CHARTA LEARNING · LESSON NOTES

Introduction to Operational Risk and Resilience

FRM Part II

1 A story: one bad week at Fernhill Bank

- Monday: a clerk keys $10m instead of $1m
- Wednesday: a software update freezes payments
- Friday: a trader's hidden losses come to light
- No borrower defaulted and no market crashed
- The common thread: operational risk

IN THE LESSON

- Imagine a bad week at Fernhill Bank, a mid sized bank we will follow throughout.
- On Monday, a clerk sends a payment of ten million dollars instead of one million, ten times the intended amount, and the bank spends days getting it back.
- On Wednesday, a software update freezes the payments system, and customers cannot pay their bills.
- On Friday, the bank discovers that a trader has been hiding losing positions for months.
- Now notice what did not happen.
- No borrower defaulted, and no market crashed.
- Every loss came from the way the bank works, or from an event that hit its operations.
- The common thread is operational risk.
- To manage it, Fernhill needs a framework, and to survive weeks like this one, it needs resilience.

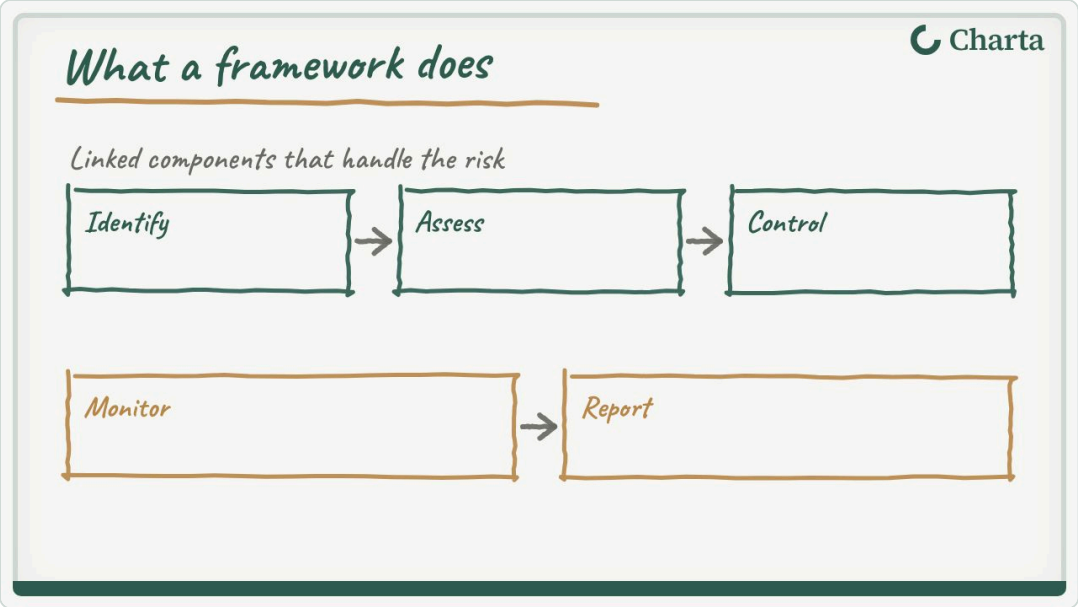
2 What operational risk is

- Inadequate/failed internal processes, people, systems
- Or from external events: flood, fire, crime
- Basel: includes legal risk
- Basel: excludes strategic and reputational risk
- Those two can still follow an operational failure

IN THE LESSON

- Here is the standard definition, from the Basel Committee, the international body of bank supervisors.
- Operational risk is the risk of loss from inadequate or failed internal processes, people and systems, or from external events.
- Processes are the steps the bank follows, people are its staff, and systems are its technology.
- External events include floods, fires and crime.
- Two boundary rules matter.
- The Basel definition includes legal risk, the risk of fines, penalties and damages from lawsuits or breaches of law.
- It excludes strategic risk, the risk of a bad business decision, and reputational risk, the risk that the bank's good name is damaged.
- But those two can still follow from an operational failure.
- A payments outage can hurt Fernhill's reputation, even though the reputational loss itself sits outside the definition.

3 What a framework does



IN THE LESSON

- An operational risk management framework is the set of linked components that handle this risk.
- Look at the boxes in order.
- First, identify: find the risks in each process, product and system.
- Second, assess: judge how likely each risk is, and how much it could cost.
- Third, control: put in place checks that make the risk smaller, such as a second person approving every large payment.
- Fourth, monitor: watch whether the risks and the controls change over time.
- Fifth, report: tell management and the board what they need to know in order to act.
- The word linked matters.
- A framework is not a pile of separate tools.
- Each part feeds the next, so a loss that is reported should change how that risk is assessed and controlled.

4 The framework's building blocks (1)

Who is responsible, and what the bank knows from inside

Building block	What it does
Governance: three lines	Who owns, challenges, assures
Board-approved risk appetite	How much risk is acceptable
RCSA (self-assessment)	Business rates risks, controls
Loss data collection	Records what went wrong

IN THE LESSON

- Now the building blocks themselves, starting with who is responsible and what the bank knows from inside.
- First, governance, built on the three lines of defence, which decides who owns the risk, who challenges it and who gives assurance.
- We look at it closely in a moment.
- Second, a board approved risk appetite, which says how much operational risk the bank is willing to accept, for example the most it will tolerate losing to process errors in a year.
- Third, the risk and control self assessment, or R C S A, in which each business rates its own risks and how well its controls work.
- Fourth, loss data collection: a database recording every loss event, what it cost and what caused it.

5 The framework's building blocks (2)

Warning, looking ahead, reporting and capital

Building block	What it does
Key risk indicators (KRIs)	Early-warning measures
Scenario analysis	Rare, severe what-ifs
Reporting	Informs management and board
Capital, where required	Absorbs unexpected losses

IN THE LESSON

- Four more blocks complete the picture: warning, looking ahead, reporting and capital.
- Key risk indicators, or K R I s, are measures that warn of trouble early, such as staff turnover in the payments team, or the number of failed trades each day.
- Scenario analysis asks experts to imagine rare but severe events, such as a major cyber attack, and to estimate what they would cost.
- This matters because such events may never appear in the bank's own loss data.
- Reporting brings all of this together for management and the board, so that they can act.
- And last, capital, where the rules require it: money held to absorb unexpected operational losses.

6 Three lines of defence

Own it. Challenge it. Assure it.

Line	Role in operational risk
1st: the business	Owns the risk and its controls
2nd: operational risk team	Challenges the business
3rd: internal audit	Gives assurance to the board

IN THE LESSON

- Governance rests on the three lines of defence: own it, challenge it, assure it.
- The first line is the business itself, such as Fernhill's payments department.
- It owns the risk, because it runs the processes, and it owns the controls inside them.
- The second line is an independent operational risk team.
- It designs the framework, sets standards, and challenges the business, for example by questioning a self assessment that rates every control as strong.
- The third line is internal audit.
- It gives the board assurance that the first two lines are working, by testing them from outside.
- The key word is independence.
- The second line must be able to challenge without reporting to the business it challenges, and audit must not test work it designed itself.

7 Example 1: what belongs in the remit?

Fernhill's losses this quarter, $m. Which belong to operational risk?

Hidden unauthorised trading	loss 4.0	**Inside**
Bond prices fall, normal trades	loss 6.0	**Market**
Borrower defaults, sound loan	loss 3.0	**Credit**
Lien never registered	extra loss 1.5	**Inside**
Court fine for mis-selling	loss 2.5: legal	**Inside**

Operational remit: 4.0 + 1.5 + 2.5 = $8.0m of $17.0m

IN THE LESSON

- Let us sort Fernhill's losses this quarter, in millions of dollars.
- A trader hid unauthorised bets and lost four million.
- Operational: a person broke the rules.
- Bond prices fell on normal, authorised trades, a loss of six million.
- That is market risk.
- A borrower defaulted on a properly made loan, a loss of three million.
- That is credit risk.
- But on another defaulted loan, the bank's lien on the collateral, its legal claim over the asset, was never registered, so it recovered less: an extra loss of one point five million.
- That extra part has an operational cause, a failed process, so it belongs inside.
- It is recorded and managed in the operational risk framework, although for capital, Basel treats such credit related losses as credit risk.
- Last, a court fine of two point five million for mis-selling is legal risk, which is inside.
- The operational remit is eight million of the seventeen million lost.

8 Mistakes to avoid: boundary and independence

- A loss alone is not operational: find the cause
- Only the operational cause belongs in the remit
- Legal risk is in; strategic and reputational are out
- Business rating its own controls, unchallenged
- Second line reporting to the business it checks

IN THE LESSON

- Exam questions here test two things.
- The first is the boundary.
- A loss alone does not make an event operational, so find the cause.
- The common error is to put credit or market losses inside the remit just because money was lost.
- Only the operational cause belongs there, as with the unregistered lien.
- Remember too that legal risk is in, while strategic and reputational risk are out.
- The second kind is about independence.
- Watch for a business that rates its own controls with no one challenging it, which leaves the first line marking its own homework.
- And watch for a second line that reports to the head of the business it is meant to challenge.
- In both cases the framework exists on paper, but the challenge has gone.

9 Sorting losses by cause

- Basel II sorts losses into seven event types
- Sorted by cause, not where the loss shows up
- A common language across years, units and peers
- Two keys: root cause and intent

IN THE LESSON

- Fernhill now has a loss database, but a database is only useful if every loss is filed the same way.
- Basel Two, the second set of Basel capital rules, sorts operational losses into seven event types.
- They are sorted by cause, meaning what actually went wrong, and not by the department where the loss happened to show up.
- This gives a common language.
- Fernhill can compare losses across years and business lines, and with other banks.
- When you classify an event, two keys unlock almost every question.
- The first is the root cause: what was the original failure?
- The second is intent: did someone act deliberately, or was it an honest mistake?
- Let us meet the seven types.

10 Seven event types: the first four

Sorted by cause, with sample events for each

Event type	Sample events
1 Internal fraud	Theft, bribery, hidden trades
2 External fraud	Forgery, robbery, hacking
3 Employment, workplace safety	Discrimination, injury claims
4 Clients, products, practices	Mis-selling, manipulation

IN THE LESSON

- Here are the first four, with sample events for each.
- One, internal fraud: intentional acts by the bank's own staff, such as theft, bribery, or a trader hiding unauthorised trades.
- Two, external fraud: deliberate acts by outsiders, such as forging a cheque, robbing a branch, or hacking into the bank's systems to steal money.
- Three, employment practices and workplace safety: losses from how the bank treats its staff, such as discrimination claims, compensation claims, and breaches of health and safety rules, for example after an injury at work.
- Four, clients, products and business practices: failures in how the bank deals with its customers and markets.
- This covers mis-selling, selling a product that does not suit the client, breaching a duty of trust, manipulating a market, and breaching customers' privacy.

11 Seven event types: the last three

The last three, then one rule for all seven

Event type	Sample events
5 Damage to physical assets	Disaster, terrorism, vandalism
6 Disruption, system failures	IT, telecoms, utility failures
7 Execution and process	Keying errors, failed settlement
Rule for all seven	Root cause, then intent

IN THE LESSON

- And the last three, then one rule for all seven.
- Five, damage to physical assets: loss of or damage to buildings and equipment from natural disasters, such as a flood, from terrorism, or from vandalism.
- Six, business disruption and system failures: the bank's operations stop because hardware, software, telecommunications or a utility, such as the power supply, fails.
- Seven, execution, delivery and process management: mistakes in the bank's everyday processing.
- Examples are data entry errors, missed deadlines, trades that fail to settle, disputes with vendors, and mistakes in documentation.
- Under all seven sits one rule.
- Classify by the root cause, and then by intent.
- A deliberate act by staff to steal, defraud or get around the rules is internal fraud, and an honest processing error is an execution failure.
- Failures towards clients, deliberate or not, are clients, products and business practices.

12 Example 2: filing Fernhill's events

Five events from Fernhill's loss log. Which event type?

Cashier takes cash from the till	deliberate, staff	**Internal fraud**
Gang forges a client's cheque	deliberate, outsider	**External fraud**
Flood ruins a branch	natural disaster	**Physical assets**
Power cut halts payments	utility failure	**Disruption**
Clerk keys $10m, not $1m	honest error	**Execution**

IN THE LESSON

- Let us file five events from Fernhill's loss log.
- A cashier takes cash from the till.
- The act is deliberate and the person is staff, so it is internal fraud.
- A gang forges a client's cheque and cashes it.
- Deliberate, but by outsiders, so external fraud.
- A flood ruins a branch.
- That is a natural disaster damaging a building, so damage to physical assets.
- A power cut halts the payments system for a day.
- The cause is a utility failure, so business disruption and system failures.
- And Monday's clerk, who keyed ten million dollars where one million was meant, made an honest error in processing, so execution, delivery and process management.
- Notice how each answer came from asking two things: what was the root cause, and was it deliberate?

13 Example 3: intent and cause decide

Same desk or same result, different cause: which type?

Trader hides losing positions	deliberate, staff	**Internal fraud**
Trader books a trade wrongly	honest error	**Execution**
Risky fund sold to a retiree	unsuitable product	**Clients, products**
Employee wins discrimination case	how staff are treated	**Employment**
Server crash stops trading	system failure	**Disruption**

IN THE LESSON

- Now harder cases, where the same desk or the same result can come from different causes.
- A trader deliberately hides losing positions.
- Staff, deliberate, so internal fraud, even though the loss looks like a trading loss.
- Another trader books a trade wrongly by mistake.
- Same desk, but an honest error, so execution, delivery and process management.
- An adviser sells a risky fund to a retiree, for whom it is unsuitable.
- The cause is how the bank treats a client, so clients, products and business practices.
- An employee wins a discrimination case.
- That is about how staff are treated, so employment practices and workplace safety.
- Last, a server crash stops trading for an afternoon.
- The cause is a system, so business disruption and system failures, not execution.

14 Mistakes to avoid: classifying events

- Classify by root cause, not where the loss appears
- Staff stealing or defrauding: internal fraud
- Honest processing error: execution and process
- Deliberate act by an outsider: external fraud
- System down: disruption. Wrong input: execution

IN THE LESSON

- A few traps.
- First, do not classify by where the loss shows up.
- A loss on a trading desk might be internal fraud, a processing error or a system failure, so ask for the root cause.
- Second, intent separates the two staff categories.
- Staff stealing from or defrauding the bank is internal fraud, while an honest processing error by staff is execution, delivery and process management.
- Third, a deliberate act by an outsider is external fraud.
- Fourth, separate the system from the person.
- When a system goes down, that is business disruption and system failures.
- When a system works but someone feeds it the wrong input, that is execution.
- Always reason from cause and intent.

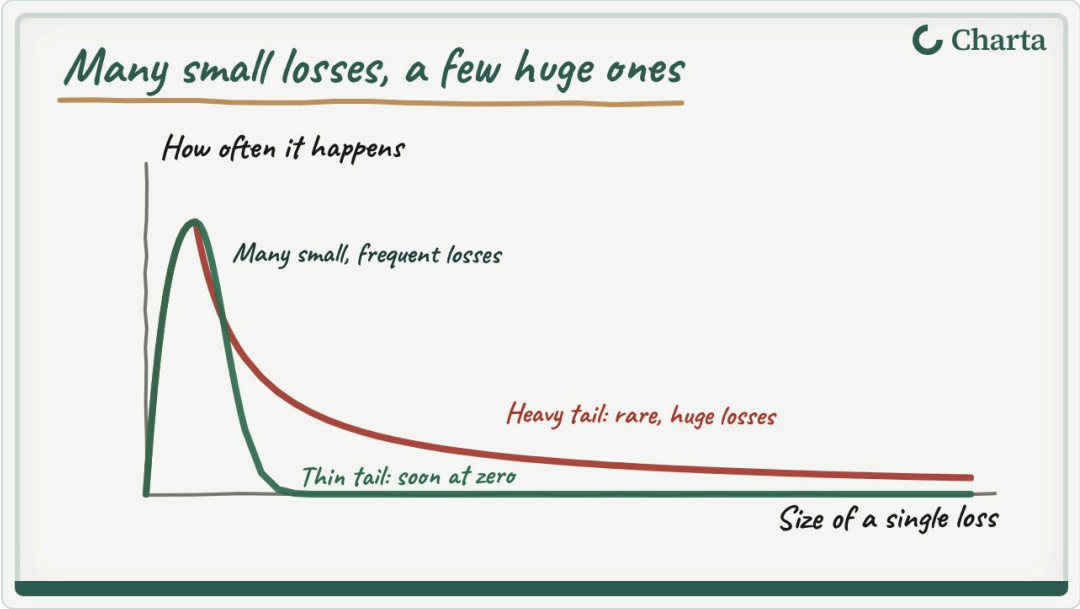
15 A story: Fernhill's loss log

- 1,000 loss events last year
- Most were small: under $10,000 each
- Five were huge: over $1m each
- The five made up most of the total

IN THE LESSON

- Look at a whole year of Fernhill's loss log.
- It holds one thousand loss events.
- Most were small, under ten thousand dollars each: a misdirected payment fixed for a fee, a small card fraud, a late settlement.
- Then there were five huge events, each costing over a million dollars, including the hidden trading losses.
- When the risk team added everything up, those five made up most of the year's total.
- This is the typical shape of operational losses.
- It drives everything about how they are measured, and how hard they are to manage.
- Let us draw it, and then put numbers on it.

16 Many small losses, a few huge ones



IN THE LESSON

- Here is that shape as a picture.
- The bottom axis is the size of a single loss, growing to the right, and the side axis is how often a loss of that size happens.
- The red curve is operational risk.
- It rises steeply to a high peak near zero, then falls, but it stretches far to the right without ever reaching the floor.
- The green curve, for contrast, has the same peak but a thin tail.
- Now read the labels.
- Near zero sit the many small, frequent losses.
- Far out on the red curve is the heavy tail of rare, huge losses.
- And the green curve's thin tail is soon at zero.
- A handful of these huge events dominate the total.
- This is called a heavy tailed severity distribution, where severity means the size of one loss.

17 Example 4: a handful dominate

Fernhill's year: 1,000 events, $50m lost in all

Under $10,000 each	900 events	**$2.0m**
$10,000 to $1m each	95 events	**$8.0m**
Over $1m each	5 events	**$40.0m**
Big five: 0.5% of events	40 ÷ 50	**80% of loss**
Mean severity	50m ÷ 1,000	**$50,000**

90% of events are under $10,000, yet the mean is $50,000

IN THE LESSON

- Here are Fernhill's numbers for the year: one thousand events, and fifty million dollars lost in all.
- Nine hundred events were under ten thousand dollars each, and together they cost two million.
- Ninety five events were between ten thousand and one million each, costing eight million.
- Just five events were over one million each, and they cost forty million.
- So five events, half of one per cent of the count, made up forty out of fifty, which is eighty per cent of the total.
- The mean severity, the average size of a loss, is fifty million over one thousand, which is fifty thousand dollars.
- Yet ninety per cent of events were under ten thousand.
- The mean is pulled up by the tail, and almost no event looks like the average one.

18 Expected annual loss

Expected annual loss = λ × mean severity
Bank total = sum over event types

Frequency λ	Events a year, often Poisson
Mean severity	Average size of one loss
Expected annual loss	Summed across event types

IN THE LESSON

- Now the core formula.
- Expected annual loss for one event type is the frequency times the mean severity, and the bank total is the sum over event types.
- Now the pieces.
- Frequency, written lambda, is the average number of events in a year.
- It is often modelled with a Poisson distribution, which describes events that arrive at random and independently, at a steady average rate.
- Mean severity is the average size of one loss.
- Their product, expected annual loss, is the loss to expect in an average year, and it is summed across event types.
- Remember that this is an average.
- It says nothing about how bad a bad year can be.

19 Example 5: Fernhill's expected annual loss

Frequency a year × mean severity, by event type

External fraud	400 × $5,000	**$2.0m**
Execution and process	500 × $8,000	**$4.0m**
Business disruption	4 × $250,000	**$1.0m**
Internal fraud	0.2 × $10m	**$2.0m**
Expected annual loss	2 + 4 + 1 + 2	**$9.0m**

IN THE LESSON

- Let us apply it to Fernhill, type by type.
- External fraud happens about four hundred times a year, with a mean severity of five thousand dollars, so two million dollars is expected.
- Execution and process errors happen five hundred times a year, at eight thousand dollars each on average, so four million.
- Business disruption happens about four times a year at two hundred and fifty thousand dollars, so one million.
- Serious internal fraud is rare, with a frequency of point two, about one event every five years, but each costs around ten million dollars, so it adds two million a year on average.
- Summed over the four types, expected annual loss is nine million dollars.
- Last year's fifty million was a bad year, far above this average, which is exactly what a heavy tail produces.
- The rarest type contributes as much as external fraud, yet in most years its actual loss will be zero.

20 A risk taken without reward

- A by-product of doing business
- Not taken on to earn a reward
- Hard to diversify away
- Often idiosyncratic: specific to one firm

IN THE LESSON

- Operational risk also differs in nature from credit and market risk.
- A bank takes credit risk on purpose, because lending earns interest, and it takes market risk because positions can earn returns.
- Operational risk is a by-product of doing business.
- Fernhill does not process payments in order to make errors.
- The errors simply come with the processing.
- So there is no reward for bearing it, and more of it is never better.
- It is also hard to diversify.
- Doubling the number of payments does not cancel errors out, and one flaw in a system hits everything that runs on it.
- And it is often idiosyncratic, meaning specific to one firm: its own systems, its own people, its own culture.
- Another bank's losses may tell Fernhill little.

21 Example 6: why a clean record misleads

Internal fraud: Poisson, $\lambda = 0.2$ a year, about $10m an event

No event in one year	exp(−0.2)	**81.9%**
Events expected in 5 years	5 × 0.2	**1.0**
No event in 5 years	exp(−1.0)	**36.8%**
Clean 5 years: mean and max	from the history	**$0**
True expected annual loss	0.2 × $10m	**$2.0m**

IN THE LESSON

- Take Fernhill's internal fraud: a Poisson frequency of point two a year, and about ten million dollars an event.
- Under the Poisson model, the chance of no event in a year is e to the power minus point two, which is eighty one point nine per cent.
- Over five years we expect one event, five times point two.
- The chance of seeing no event at all in five years is e to the power minus one, thirty six point eight per cent.
- So more than a third of the time, a five year history is perfectly clean.
- Its sample mean is zero and its historical maximum is zero.
- Yet the true expected annual loss is two million dollars.
- A short history simply does not contain the tail.

22 Each feature, and the problem it causes

Examiners test the link from feature to problem

Feature	Measurement problem
Heavy tail, rare big losses	Little internal data in the tail
Idiosyncratic to each firm	External data need scaling
Recording threshold	Small losses missing
Reporting bias	Samples distorted
Losses found years later	Recent years look too clean

IN THE LESSON

- Examiners test the link from each feature to the problem it causes.
- Because the tail is heavy and big losses are rare, the bank's own data hold very few points in the tail, which is where the risk really sits.
- Because the risk is idiosyncratic, borrowing other banks' losses is not simple: external data need scaling to the bank's own size and business before they mean anything.
- Because banks record only losses above a set threshold, small losses are missing from the sample.
- Because some losses are more likely to be reported than others, for example large ones that make the news, samples are distorted.
- And because losses can be discovered years after they occur, as with long hidden fraud, recent years look too clean.

23 Mistakes to avoid: measuring the tail

- A sample mean is not a tail quantile
- A historical maximum is not a tail quantile
- Expected loss uses the mean severity, not the median
- Scale external data before using them
- Few recorded losses do not mean low risk

IN THE LESSON

- To close this outcome, five points to remember.
- First, a sample mean is not a tail quantile.
- A tail quantile is a loss that is exceeded only rarely, for example in one year out of a thousand, and an average tells you nothing about it.
- Second, a historical maximum is not a tail quantile either.
- Fernhill's worst loss in five years may be far below what one bad year could bring, and a clean history may hold no big loss at all.
- Third, expected loss uses the mean severity, not the median or the typical loss, which in a heavy tail sit far below the mean.
- Fourth, external data must be scaled before they are used.
- Fifth, and above all, few recorded losses do not mean low risk.

24 From losses to services

- Risk management asks: what could we lose?
- Resilience asks: can customers still be served?
- Deliver critical operations through disruption
- Prevent, adapt, respond, recover and learn
- Assume disruption will happen

IN THE LESSON

- Go back to Wednesday, when the software update froze Fernhill's payments.
- Operational risk management asks: what could we lose, and how do we control it?
- Operational resilience asks a different question: can customers still be served when something goes wrong?
- Operational resilience is the ability of a firm to deliver its critical operations through disruption.
- That means the firm can prevent disruption where it can, adapt to it, respond to it, recover from it, and learn from it afterwards.
- The starting assumption is that disruption will happen.
- A resilient Fernhill does not promise that payments never stop.
- It knows how long they can stop before customers are seriously harmed, and it has shown that it can bring them back within that time.

25 How resilience differs

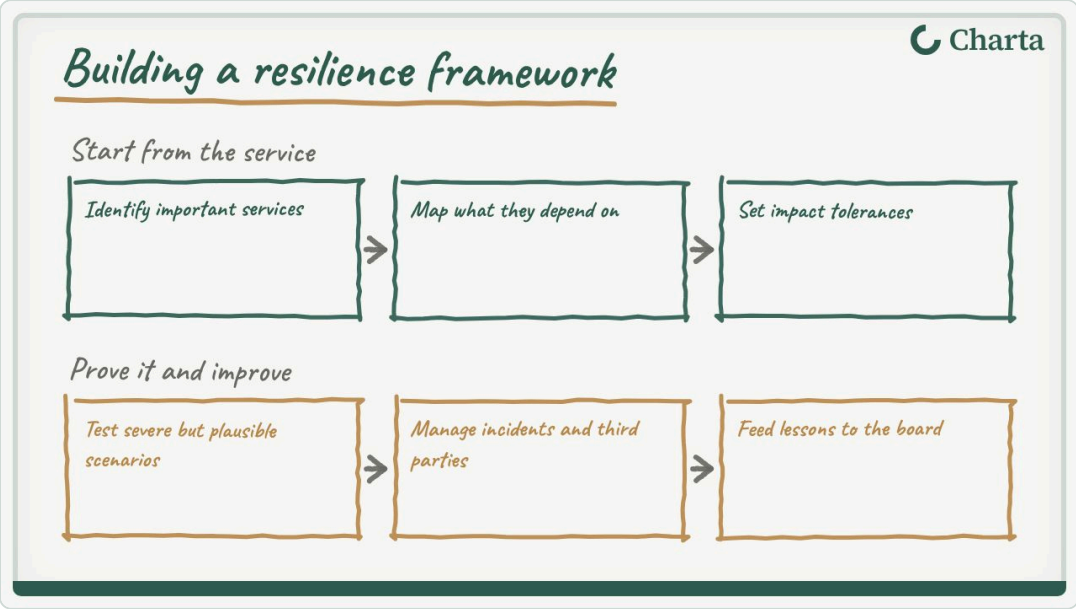
Same events, a different starting point

Approach	Starts from
Operational risk management	Individual risks, loss events
Business continuity	Recovering systems and sites
Operational resilience	Services for customers, markets

IN THE LESSON

- The difference is in the starting point.
- Traditional operational risk management starts from individual risks and loss events: what went wrong, what it cost, and how to control it.
- Business continuity planning starts from recovering individual systems and sites, for example getting the data centre back.
- Operational resilience starts from the services that matter to customers and to markets, such as making payments, and works backwards to everything those services need.
- The three are linked, and resilience uses the tools of the other two.
- But the question changes.
- A payments system may be restored quickly while the service is still broken, because the data are wrong or a supplier is down.
- Resilience judges success by whether the service is delivered.

26 Building a resilience framework



IN THE LESSON

- Here is the framework, box by box, starting from the service.
- First, identify the critical operations, also called important business services: the services whose disruption would harm customers or markets.
- Second, map what each one depends on: its people, processes, technology, data and third parties.
- Third, set an impact tolerance for each service.
- That is the maximum tolerable disruption, for example how many hours the service can be down.
- Then the second row: prove it and improve.
- Fourth, test whether the bank can stay within tolerance in severe but plausible scenarios.
- Fifth, manage incidents when they happen, and manage dependence on third parties, such as cloud providers.
- Sixth, feed the lessons back to the board, which is accountable for the whole framework.

27 Mapping Fernhill's payments service

What the retail payments service depends on

Resource	Fernhill's payments service
People	Payments operations team
Processes	Checks, approvals, settlement
Technology	Payments engine, data centre
Data	Customer accounts, balances
Third parties	Cloud host, card network

IN THE LESSON

- Let us map one service, Fernhill's retail payments, which lets customers pay bills and send money.
- The people are the payments operations team, who run the service each day.
- The processes are the checks, approvals and settlement steps that every payment passes through.
- The technology is the payments engine and the data centre it runs in.
- The data are customer accounts and balances, which must be correct for any payment to go through.
- And the third parties are the cloud provider that hosts part of the system, and the card network that carries card payments.
- Mapping matters because a service is only as strong as its weakest dependency.
- On Wednesday, a single software update in the technology layer stopped the whole service.

28 Example 7: testing against the tolerance

Payments tolerance: 4 hours. Scenario: the main data centre is lost

Switch to the backup site	tested time	**2.5 hours**
Rebuild and reconcile data	tested time	**3.0 hours**
Restart and clear the queue	tested time	**1.0 hour**
Total time to restore	2.5 + 3.0 + 1.0	**6.5 hours**
Gap against tolerance	6.5 − 4.0	**2.5 hours**

IN THE LESSON

- Fernhill's board sets the impact tolerance for retail payments at four hours, because beyond that customers start to miss rent and wage payments, and the harm grows fast.
- These figures are made up for our example.
- The test scenario is severe but plausible: the main data centre is lost.
- In the test, switching to the backup site takes two and a half hours.
- Rebuilding and reconciling the data, so that every balance is right, takes three hours.
- Restarting the service and clearing the queue of waiting payments takes one hour.
- The total time to restore the service is six and a half hours.
- Against a tolerance of four, the gap is two and a half hours.
- Fernhill cannot currently stay within tolerance, and the board must be told.

29 Example 8: closing the gap

Fernhill invests to bring payments back inside 4 hours

Switch: automated failover	was 2.5	**1.5 hours**
Data: copied continuously	was 3.0	**0.5 hours**
Restart and clear the queue	unchanged	**1.0 hour**
New total time to restore	1.5 + 0.5 + 1.0	**3.0 hours**
Room inside tolerance	4.0 − 3.0	**1.0 hour**

IN THE LESSON

- Regulators expect a gap to be remediated, meaning fixed, not explained away.
- Fernhill invests in two changes.
- Automated failover cuts the switch to the backup site from two and a half hours to one and a half.
- Copying data continuously to the backup site cuts the rebuild from three hours to half an hour, because there is far less to reconcile.
- Restarting and clearing the queue still takes one hour.
- The new total time to restore is three hours, which leaves one hour of room inside the four hour tolerance.
- The test is then repeated to prove that the fix works, and the result goes to the board.
- Notice what Fernhill did not do.
- It did not raise the tolerance to seven hours to make the first test pass.

30 What regulators expect

- Basel Committee principles, among others
- Board accountability for resilience
- Evidence of testing against severe scenarios
- Remediation of any gap against tolerance
- Tolerances set by harm, not convenience

IN THE LESSON

- What do regulators expect?
- Supervisors, including the Basel Committee in its principles for operational resilience, set out broadly similar expectations.
- Basel speaks of a tolerance for disruption; some regulators call it an impact tolerance.
- First, the board is accountable.
- Resilience is not just a technology project, and the board must approve and oversee it.
- Second, there must be evidence of testing: the firm must be able to show that it has tested its important services against severe but plausible scenarios, and not merely written plans.
- Third, any gap against tolerance must be remediated.
- Finding a gap is acceptable, but leaving it is not.
- And fourth, tolerances must reflect the harm that disruption causes to customers and markets, not what the firm finds convenient or can already achieve.

31 Mistakes to avoid: resilience

- Setting tolerance at what the firm can already do
- Mapping systems instead of services
- Testing only mild, comfortable scenarios
- Ignoring the third parties a service relies on
- Treating it as a tech project, not the board's

IN THE LESSON

- Here are the traps.
- The first is setting the tolerance at whatever the firm can already achieve.
- If Fernhill had chosen seven hours because its test showed six and a half, the test would always pass, and customers would still be harmed.
- Second, mapping systems instead of services.
- Third, testing only mild, comfortable scenarios.
- The test must be severe but plausible, or it proves nothing.
- Fourth, ignoring the third parties a service depends on.
- If the cloud provider fails, the service fails, whoever is to blame.
- And fifth, treating resilience as a technology project.
- It is the board's responsibility, and the board must see the gaps.

32 Recap: the main ideas

- Op risk: processes, people, systems, external events
- Framework: identify, assess, control, monitor, report
- Seven Basel event types: root cause and intent
- Heavy tail; expected annual loss = λ × mean severity
- Resilience: services delivered within tolerance

IN THE LESSON

- Let us pull it together.
- Operational risk is the risk of loss from failed processes, people and systems, or from external events.
- It includes legal risk but not strategic or reputational risk.
- A framework identifies, assesses, controls, monitors and reports it, using three lines of defence, a risk appetite, R C S A, loss data, key risk indicators, scenarios, reporting and capital.
- Basel's seven event types are assigned by root cause and intent.
- Losses are many small ones plus a few huge ones, so the tail is heavy, and expected annual loss is frequency times mean severity, summed by type.
- Operational resilience means delivering important services through disruption, within impact tolerances that the board owns and tests.

33 Try three quick questions

1. Card fraud: 200 a year, mean $15,000. Rogue trading: 0.5 a year, mean $4m. Expected annual loss?
   Answer: 3.0m + 2.0m = $5.0m a year.
2. A branch employee secretly moves client deposits into her own account. Event type?
   Answer: Internal fraud: a deliberate act by staff.
3. Tolerance 6 hours; a severe but plausible test restores the service in 9. What now?
   Answer: 3-hour gap: remediate, tell the board; do not widen it.

IN THE LESSON

- Now try three quick questions.
- Pause the video, think, then listen to the answers.
- Question one.
- Card fraud happens two hundred times a year with a mean severity of fifteen thousand dollars.
- Rogue trading happens point five times a year with a mean severity of four million dollars.
- What is the expected annual loss?
- Card fraud gives three million and rogue trading gives two million, so five million dollars.
- Question two.
- A branch employee secretly moves client deposits into her own account.
- Which event type?
- Internal fraud, because it is a deliberate act by staff.
- Question three.
- A service has an impact tolerance of six hours, and a severe but plausible test restores it in nine.
- What must the firm do?
- There is a three hour gap, so it must remediate it and tell the board, not widen the tolerance.