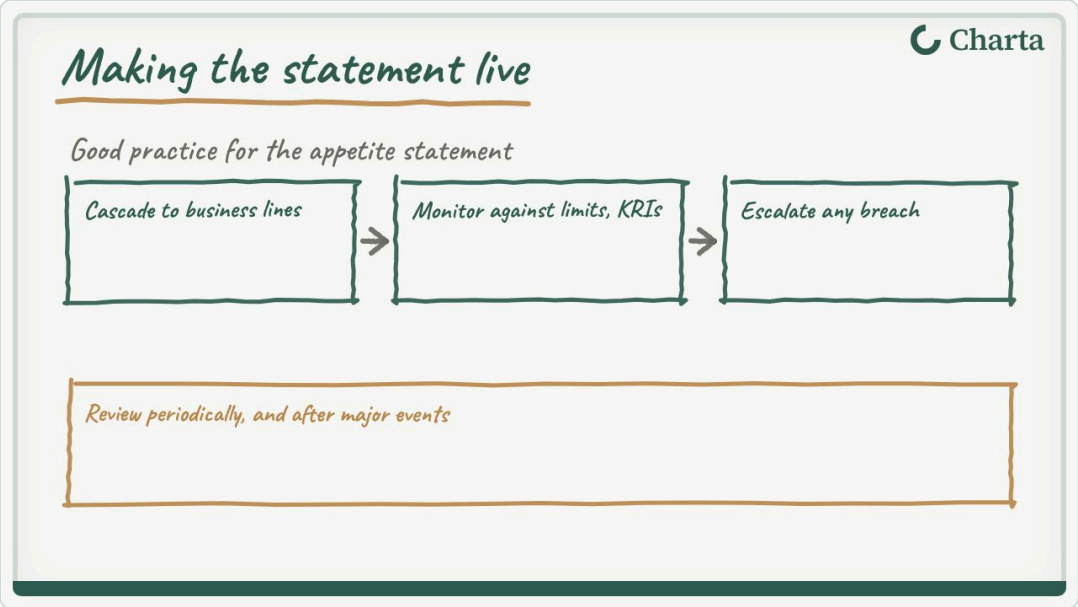
Failed payments a day	amber 40, red 80; now 55	**Amber**
Longest critical outage, hours	amber 1, red over 2; now 5	**Red**
Staff behind on training	amber 5%, red 10%; now 3%	**Green**
Internal fraud cases	zero tolerance; now 1	**Breach**

Red and breaches go to the board risk committee

IN THE LESSON

- Key risk indicators turn the appetite into early warnings.
- Each has an amber threshold, which calls for attention, and a red threshold, which calls for escalation.
- Failed payments a day: amber at forty, red at eighty, and today fifty five, so amber.
- Longest critical system outage this month, in hours: amber at one, red above two, the limit in the statement, and this month five, so red.
- Staff behind on their conduct training: amber at five per cent, red at ten, and now three per cent, so green.
- Internal fraud cases: zero tolerance, and one case this month, so that is a breach.
- The note at the bottom gives the rule.
- The red indicator and the breach both go up to the board risk committee, while management handles and watches the amber one.

28 Making the statement live



IN THE LESSON

- A statement on paper does nothing by itself.
- Good practice makes it live in four steps.
- First, cascade it.
- The bank wide appetite is broken into allocations for each business line, so that every manager knows their share.
- Second, monitor actual losses and key risk indicators against those allocations, every month.
- Third, escalate any breach, quickly and through the agreed route, to the executive committee and then to the board risk committee.
- Fourth, in the bottom row, review the statement periodically, and especially after a major event.
- After the day long payments outage, Kestrel's board reviewed its statement and added the two hour limit for critical systems.

29 Example 6: cascading the $20m appetite

Bank appetite $20m split by business line. Losses so far this year, $m

Retail banking	6.4 of 8.0	**80%**
Payments	6.6 of 6.0	**110%**
Markets	3.0 of 4.0	**75%**
Central buffer	1.5 of 2.0	**75%**
Whole bank	17.5 of 20.0	**87.5%**

Payments exceeds its own allocation, though the bank total is inside

IN THE LESSON

- Here is the cascade at Kestrel.
- The twenty million dollar appetite is split into eight million for retail banking, six million for payments, four million for markets, and a central buffer of two million.
- Look at losses so far this year.
- Retail banking has used six point four of its eight million, which is eighty per cent.
- Payments has used six point six of six, which is one hundred and ten per cent.
- Markets has used three of four, seventy five per cent.
- The central buffer has used one point five of two, also seventy five per cent.
- The whole bank has used seventeen point five of twenty, eighty seven and a half per cent.
- The lesson is in the note.
- Payments has used more than its own share of the appetite, even though the bank total is inside appetite, so monitoring must go line by line.

30 A robust risk culture

- Tone from the top: leaders say it and show it
- Accountability: named owners answer for their risks
- Incentives aligned with the appetite statement
- Training, so staff recognise and report risk
- Safe channels to speak up without fear

IN THE LESSON

- Limits and indicators only work if people act on them.
- Risk culture is the shared attitudes and behaviour of staff towards risk, and supervisors expect the board and senior management to foster a robust one.
- It needs five things.
- Tone from the top, where leaders say that risk matters and show it in their own decisions.
- Accountability, so that named owners answer for their risks, as the three lines require.
- Incentives aligned with the appetite statement, so that pay never rewards what the statement forbids.
- Training, so that staff can recognise operational risks and know how to report them.
- And safe channels to speak up, so that someone who sees a problem can raise it without fear of blame.

31 Mistakes to avoid: pay contradicts words

Kestrel before its reforms: what the words said and what people saw

Statement says	Behaviour or pay says
Zero tolerance for mis-selling	Bonus paid on sales volume alone
Systems back in 2 hours	Upgrade budget cut for profit
Speak up without fear	Bearers of bad news sidelined

IN THE LESSON

- The common mistake is a statement that behaviour and pay contradict.
- Look at three examples from Kestrel before its reforms.
- The statement said zero tolerance for mis selling, but bonuses were paid on sales volume alone.
- The statement said critical systems must be back within two hours, but the budget to upgrade the backup system was cut to protect profit.
- The statement said staff could speak up without fear, but people who brought bad news were quietly sidelined.
- In each case, people follow what is rewarded and what leaders do, not what the document says.
- That is why the remuneration committee belongs in operational risk governance, and why a statement is only as strong as the behaviour around it.

32 Recap: the main ideas

- One integrated, documented, proportionate framework
- Board approves and oversees; management implements
- Risk, audit, pay committees; executive committee escalates
- Business owns, op risk function challenges, audit assures
- Appetite by risk type; pay and behaviour must match it

IN THE LESSON

- Let us pull it together.
- Basel expects one operational risk management framework, fully integrated into overall risk management, written down, and proportionate to the bank's size, complexity and risk profile.
- The board approves and oversees, and senior management implements through clear lines of responsibility.
- The board keeps ultimate responsibility, while its risk committee advises on appetite and monitors, its audit committee oversees independent assurance, and its remuneration committee aligns pay, and an executive committee of senior managers reviews the detail and escalates.
- In the three lines of defence, the business owns the risk, the operational risk function challenges, and internal audit assures.
- And the appetite statement is set by risk type, mixing words and numbers, and pay and behaviour must match it.

33 Try three quick questions

1. Appetite $30m, early warning at 75%. Losses so far $24m. Escalate?
   Answer: Trigger 75% × 30m = $22.5m. Used 24 ÷ 30 = 80%: escalate.
2. Internal audit is asked to design the self-assessment method. What is wrong?
   Answer: Design is 2nd-line work; audit would assure its own design.
3. Senior managers review KRIs and losses monthly. Which body? May it approve appetite?
   Answer: Executive op risk committee, not a board committee. Only the board approves.

IN THE LESSON

- Now try three quick questions.
- Pause the video, think, then listen to the answers.
- Question one.
- A bank's operational loss appetite is thirty million dollars a year, with an early warning trigger at seventy five per cent.
- Losses so far this year are twenty four million.
- Must it escalate?
- The trigger is seventy five per cent of thirty million, which is twenty two and a half million.
- Twenty four over thirty is eighty per cent of appetite, above the trigger, so yes, it escalates.
- Question two.
- Internal audit is asked to design the bank's self assessment method.
- What is wrong?
- Design belongs to the second line, and audit would later be assuring its own design, so independence is lost.
- Question three.
- Senior managers meet monthly to review key risk indicators and losses, and escalate issues.
- Which body is this, and may it approve the appetite?
- It is the executive operational risk committee, not a board committee, and only the board approves the appetite.