POWER-UP YOUR RISK AND CONTROL SUPERPOWERS!

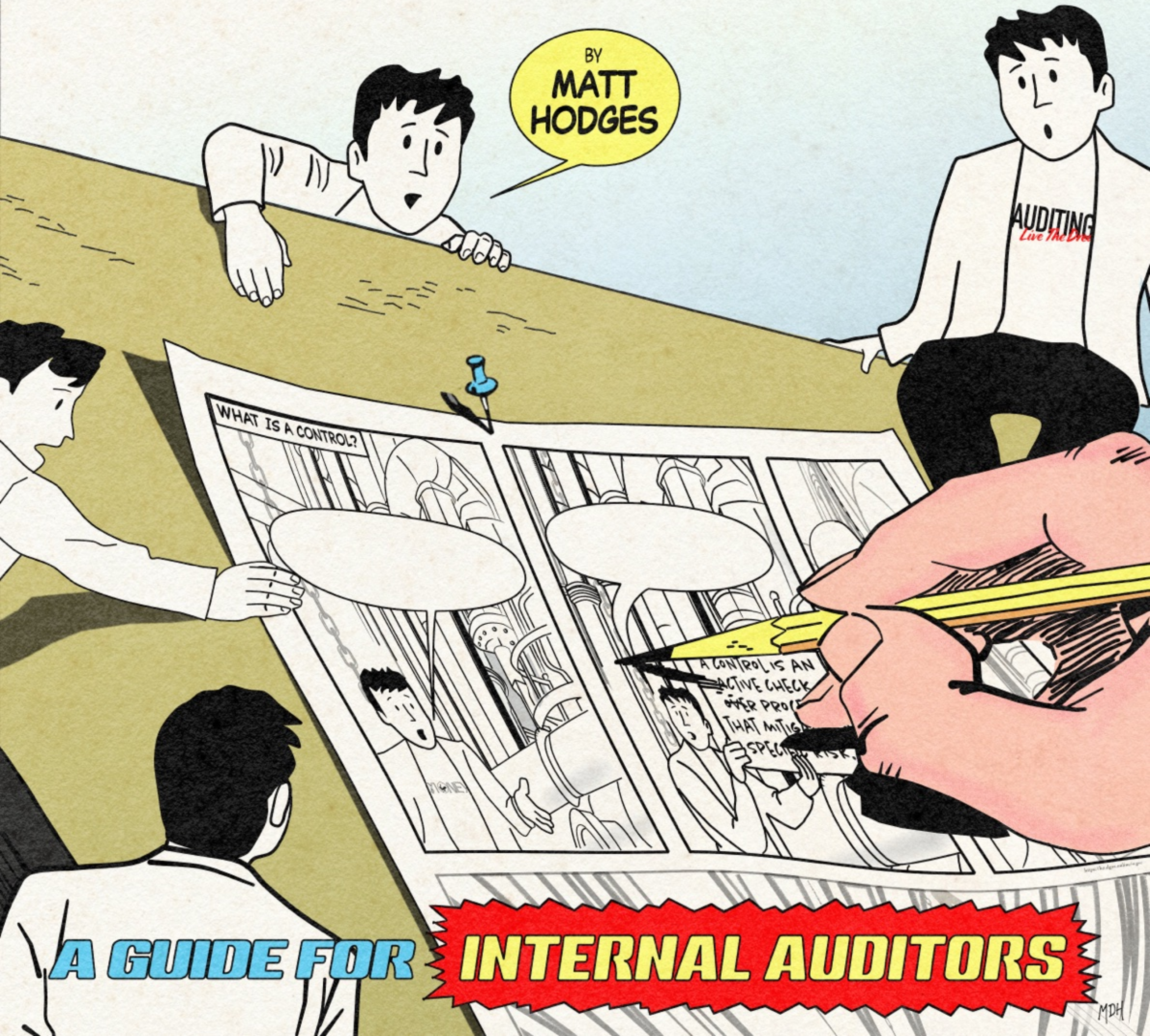
F.R.A.S.E.R.

AUG 2024

VERSION 4

WRITING GREAT

RISKS AND CONTROLS!



BY MATT HODGES

A GUIDE FOR INTERNAL AUDITORS

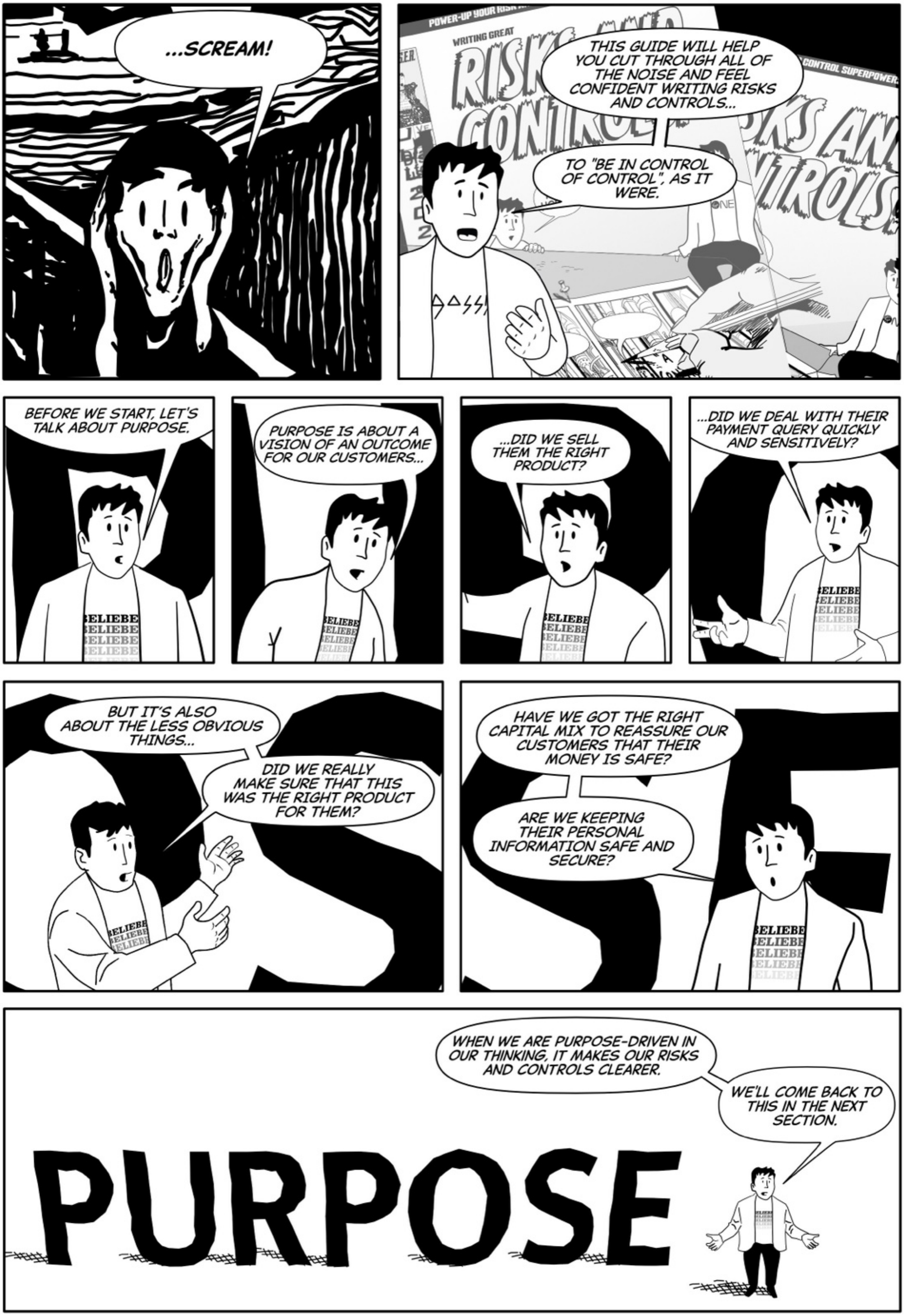
AUDITING
Live The Dre
WHAT IS A CONTROL?
A CONTROL IS AN ACTIVE CHECK OVER PROCE THAT MITIG SPECIFIED RISK
MDH

THE INTERNAL AUDITORS' (NOT ENTIRELY SERIOUS) GUIDE TO WRITING ^GREAT RISKS & CONTROLS!

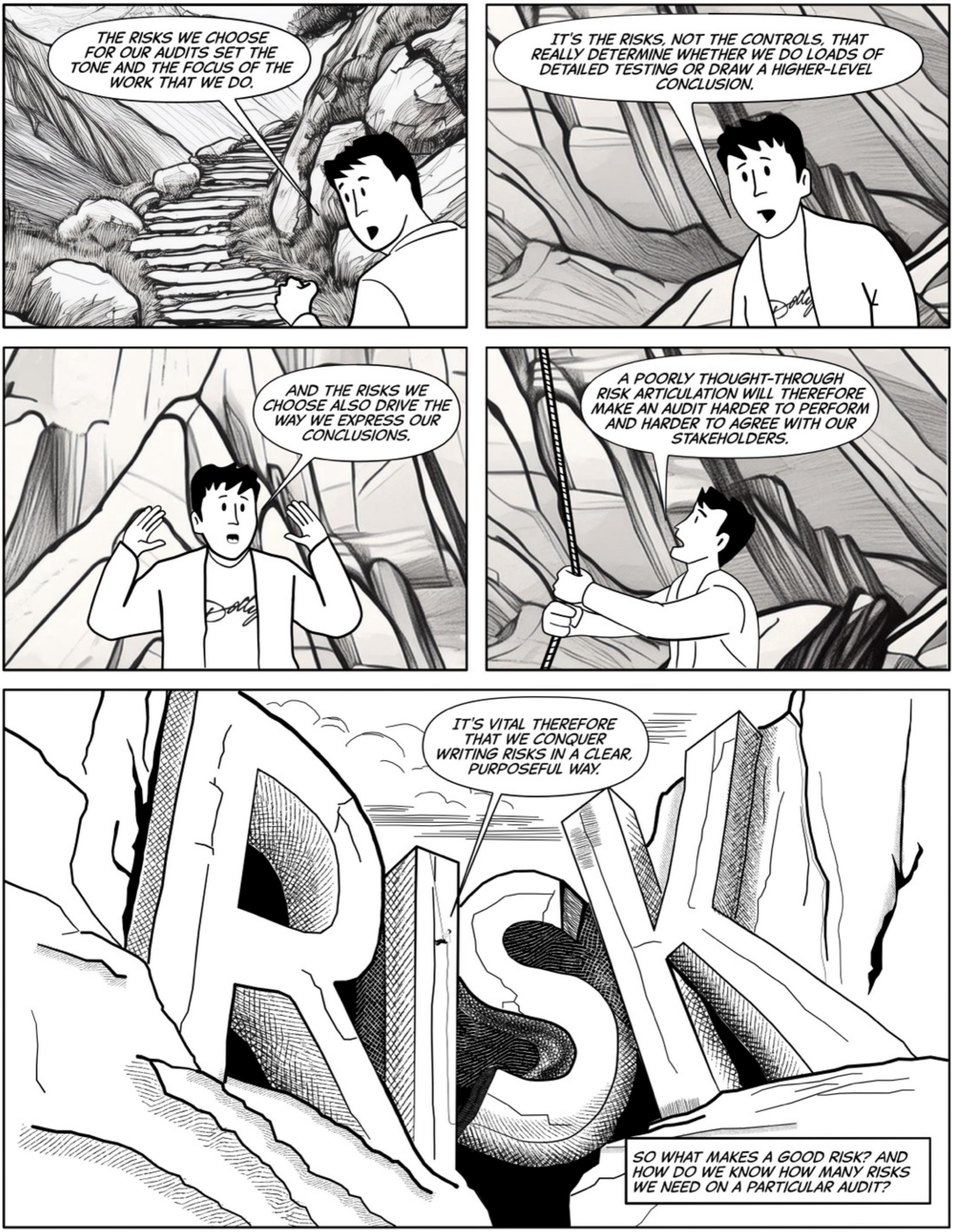
INTRODUCTION

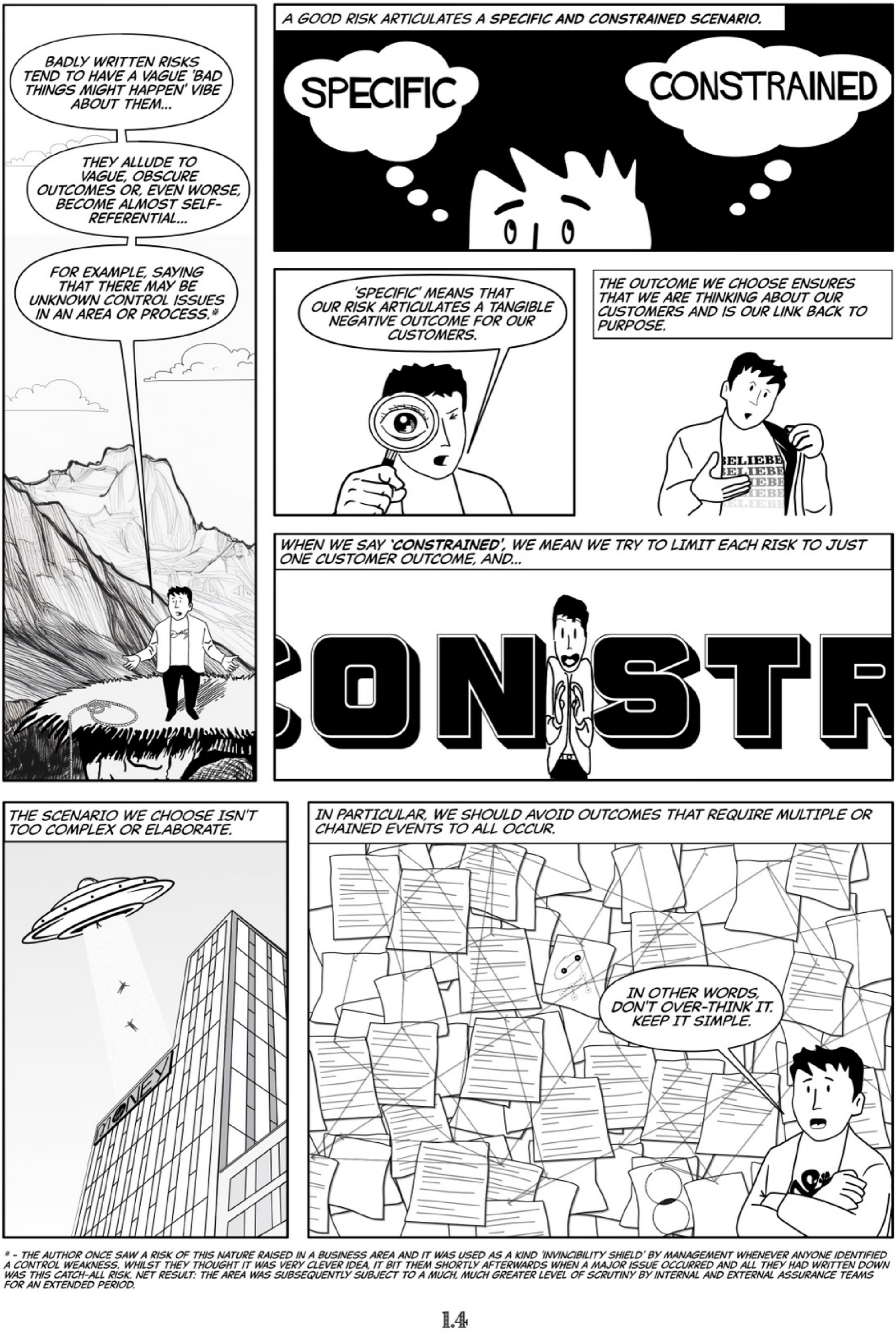
DIRECTIVE
LIKELIHOOD
KRI
AUTOMATED
MEDIUM
MONITORING
CONTROL
FREQUENCY
INHERENT
PROCES
SEVERE
PREVENTATIVE
DETECTIVE
WRITING GOOD RISKS AND CONTROLS IS HARD...
THERE'S A LOT OF JARGON, A SEEMINGLY INFINITE NUMBER OF RISKS THAT YOU COULD AUDIT, AND...
FINDING THE RIGHT NUMBER AND COMBINATION OF CONTROLS CAN SEEM LIKE AN IMPOSSIBLE TASK.
FRANKLY, IT'S ENOUGH TO MAKE YOU WANT TO...

Artwork, script, editing, self-doubt, long-moody-silences and starting-all-over-again by Matt Hodges. This project's home on the internet is at https://ho.dges.online and the latest version of this guide is always available for free from there. I am very grateful for the encouragement, feedback and support from the following people during the completion of this project: Ben Anderson, Lisa Bell, Stuart Clark, Gill Harris, Claire Manson, Claire McFadyen, Ingrid McRitchie, Clare Pollock, Stephen Sabat, my wonderful wife, Lorna, my boys Alex and Ben and Bella the cocker spaniel (evening walk consultant script editor).

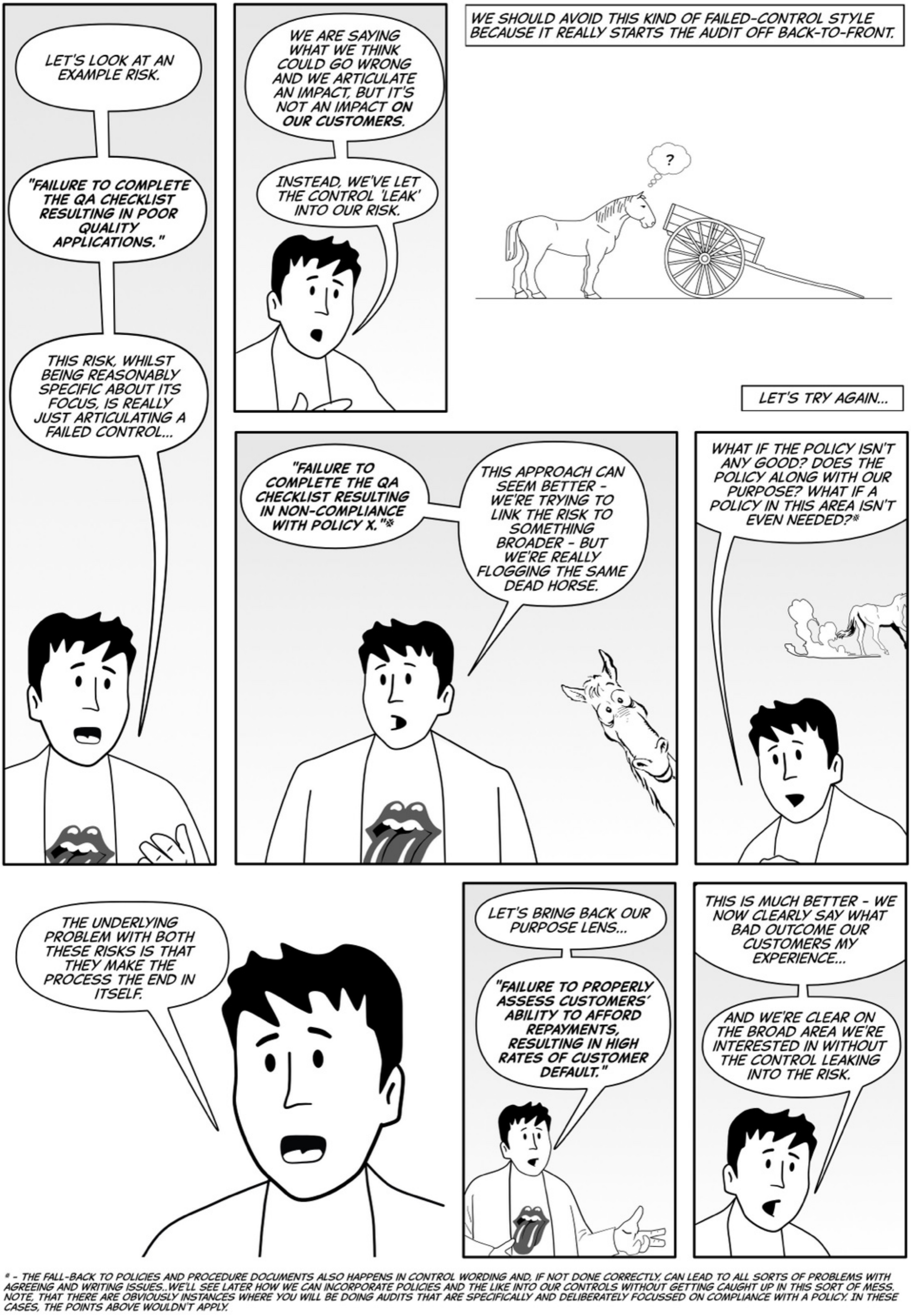

...SCREAM!
POWER-UP YOUR RISK
WRITING GREAT
RISKS AND CONTROLS
CONTROL SUPERPOWER
THIS GUIDE WILL HELP YOU CUT THROUGH ALL OF THE NOISE AND FEEL CONFIDENT WRITING RISKS AND CONTROLS...
TO "BE IN CONTROL OF CONTROL", AS IT WERE.
BEFORE WE START, LET'S TALK ABOUT PURPOSE.
PURPOSE IS ABOUT A VISION OF AN OUTCOME FOR OUR CUSTOMERS...
...DID WE SELL THEM THE RIGHT PRODUCT?
...DID WE DEAL WITH THEIR PAYMENT QUERY QUICKLY AND SENSITIVELY?
BUT IT'S ALSO ABOUT THE LESS OBVIOUS THINGS...
DID WE REALLY MAKE SURE THAT THIS WAS THE RIGHT PRODUCT FOR THEM?
HAVE WE GOT THE RIGHT CAPITAL MIX TO REASSURE OUR CUSTOMERS THAT THEIR MONEY IS SAFE?
ARE WE KEEPING THEIR PERSONAL INFORMATION SAFE AND SECURE?
WHEN WE ARE PURPOSE-DRIVEN IN OUR THINKING, IT MAKES OUR RISKS AND CONTROLS CLEARER.
WE'LL COME BACK TO THIS IN THE NEXT SECTION.
PURPOSE

WRITING GREAT RISKS

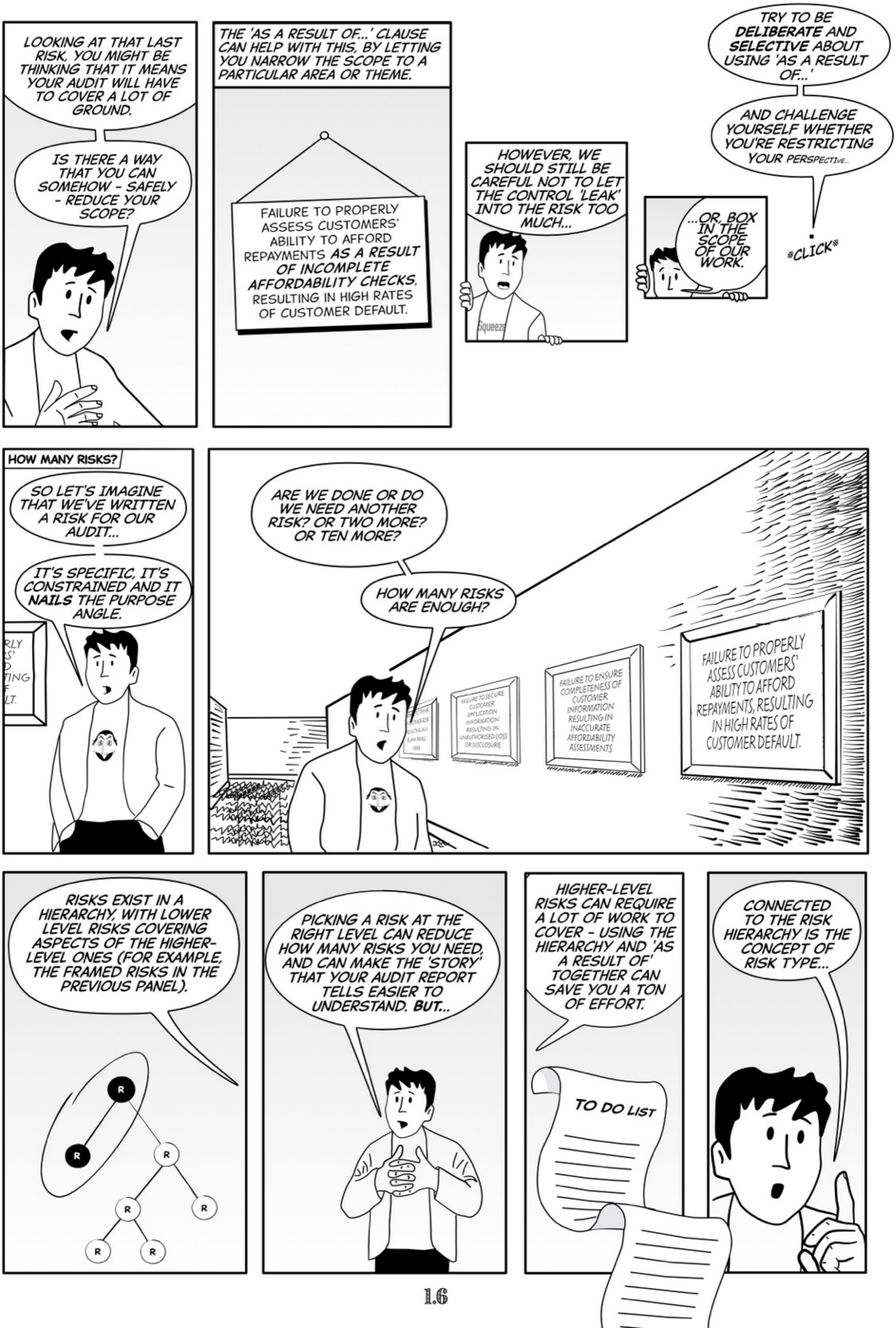

THE RISKS WE CHOOSE FOR OUR AUDITS SET THE TONE AND THE FOCUS OF THE WORK THAT WE DO.
IT'S THE RISKS, NOT THE CONTROLS, THAT REALLY DETERMINE WHETHER WE DO LOADS OF DETAILED TESTING OR DRAW A HIGHER-LEVEL CONCLUSION.
AND THE RISKS WE CHOOSE ALSO DRIVE THE WAY WE EXPRESS OUR CONCLUSIONS.
A POORLY THOUGHT-THROUGH RISK ARTICULATION WILL THEREFORE MAKE AN AUDIT HARDER TO PERFORM AND HARDER TO AGREE WITH OUR STAKEHOLDERS.
IT'S VITAL THEREFORE THAT WE CONQUER WRITING RISKS IN A CLEAR, PURPOSEFUL WAY.
RISK
SO WHAT MAKES A GOOD RISK? AND HOW DO WE KNOW HOW MANY RISKS WE NEED ON A PARTICULAR AUDIT?

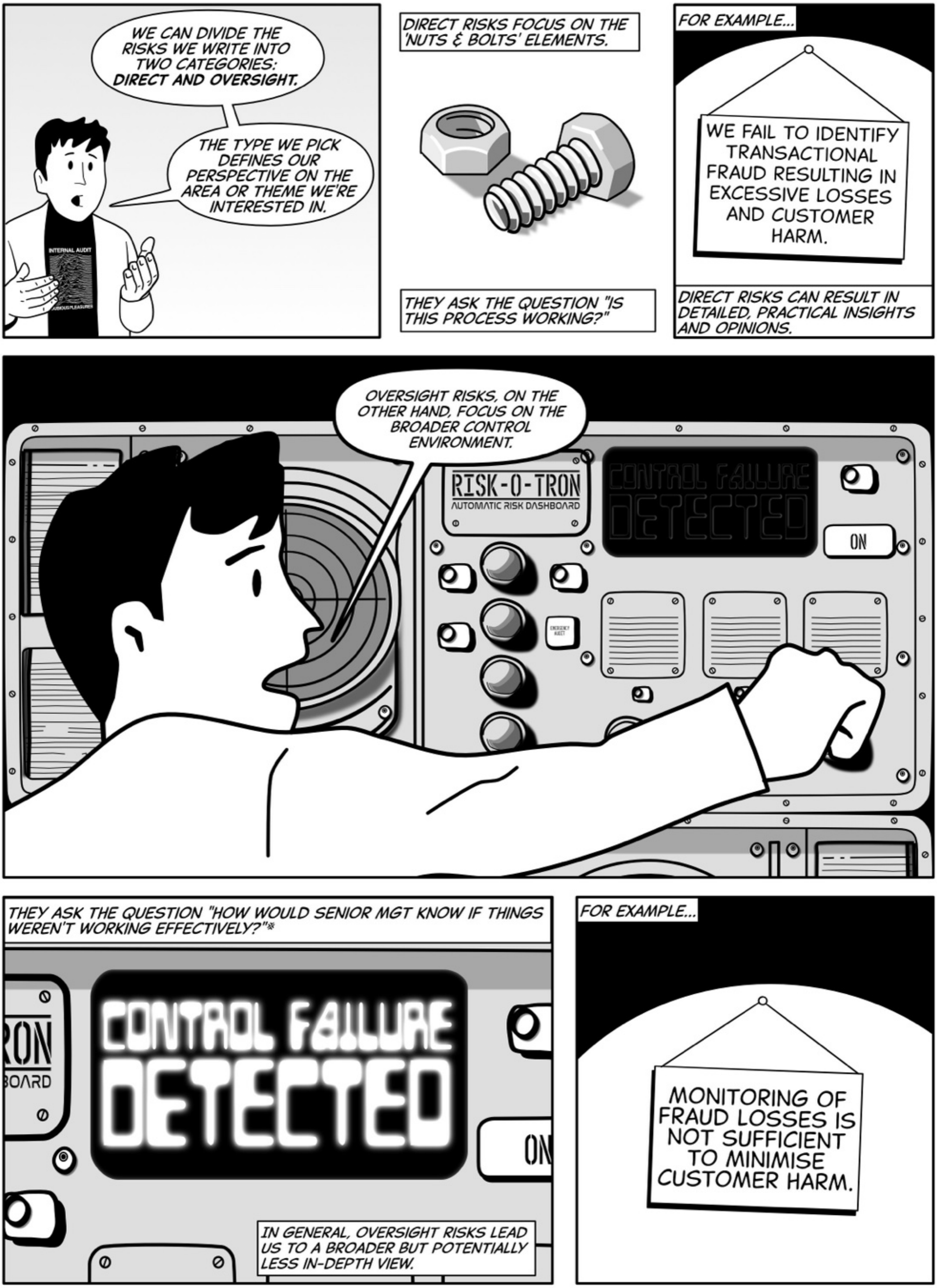

BADLY WRITTEN RISKS TEND TO HAVE A VAGUE 'BAD THINGS MIGHT HAPPEN' VIBE ABOUT THEM...
THEY ALLUDE TO VAGUE, OBSCURE OUTCOMES OR, EVEN WORSE, BECOME ALMOST SELF-REFERENTIAL...
FOR EXAMPLE, SAYING THAT THERE MAY BE UNKNOWN CONTROL ISSUES IN AN AREA OR PROCESS.*
A GOOD RISK ARTICULATES A SPECIFIC AND CONSTRAINED SCENARIO.
SPECIFIC
CONSTRAINED
'SPECIFIC' MEANS THAT OUR RISK ARTICULATES A TANGIBLE NEGATIVE OUTCOME FOR OUR CUSTOMERS.
THE OUTCOME WE CHOOSE ENSURES THAT WE ARE THINKING ABOUT OUR CUSTOMERS AND IS OUR LINK BACK TO PURPOSE.
BELIEBE
WHEN WE SAY 'CONSTRAINED', WE MEAN WE TRY TO LIMIT EACH RISK TO JUST ONE CUSTOMER OUTCOME, AND...
CONSTR
THE SCENARIO WE CHOOSE ISN'T TOO COMPLEX OR ELABORATE.
MONEY
IN PARTICULAR, WE SHOULD AVOID OUTCOMES THAT REQUIRE MULTIPLE OR CHAINED EVENTS TO ALL OCCUR.
IN OTHER WORDS, DON'T OVER-THINK IT. KEEP IT SIMPLE.

* - THE AUTHOR ONCE SAW A RISK OF THIS NATURE RAISED IN A BUSINESS AREA AND IT WAS USED AS A KIND 'INVINCIBILITY SHIELD' BY MANAGEMENT WHENEVER ANYONE IDENTIFIED A CONTROL WEAKNESS. WHILST THEY THOUGHT IT WAS VERY CLEVER IDEA, IT BIT THEM SHORTLY AFTERWARDS WHEN A MAJOR ISSUE OCCURRED AND ALL THEY HAD WRITTEN DOWN WAS THIS CATCH-ALL RISK. NET RESULT: THE AREA WAS SUBSEQUENTLY SUBJECT TO A MUCH, MUCH GREATER LEVEL OF SCRUTINY BY INTERNAL AND EXTERNAL ASSURANCE TEAMS FOR AN EXTENDED PERIOD.


LET'S LOOK AT AN EXAMPLE RISK.
"FAILURE TO COMPLETE THE QA CHECKLIST RESULTING IN POOR QUALITY APPLICATIONS."
THIS RISK, WHILST BEING REASONABLY SPECIFIC ABOUT ITS FOCUS, IS REALLY JUST ARTICULATING A FAILED CONTROL...
WE ARE SAYING WHAT WE THINK COULD GO WRONG AND WE ARTICULATE AN IMPACT, BUT IT'S NOT AN IMPACT ON OUR CUSTOMERS.
INSTEAD, WE'VE LET THE CONTROL 'LEAK' INTO OUR RISK.
WE SHOULD AVOID THIS KIND OF FAILED-CONTROL STYLE BECAUSE IT REALLY STARTS THE AUDIT OFF BACK-TO-FRONT.
?
LET'S TRY AGAIN...
"FAILURE TO COMPLETE THE QA CHECKLIST RESULTING IN NON-COMPLIANCE WITH POLICY X."*
THIS APPROACH CAN SEEM BETTER - WE'RE TRYING TO LINK THE RISK TO SOMETHING BROADER - BUT WE'RE REALLY FLOGGING THE SAME DEAD HORSE.
WHAT IF THE POLICY ISN'T ANY GOOD? DOES THE POLICY ALONG WITH OUR PURPOSE? WHAT IF A POLICY IN THIS AREA ISN'T EVEN NEEDED?*
THE UNDERLYING PROBLEM WITH BOTH THESE RISKS IS THAT THEY MAKE THE PROCESS THE END IN ITSELF.
LET'S BRING BACK OUR PURPOSE LENS...
"FAILURE TO PROPERLY ASSESS CUSTOMERS' ABILITY TO AFFORD REPAYMENTS, RESULTING IN HIGH RATES OF CUSTOMER DEFAULT."
THIS IS MUCH BETTER - WE NOW CLEARLY SAY WHAT BAD OUTCOME OUR CUSTOMERS MY EXPERIENCE...
AND WE'RE CLEAR ON THE BROAD AREA WE'RE INTERESTED IN WITHOUT THE CONTROL LEAKING INTO THE RISK.

* - THE FALL-BACK TO POLICIES AND PROCEDURE DOCUMENTS ALSO HAPPENS IN CONTROL WORDING AND, IF NOT DONE CORRECTLY, CAN LEAD TO ALL SORTS OF PROBLEMS WITH AGREEING AND WRITING ISSUES..WE'LL SEE LATER HOW WE CAN INCORPORATE POLICIES AND THE LIKE INTO OUR CONTROLS WITHOUT GETTING CAUGHT UP IN THIS SORT OF MESS. NOTE, THAT THERE ARE OBVIOUSLY INSTANCES WHERE YOU WILL BE DOING AUDITS THAT ARE SPECIFICALLY AND DELIBERATELY FOCUSSED ON COMPLIANCE WITH A POLICY. IN THESE CASES, THE POINTS ABOVE WOULDN'T APPLY.


LOOKING AT THAT LAST RISK, YOU MIGHT BE THINKING THAT IT MEANS YOUR AUDIT WILL HAVE TO COVER A LOT OF GROUND.
IS THERE A WAY THAT YOU CAN SOMEHOW - SAFELY - REDUCE YOUR SCOPE?
THE 'AS A RESULT OF...' CLAUSE CAN HELP WITH THIS, BY LETTING YOU NARROW THE SCOPE TO A PARTICULAR AREA OR THEME.
FAILURE TO PROPERLY ASSESS CUSTOMERS' ABILITY TO AFFORD REPAYMENTS **AS A RESULT OF INCOMPLETE AFFORDABILITY CHECKS**, RESULTING IN HIGH RATES OF CUSTOMER DEFAULT.
HOWEVER, WE SHOULD STILL BE CAREFUL NOT TO LET THE CONTROL 'LEAK' INTO THE RISK TOO MUCH...
Squeeze
...OR, BOX IN THE SCOPE OF OUR WORK.
TRY TO BE **DELIBERATE** AND **SELECTIVE** ABOUT USING 'AS A RESULT OF...'
AND CHALLENGE YOURSELF WHETHER YOU'RE RESTRICTING YOUR PERSPECTIVE...
CLICK
HOW MANY RISKS?
SO LET'S IMAGINE THAT WE'VE WRITTEN A RISK FOR OUR AUDIT...
IT'S SPECIFIC, IT'S CONSTRAINED AND IT **NAILS** THE PURPOSE ANGLE.
ARE WE DONE OR DO WE NEED ANOTHER RISK? OR TWO MORE? OR TEN MORE?
HOW MANY RISKS ARE ENOUGH?
TO THINK ANOTHER RISK RESULTING IN A BLANK PANEL HERE
FAILURE TO SECURE CUSTOMER APPLICATION INFORMATION RESULTING IN UNAUTHORISED LOSS OR DISCLOSURE
FAILURE TO ENSURE COMPLETENESS OF CUSTOMER INFORMATION RESULTING IN INACCURATE AFFORDABILITY ASSESSMENTS
FAILURE TO PROPERLY ASSESS CUSTOMERS' ABILITY TO AFFORD REPAYMENTS, RESULTING IN HIGH RATES OF CUSTOMER DEFAULT.
RISKS EXIST IN A HIERARCHY, WITH LOWER LEVEL RISKS COVERING ASPECTS OF THE HIGHER-LEVEL ONES (FOR EXAMPLE, THE FRAMED RISKS IN THE PREVIOUS PANEL).
R
R
R
R
R
R
R
PICKING A RISK AT THE RIGHT LEVEL CAN REDUCE HOW MANY RISKS YOU NEED, AND CAN MAKE THE 'STORY' THAT YOUR AUDIT REPORT TELLS EASIER TO UNDERSTAND. **BUT...**
HIGHER-LEVEL RISKS CAN REQUIRE A LOT OF WORK TO COVER - USING THE HIERARCHY AND 'AS A RESULT OF' TOGETHER CAN SAVE YOU A TON OF EFFORT.
TO DO LIST
CONNECTED TO THE RISK HIERARCHY IS THE CONCEPT OF RISK TYPE...


WE CAN DIVIDE THE RISKS WE WRITE INTO TWO CATEGORIES: **DIRECT AND OVERSIGHT.**
THE TYPE WE PICK DEFINES OUR PERSPECTIVE ON THE AREA OR THEME WE'RE INTERESTED IN.
INTERNAL AUDIT
DUBIOUS PLEASURES
DIRECT RISKS FOCUS ON THE 'NUTS & BOLTS' ELEMENTS.
THEY ASK THE QUESTION "IS THIS PROCESS WORKING?"
FOR EXAMPLE...
WE FAIL TO IDENTIFY TRANSACTIONAL FRAUD RESULTING IN EXCESSIVE LOSSES AND CUSTOMER HARM.
DIRECT RISKS CAN RESULT IN DETAILED, PRACTICAL INSIGHTS AND OPINIONS.
OVERSIGHT RISKS, ON THE OTHER HAND, FOCUS ON THE BROADER CONTROL ENVIRONMENT.
RISK-O-TRON
AUTOMATIC RISK DASHBOARD
CONTROL FAILURE DETECTED
ON
EMERGENCY AUDIT
THEY ASK THE QUESTION "HOW WOULD SENIOR MGT KNOW IF THINGS WEREN'T WORKING EFFECTIVELY?"*
CONTROL FAILURE DETECTED
IN GENERAL, OVERSIGHT RISKS LEAD US TO A BROADER BUT POTENTIALLY LESS IN-DEPTH VIEW.
FOR EXAMPLE...
MONITORING OF FRAUD LOSSES IS NOT SUFFICIENT TO MINIMISE CUSTOMER HARM.

* - I'VE USED THE PHRASE '**SENIOR** MGT' HERE VERY DELIBERATELY: OVERSIGHT-FOCUSSED RISKS ARE GENERALLY ABOUT THE TOP-DOWN VIEW OF RISK MITIGATION - HOW DO THE PEOPLE THAT HAVE ACCOUNTABILITY FOR THE AREAS WE'RE INTERESTED IN ACTUALLY FIND OUT IF THERE'S A PROBLEM AT AN AGGREGATE LEVEL? THIS IS DIFFERENT FROM DIRECT RISKS WHERE WE TEND TO BE MORE INTERESTED IN HOW THE CONTROLS AT THE 'COAL-FACE' OPERATE TO IDENTIFY PROBLEMS WITH INDIVIDUAL CUSTOMERS, TRANSACTIONS ETC.

ONE FINAL THING...
SOMETIMES, WE START AN AUDIT KNOWING THERE IS AN ISSUE.
IT CAN BE TEMPTING TO WRITE A RISK FOR THE AUDIT THAT JUST SETS THIS UP...
AUDIT REPORT
LATE NIGHT FINAL
FINAL
BROKEN GLASS ISSUE!
3RD NOVERMBER, 2006
FOURTH WALL SHATTERED – FULL REPORT PAGE 5
Aliquam vel quam ut tellus gravida faucibus. Vivamus justo
elementum vitae, malesuada eu, ferm
amet justo. In
THE DANGER WITH THIS IS THAT WE MIGHT NARROW OUR FOCUS ONTO JUST THAT AREA. AND MISS SOMETHING ELSE, OR DO AN ENTIRE AUDIT JUST TO POINT OUT SOMETHING WE ALREADY KNEW.
INSTEAD, WE SHOULD CHALLENGE OURSELVES TO COME UP WITH A BETTER RISK – MAYBE THE ISSUE IS A SYMPTOM OF A MUCH BIGGER PROBLEM, OR MAYBE MGT OVERSIGHT ISN'T WHAT IT SHOULD BE.*

* – DEPENDING ON THE CULTURE OF RISK MGT AND CONTROL IN THE AREA IN QUESTION, IT MAY EVEN BE BETTER TO NOT DO AN AUDIT AT ALL AND PERSUADE MGT THAT THEY SHOULD RAISE THEIR OWN ISSUE ABOUT THE PROBLEM. YOUR AVERAGE MANAGER IN AN OPERATIONAL ROLE WILL NORMALLY PREFER A SELF-IDENTIFIED ISSUE TO AN AUDIT ISSUE, AND IT MEANS YOU CAN FOCUS YOUR AUDIT WORK IN OTHER AREAS.

SUMMARY - GOOD RISKS CHEATSHEET

HERE'S A FEW POINTERS FOR EACH KEY CONCEPT FOR YOU TO CONSIDER WHEN WRITING RISKS.
DON'T HOWEVER JUST USE THIS AS A MECHANICAL CHECKLIST: INSTEAD, USE IT AS A WAY OF CHALLENGING YOURSELF TO FIND THE RIGHT RISK (OR RISKS) FOR YOUR AUDIT.
FINALLY, HERE ARE SOME BORROWED WISE WORDS THAT MAY HELP YOU AS YOUR WRITE YOUR RISKS:
SIMPLE IS BETTER THAN COMPLEX...
COMPLEX IS BETTER THAN COMPLICATED...
PRACTICALITY BEATS PURITY.*
SUMMARY - GOOD RISKS CHEATSHEET

1 SPECIFIC

- **Focus on customer impact**. What negative outcome would they see if the risk materialised (either individual customers or groups of customers)?
- But **beware of outcomes that require multiple 'and if...' statements** to define: there are probably simpler, more likely risks in the same space.
- **Not following a process or complying with a policy is not in itself a risk.** What was the policy trying to achieve for our customers? Does your risk pass a 'so what?' test?
- For audits that aren't directly about customers, **be very clear about who the risk will impact** - the Board? Colleagues?

2 CONSTRAINED

- **Risks aren't Hollywood movie scripts** - keep your risks to those that might actually happen, not disaster-movie scenarios.
- **Stick to a single outcome for your risks**, and focus on clarity rather than trying to shoehorn in multiple, separate outcomes.
- **Don't word your risks to require perfection** - we can't expect that no errors will ever occur (for example, we wouldn't expect fraud controls to reduce fraud completely to zero). Think about what a good outcome for our customers would look like, including how we'd know that it's good enough.

3 AS A RESULT OF...

- **Don't let the controls you expect to review 'leak' into the risk wording** except as part of a deliberate decision.
- Don't use 'as a result of...' clauses unless you **understand how it will limit your scope and opinion.**
- Be very careful with the wording of the clause that you **understand the implications for your scope** and reflect on whether your audit title is still appropriate (or too broad).

  If you do use 'as a result of...', make sure that you **don't descope too much**: if you are only looking at a tiny slice of a risk, it can be hard to form a worthwhile opinion.

4 NO. OF RISKS

- If your risk is specific enough, **you may only need one**. Ask yourself whether further risks are really needed or whether a single higher-level risk will do the same job (yes, this is the opposite point to the bullet in box 3. Balancing these two concepts is key).
- Similarly, if there are multiple risks that could be in scope, **ask whether we need to cover them all on this audit** or whether we could cover them in a separate, future one.
- **Don't use risks as a way of partitioning scope areas within the team.** Having a separate technology, ops or change sub-risk may not be adding anything to your audit except extra work.

5 DIRECT OR OVERSIGHT

- If your outcome is about the **cumulative impact on customers**, you may want to consider an oversight focussed risk. If your outcome is more about **how individual customers are affected**, a direct risk may be more appropriate. If you think your outcome is about both, your risk is outcome focussed.
- Direct risks in combination with 'as a result of...' clauses can be **more susceptible to controls leaking into the risk** wording because they tend to focus on 'nuts and bolts'.
- If you go for an oversight risk, your **scope will probably start with some high-level MI and work backwards**. **Direct risks can start at the bottom and work up**. Make this an explicit decision (and make sure your stakeholders understand the focus too).

6 ISSUES IN DISGUISE

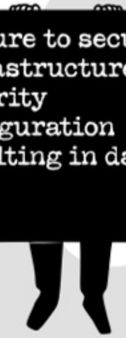
- **An audit isn't the only way for us to raise issues.** If you think something is broken, speak to your stakeholders. They may agree, raise an issue themselves and save you an audit.
- Remember that **the best audit work links outcomes to root causes**. If your risk narrows your focus too much, you might find getting to root cause - or other issues - much harder.
- If you do write a risk that hints at an issue, the risk wording must still make clear the outcome that will result from the problem. **Don't assume any issue is self-evident.**

-*THE ZEN OF PYTHON' BY MARK PETERS.

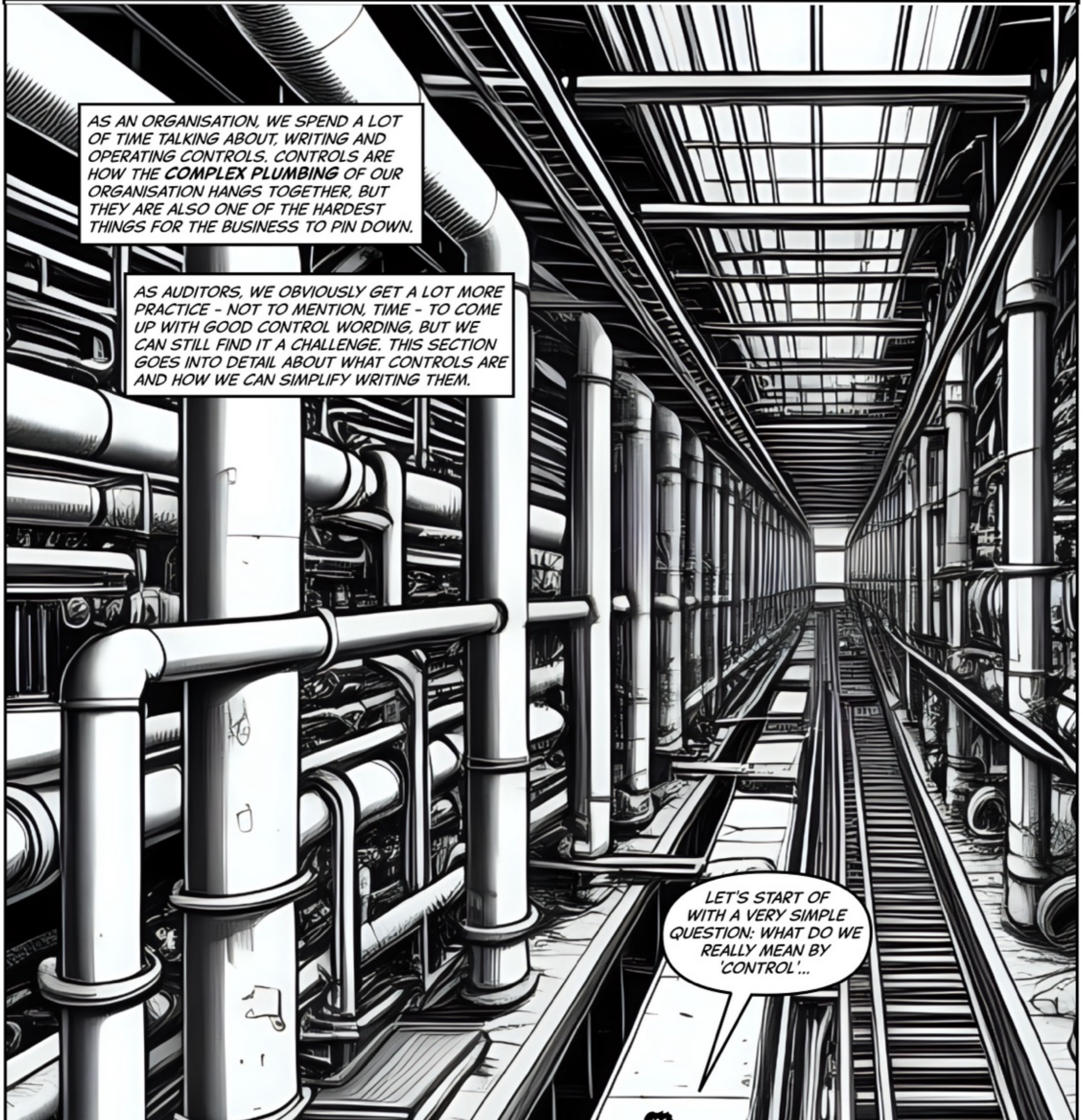
SUMMARY - APPLYING THE CONCEPTS

HERE'S A FEW WORKED EXAMPLES TO SHOW YOU HOW YOU CAN APPLY THE CONCEPTS WE'VE COVERED.
AS AUDITORS, YOU MIGHT READ SOME OF THESE AND THINK THAT THEY DON'T FULLY ALIGN TO ONE OR MORE OF THE CONCEPTS WE'VE COVERED.
OR, YOU MIGHT THINK THERE IS A BETTER RISK TO BE WRITTEN THAT DELIBERATELY VIOLATES ONE OF THESE PRINCIPLES.
IF THAT HAPPENS, MY WORK HERE IS DONE: THE POINT OF THIS IS NOT TO HAVE A RIGID SET OF RULES THAT ARE ALWAYS APPLIED. THE POINT IS TO MAKE RISK ARTICULATION A MORE ACTIVE AND CONSIDERED PROCESS.
AUDITING
Live the dream!

Basic	Better	Best
Failure to secure infrastructure security configuration in line with the information security standard.	Failure to secure infrastructure security configuration resulting in data loss.	Failure to protect customer data at rest and in transit, resulting in unauthorised access to sensitive customer information.
Audit teams don't complete their audit files properly.	Audit teams' audit files don't effectively manage audit risk.	Audit delivery does not highlight material control issues resulting in poor decision-making by senior management.
Failure to prevent fraud.	Failure to prevent fraud because of incomplete transactional fraud checks.	Transactional fraud exceeds risk appetite as a result of incomplete fraud checks, resulting in material losses to customers



UNDERSTANDING CONTROLS

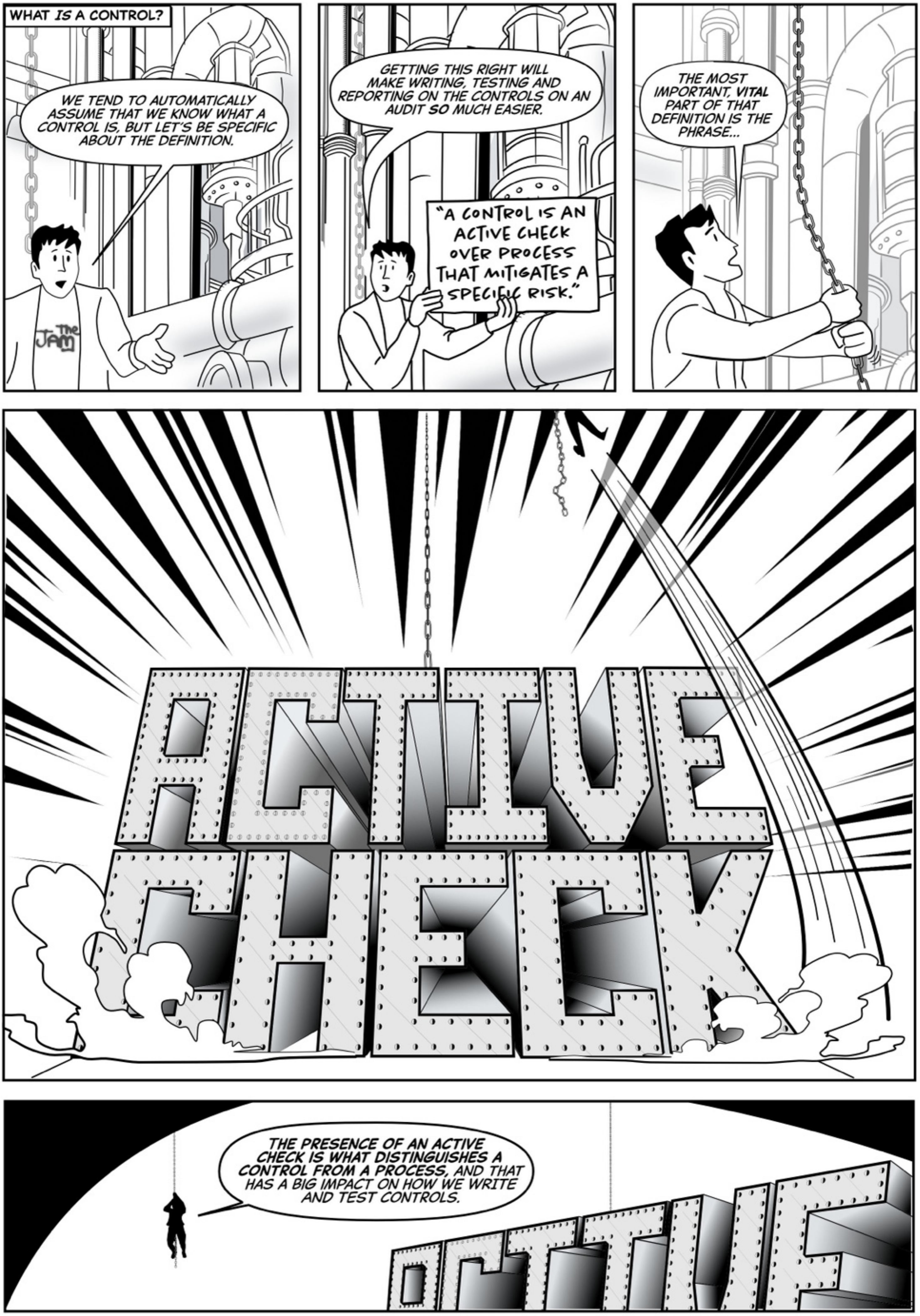


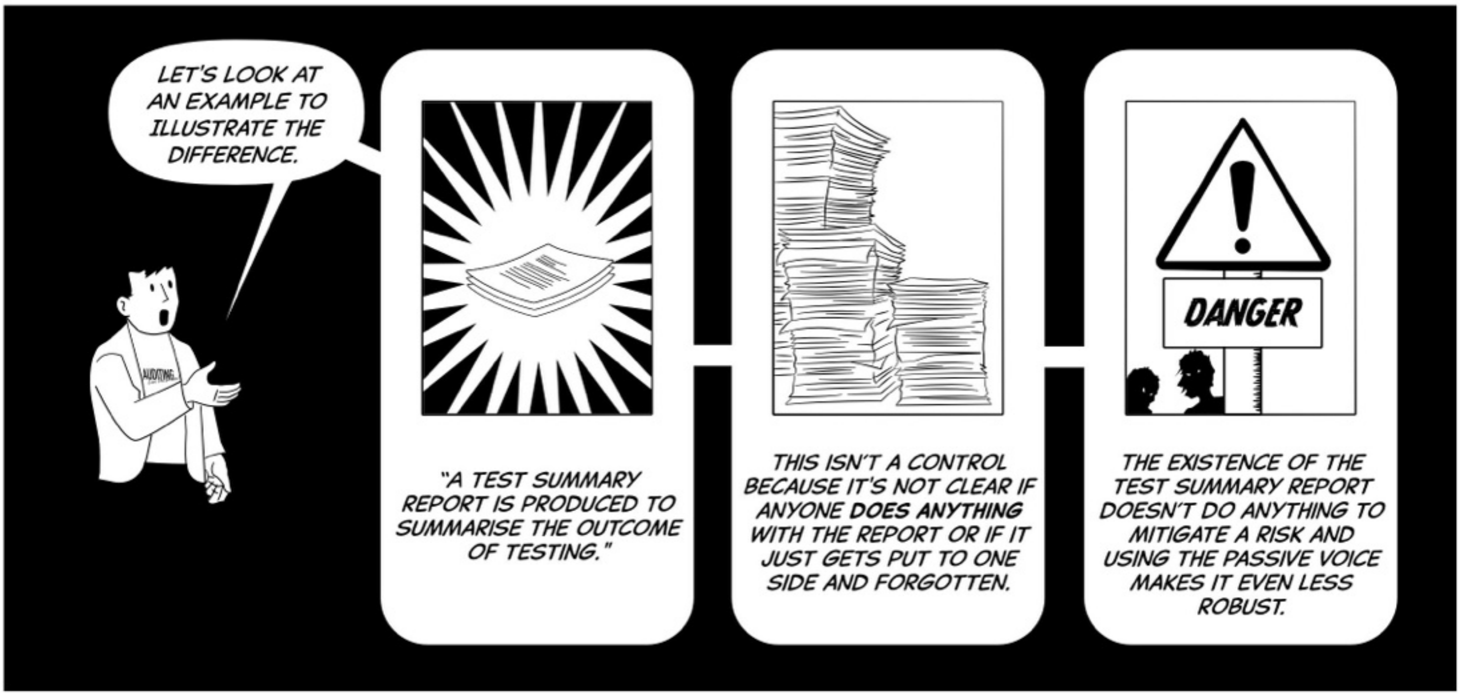
AS AN ORGANISATION, WE SPEND A LOT OF TIME TALKING ABOUT, WRITING AND OPERATING CONTROLS. CONTROLS ARE HOW THE **COMPLEX PLUMBING** OF OUR ORGANISATION HANGS TOGETHER, BUT THEY ARE ALSO ONE OF THE HARDEST THINGS FOR THE BUSINESS TO PIN DOWN.

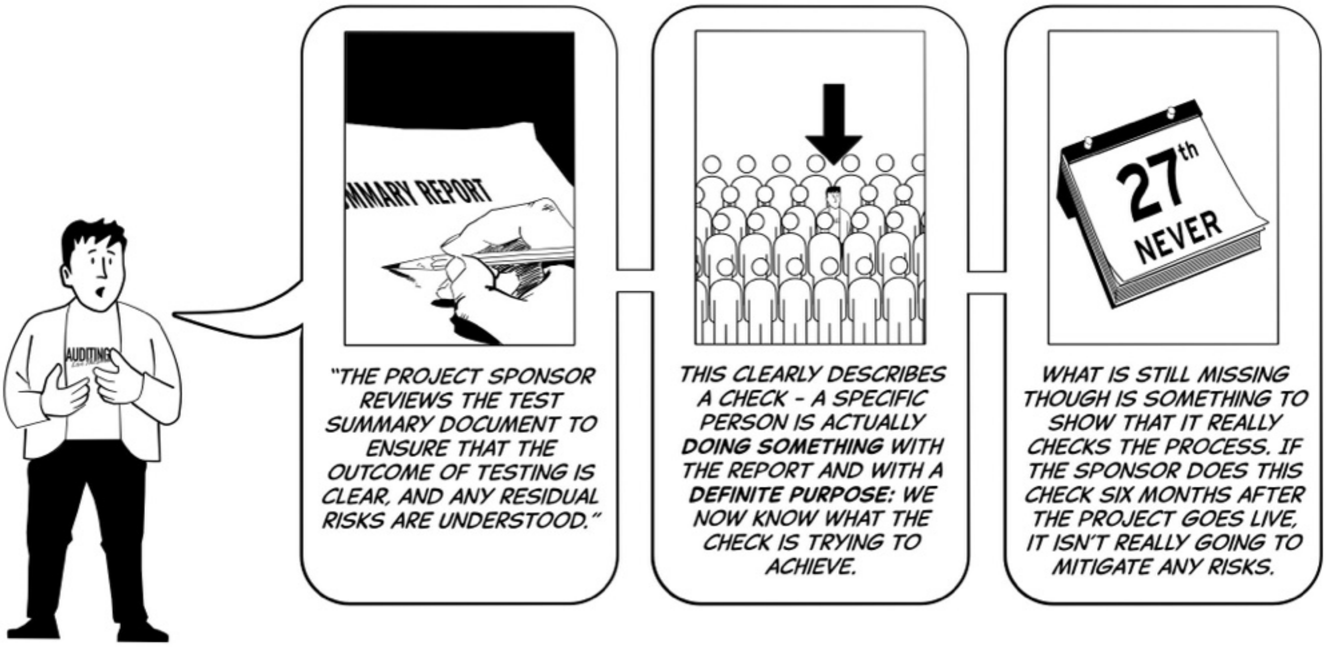
AS AUDITORS, WE OBVIOUSLY GET A LOT MORE PRACTICE - NOT TO MENTION, TIME - TO COME UP WITH GOOD CONTROL WORDING, BUT WE CAN STILL FIND IT A CHALLENGE. THIS SECTION GOES INTO DETAIL ABOUT WHAT CONTROLS ARE AND HOW WE CAN SIMPLIFY WRITING THEM.

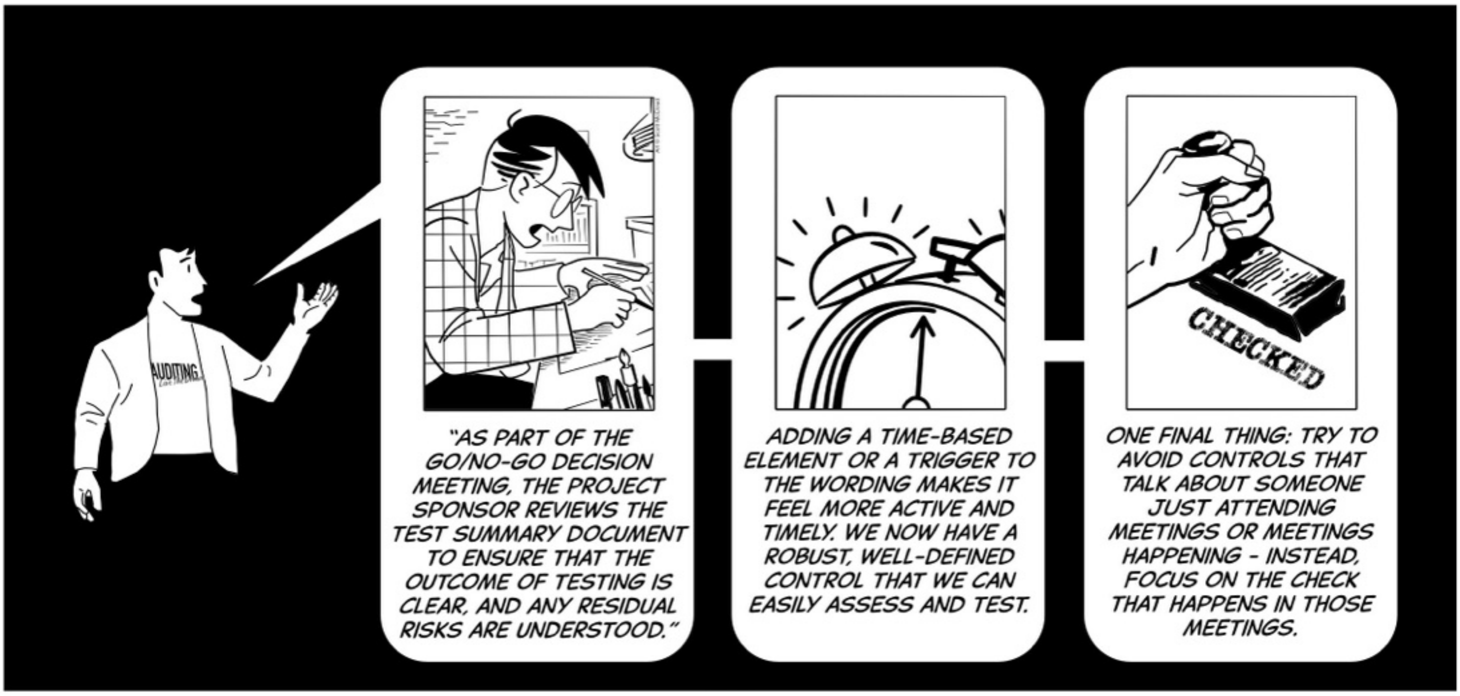
LET'S START OF WITH A VERY SIMPLE QUESTION: WHAT DO WE REALLY MEAN BY 'CONTROL'...

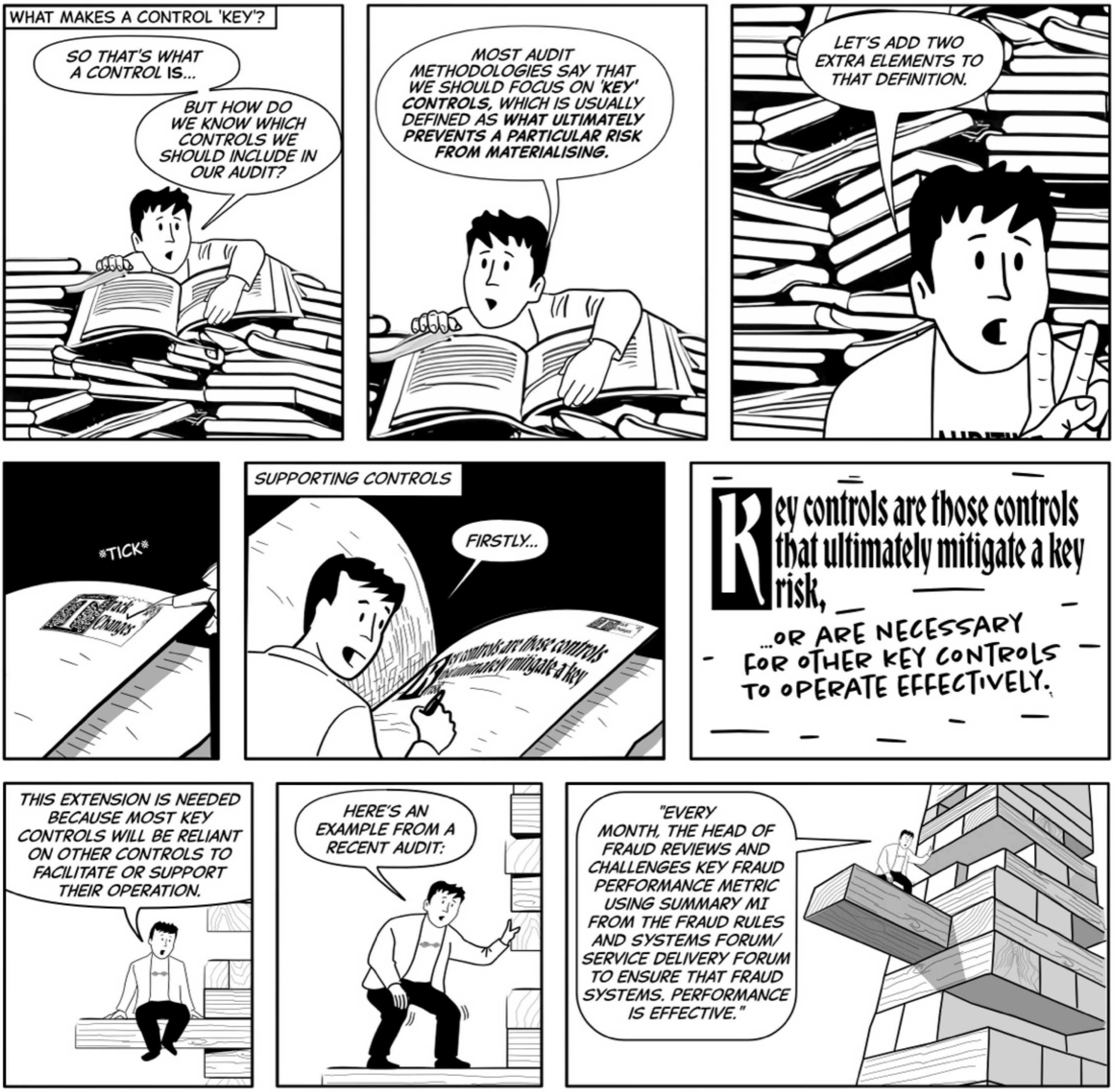
AUTHOR'S NOTE - YOU MIGHT BE TEMPTED TO SKIP THIS CHAPTER AS IT SEEMS A BIT THEORETICAL, OR BECAUSE YOU THINK YOU ALREADY KNOW WHAT A CONTROL IS. MY ADVICE IS THAT YOU DON'T (AND NOT JUST BECAUSE I'VE SPENT AGES DRAWING AND WRITING THIS CHAPTER). WHAT WE COVER IN THIS CHAPTER IS ABSOLUTELY KEY TO THE SUBSEQUENT MORE PRACTICAL STUFF. YOU NEVER KNOW, YOU MIGHT EVEN LEARN SOMETHING.

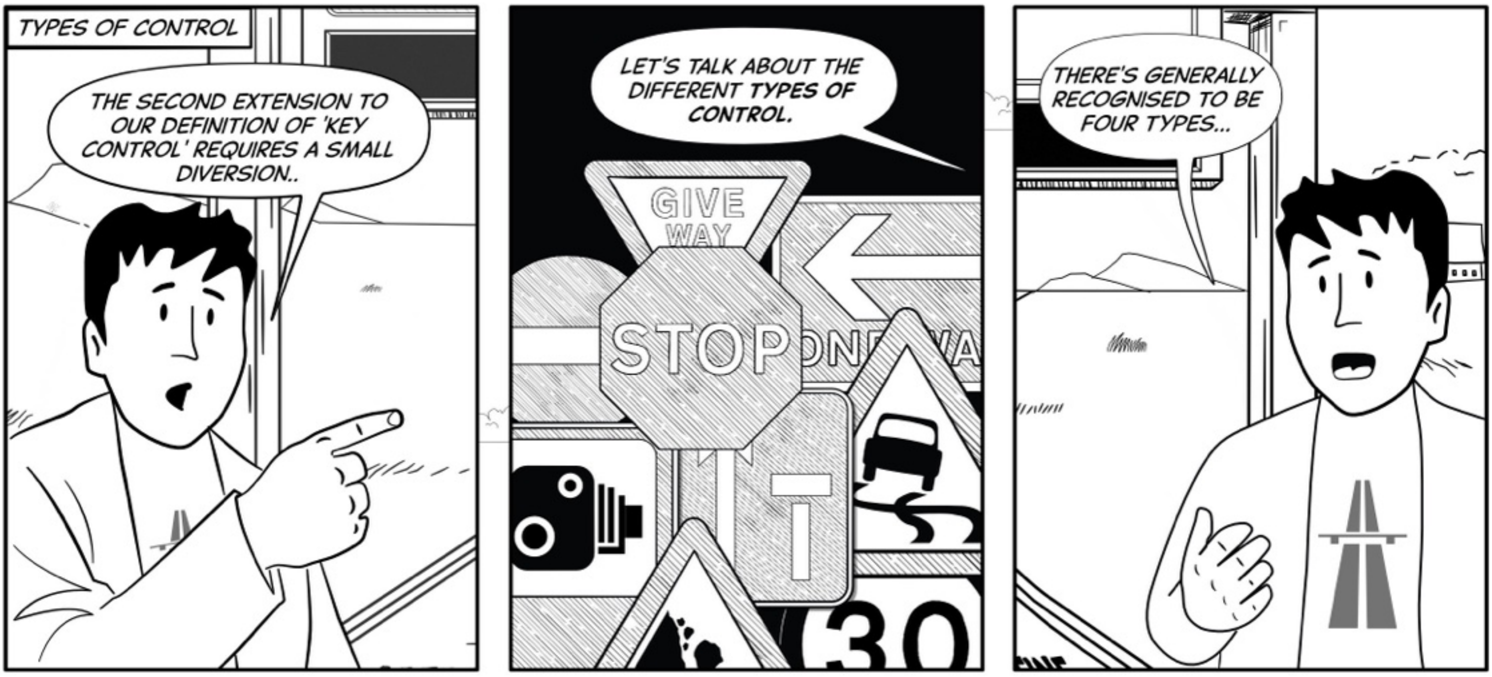

WHAT *IS* A CONTROL?
WE TEND TO AUTOMATICALLY ASSUME THAT WE KNOW WHAT A CONTROL IS, BUT LET'S BE SPECIFIC ABOUT THE DEFINITION.
The JAM
GETTING THIS RIGHT WILL MAKE WRITING, TESTING AND REPORTING ON THE CONTROLS ON AN AUDIT **SO MUCH** EASIER.
"A CONTROL IS AN ACTIVE CHECK OVER PROCESS THAT MITIGATES A SPECIFIC RISK."
THE MOST IMPORTANT, **VITAL** PART OF THAT DEFINITION IS THE PHRASE...
ACTIVE CHECK
THE PRESENCE OF AN ACTIVE CHECK IS WHAT DISTINGUISHES A CONTROL FROM A PROCESS, AND THAT HAS A BIG IMPACT ON HOW WE WRITE AND TEST CONTROLS.
ACTIVE

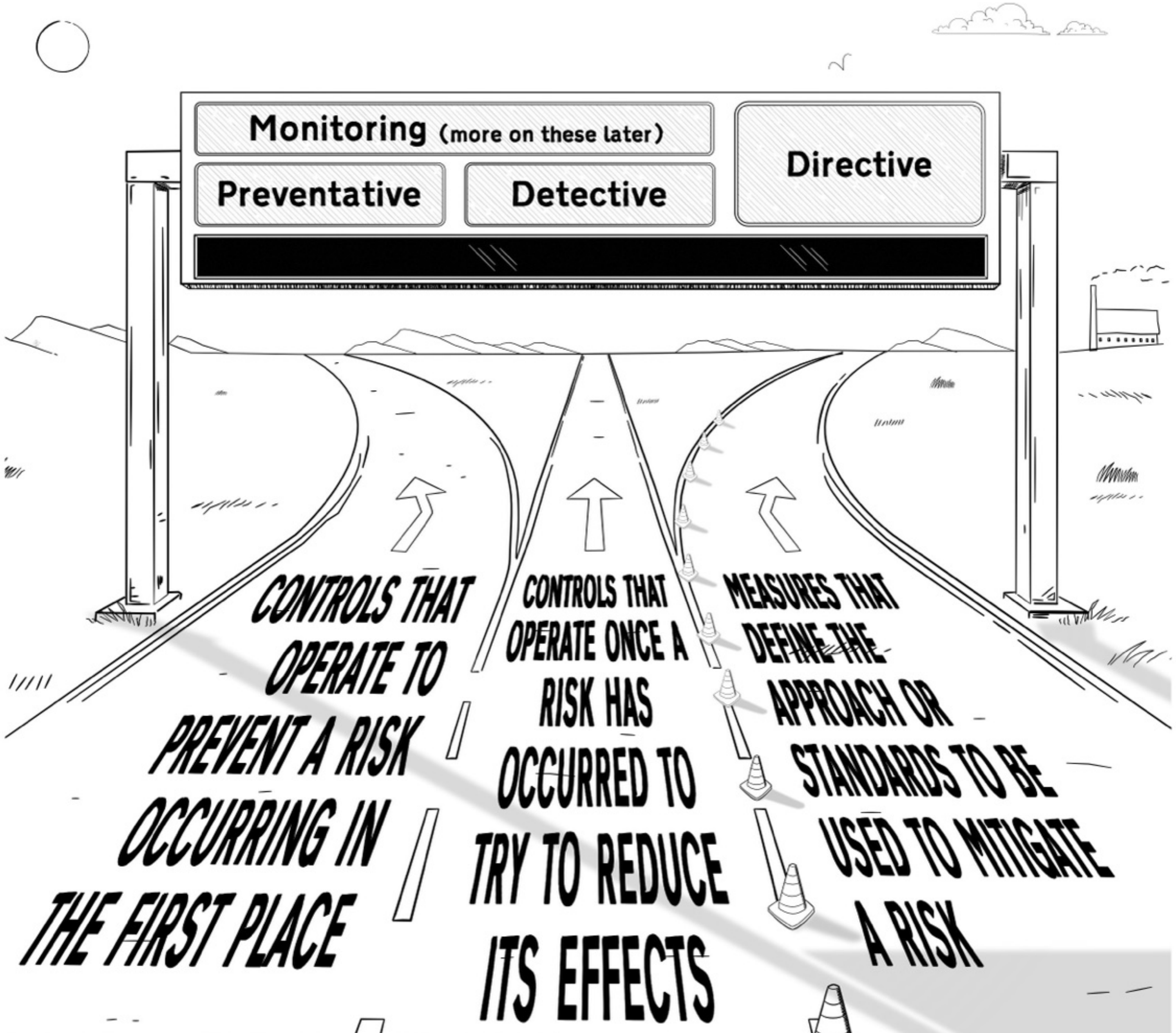

LET'S LOOK AT AN EXAMPLE TO ILLUSTRATE THE DIFFERENCE.
AUDITING
"A TEST SUMMARY REPORT IS PRODUCED TO SUMMARISE THE OUTCOME OF TESTING."
THIS ISN'T A CONTROL BECAUSE IT'S NOT CLEAR IF ANYONE **DOES ANYTHING** WITH THE REPORT OR IF IT JUST GETS PUT TO ONE SIDE AND FORGOTTEN.
DANGER
THE EXISTENCE OF THE TEST SUMMARY REPORT DOESN'T DO ANYTHING TO MITIGATE A RISK AND USING THE PASSIVE VOICE MAKES IT EVEN LESS ROBUST.


AUDITING
MMARY REPORT
"THE PROJECT SPONSOR REVIEWS THE TEST SUMMARY DOCUMENT TO ENSURE THAT THE OUTCOME OF TESTING IS CLEAR, AND ANY RESIDUAL RISKS ARE UNDERSTOOD."
THIS CLEARLY DESCRIBES A CHECK - A SPECIFIC PERSON IS ACTUALLY **DOING SOMETHING** WITH THE REPORT AND WITH A **DEFINITE PURPOSE:** WE NOW KNOW WHAT THE CHECK IS TRYING TO ACHIEVE.
27th
NEVER
WHAT IS STILL MISSING THOUGH IS SOMETHING TO SHOW THAT IT REALLY CHECKS THE PROCESS. IF THE SPONSOR DOES THIS CHECK SIX MONTHS AFTER THE PROJECT GOES LIVE, IT ISN'T REALLY GOING TO MITIGATE ANY RISKS.

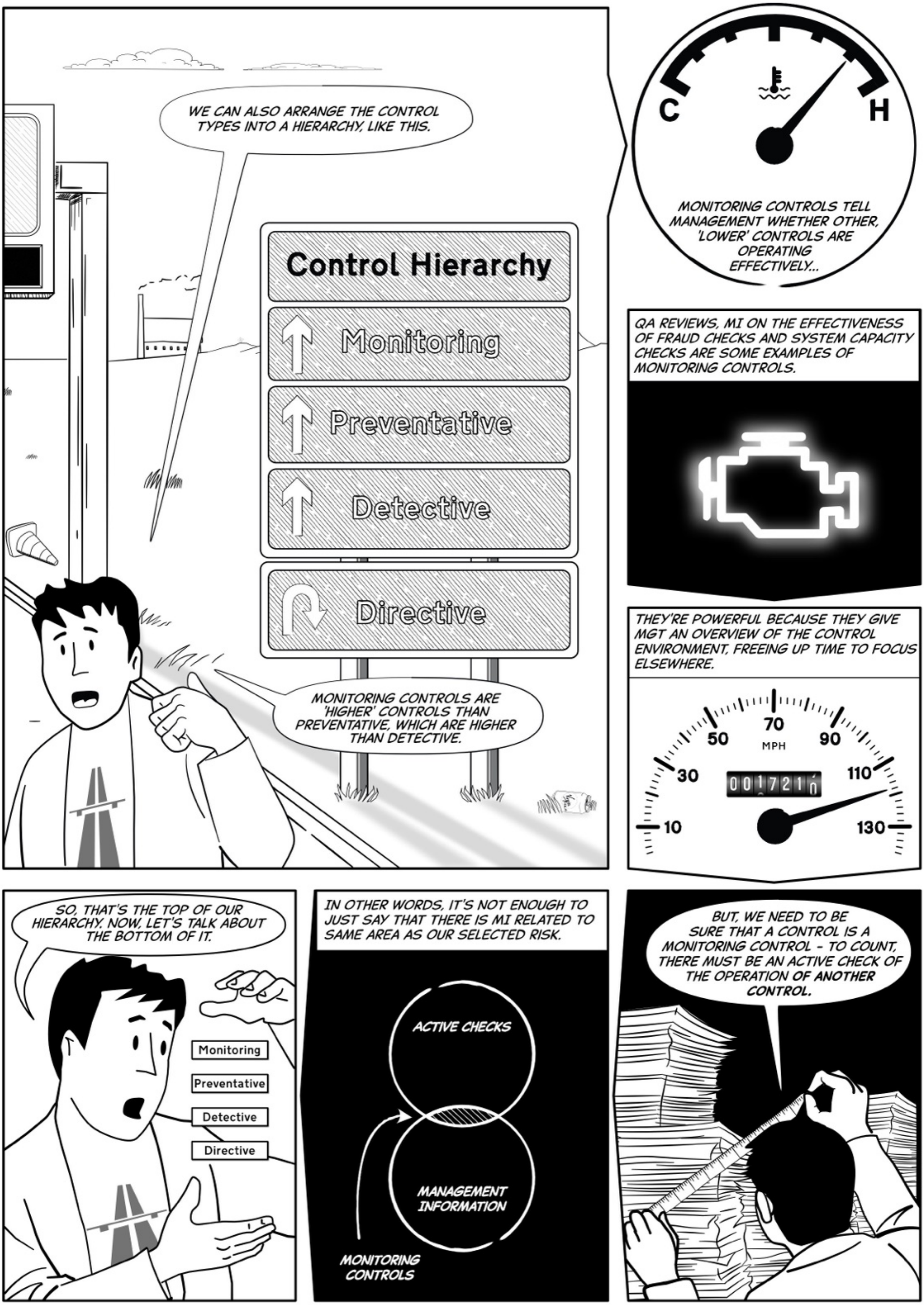

AUDITING
"AS PART OF THE GO/NO-GO DECISION MEETING, THE PROJECT SPONSOR REVIEWS THE TEST SUMMARY DOCUMENT TO ENSURE THAT THE OUTCOME OF TESTING IS CLEAR, AND ANY RESIDUAL RISKS ARE UNDERSTOOD."
ADDING A TIME-BASED ELEMENT OR A TRIGGER TO THE WORDING MAKES IT FEEL MORE ACTIVE AND TIMELY. WE NOW HAVE A ROBUST, WELL-DEFINED CONTROL THAT WE CAN EASILY ASSESS AND TEST.
CHECKED
ONE FINAL THING: TRY TO AVOID CONTROLS THAT TALK ABOUT SOMEONE JUST ATTENDING MEETINGS OR MEETINGS HAPPENING - INSTEAD, FOCUS ON THE CHECK THAT HAPPENS IN THOSE MEETINGS.

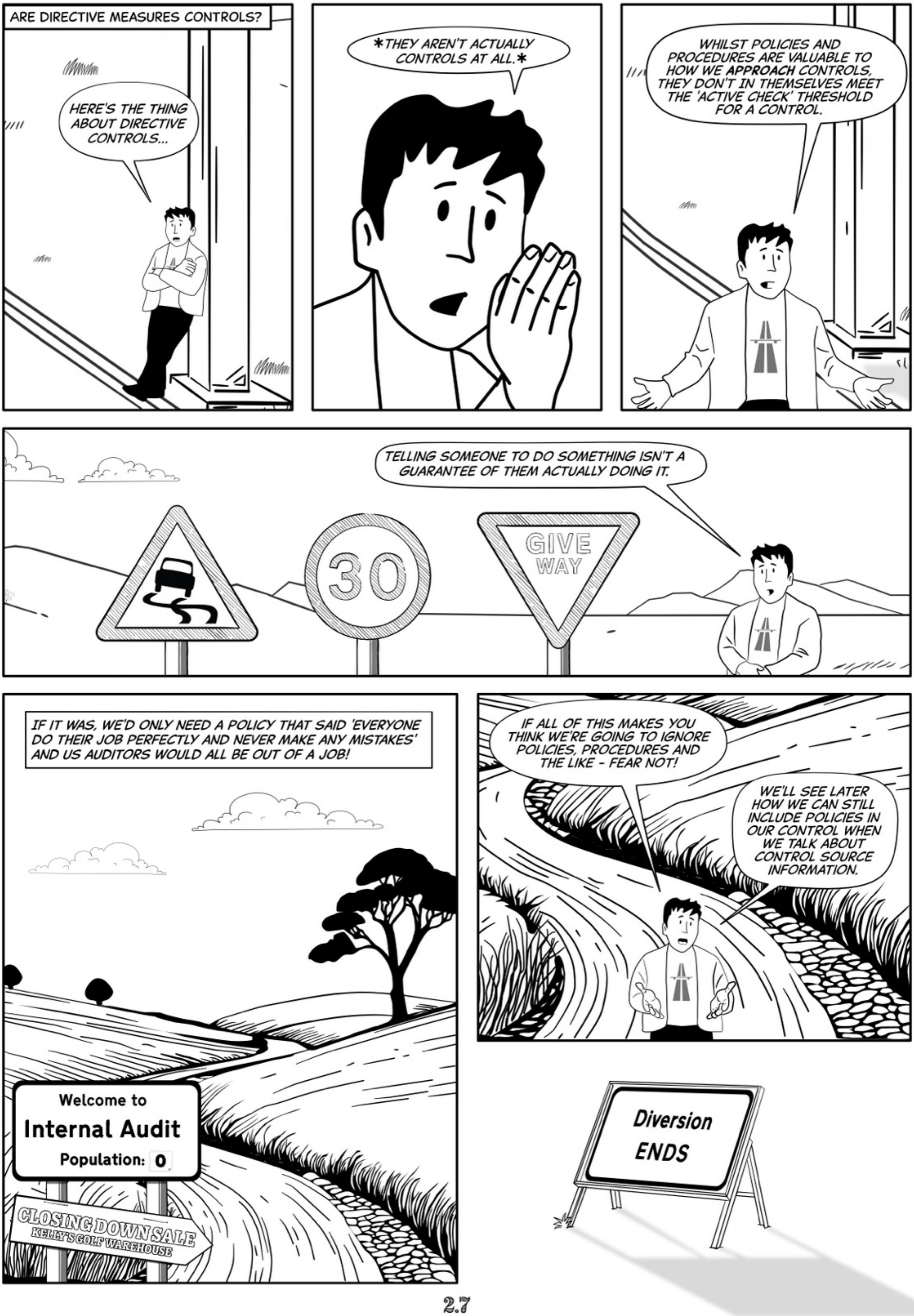

WHAT MAKES A CONTROL 'KEY'?
SO THAT'S WHAT A CONTROL IS...
BUT HOW DO WE KNOW WHICH CONTROLS WE SHOULD INCLUDE IN OUR AUDIT?
MOST AUDIT METHODOLOGIES SAY THAT WE SHOULD FOCUS ON 'KEY' CONTROLS, WHICH IS USUALLY DEFINED AS WHAT ULTIMATELY PREVENTS A PARTICULAR RISK FROM MATERIALISING.
LET'S ADD TWO EXTRA ELEMENTS TO THAT DEFINITION.
TICK
SUPPORTING CONTROLS
FIRSTLY...
Key controls are those controls that ultimately mitigate a key risk,
...OR ARE NECESSARY FOR OTHER KEY CONTROLS TO OPERATE EFFECTIVELY.
THIS EXTENSION IS NEEDED BECAUSE MOST KEY CONTROLS WILL BE RELIANT ON OTHER CONTROLS TO FACILITATE OR SUPPORT THEIR OPERATION.
HERE'S AN EXAMPLE FROM A RECENT AUDIT:
"EVERY MONTH, THE HEAD OF FRAUD REVIEWS AND CHALLENGES KEY FRAUD PERFORMANCE METRIC USING SUMMARY MI FROM THE FRAUD RULES AND SYSTEMS FORUM/ SERVICE DELIVERY FORUM TO ENSURE THAT FRAUD SYSTEMS. PERFORMANCE IS EFFECTIVE."
THIS CONTROL OBVIOUSLY DEPENDS ON THE MI TO OPERATE. BUT WHAT IF THAT MI IS INCOMPLETE OR INACCURATE?
OR WHAT IF THE DATA FEEDS THAT ARE USED TO CREATE THE MI DON'T CONTAIN ALL OF THE INFORMATION WE'D EXPECT?
IF THE UNDERLYING CONTROLS AREN'T EFFECTIVE, THE WHOLE STACK MAY...
...FALL!
FOR THESE REASONS, WE ALSO CLASS THESE UNDERLYING CONTROLS AS KEY.
IN THE NEXT SECTION, WE'LL SEE HOW RECOGNISING THIS HIERARCHY OF KEY CONTROLS CAN MAKE OUR CONTROL DESCRIPTIONS SIMPLER AND EASIER.

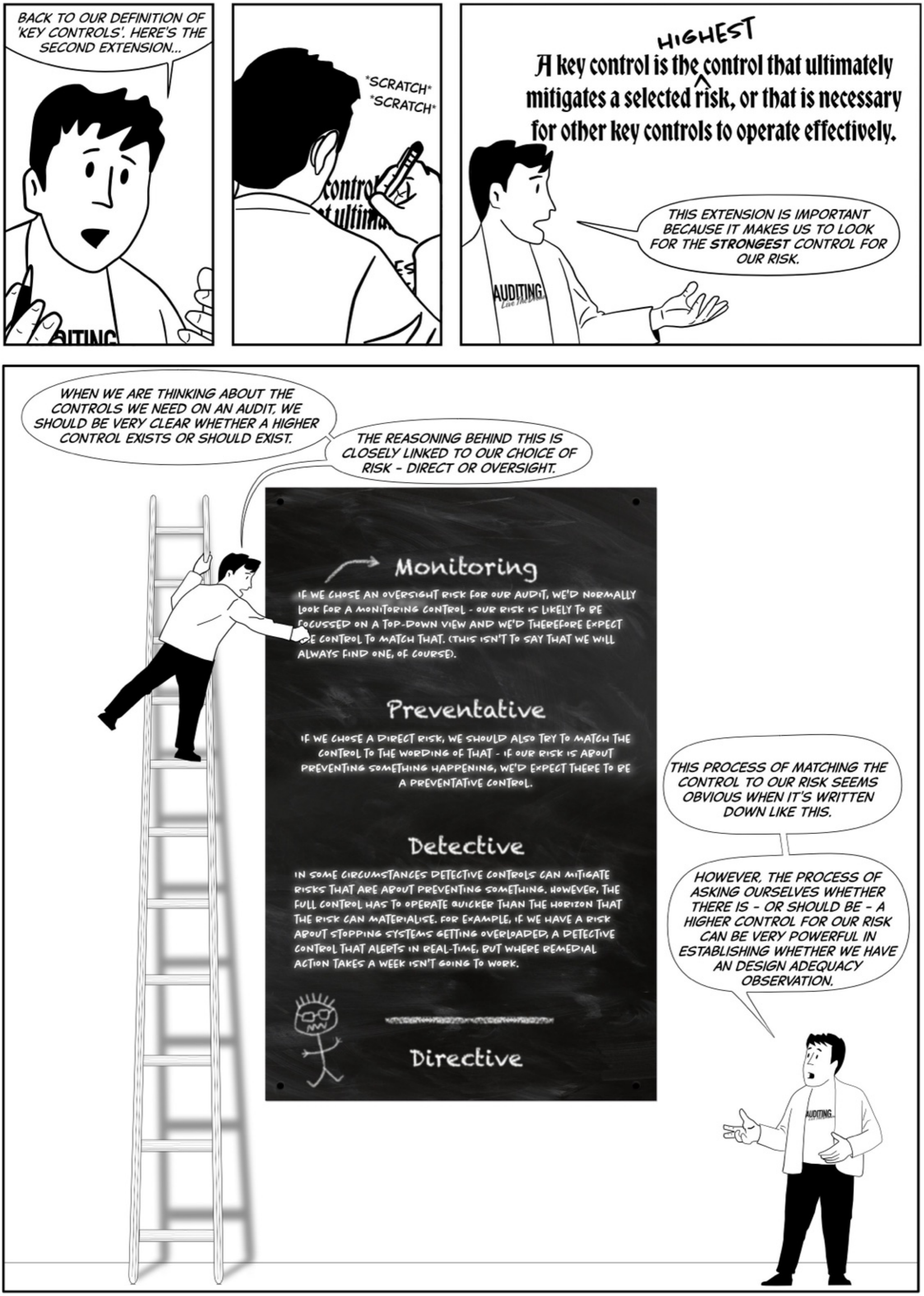

TYPES OF CONTROL
THE SECOND EXTENSION TO OUR DEFINITION OF 'KEY CONTROL' REQUIRES A SMALL DIVERSION..
LET'S TALK ABOUT THE DIFFERENT TYPES OF CONTROL.
GIVE WAY
STOP
30
THERE'S GENERALLY RECOGNISED TO BE FOUR TYPES...


Monitoring (more on these later)
Preventative
Detective
Directive
CONTROLS THAT OPERATE TO PREVENT A RISK OCCURRING IN THE FIRST PLACE
CONTROLS THAT OPERATE ONCE A RISK HAS OCCURRED TO TRY TO REDUCE ITS EFFECTS
MEASURES THAT DEFINE THE APPROACH OR STANDARDS TO BE USED TO MITIGATE A RISK

FOOTNOTE: THERE IS A FIFTH TYPE OF CONTROL THAT IS SOMETIMES SPECIFIED IN AUDIT METHODOLOGIES ETC KNOWN AS CORRECTIVE CONTROLS. HOWEVER, THESE ARE REALLY JUST A SUBSET OF DETECTIVE CONTROLS AND ARE ESSENTIALLY REDUNDANT IF WE HAVE PURPOSEFUL RISKS.

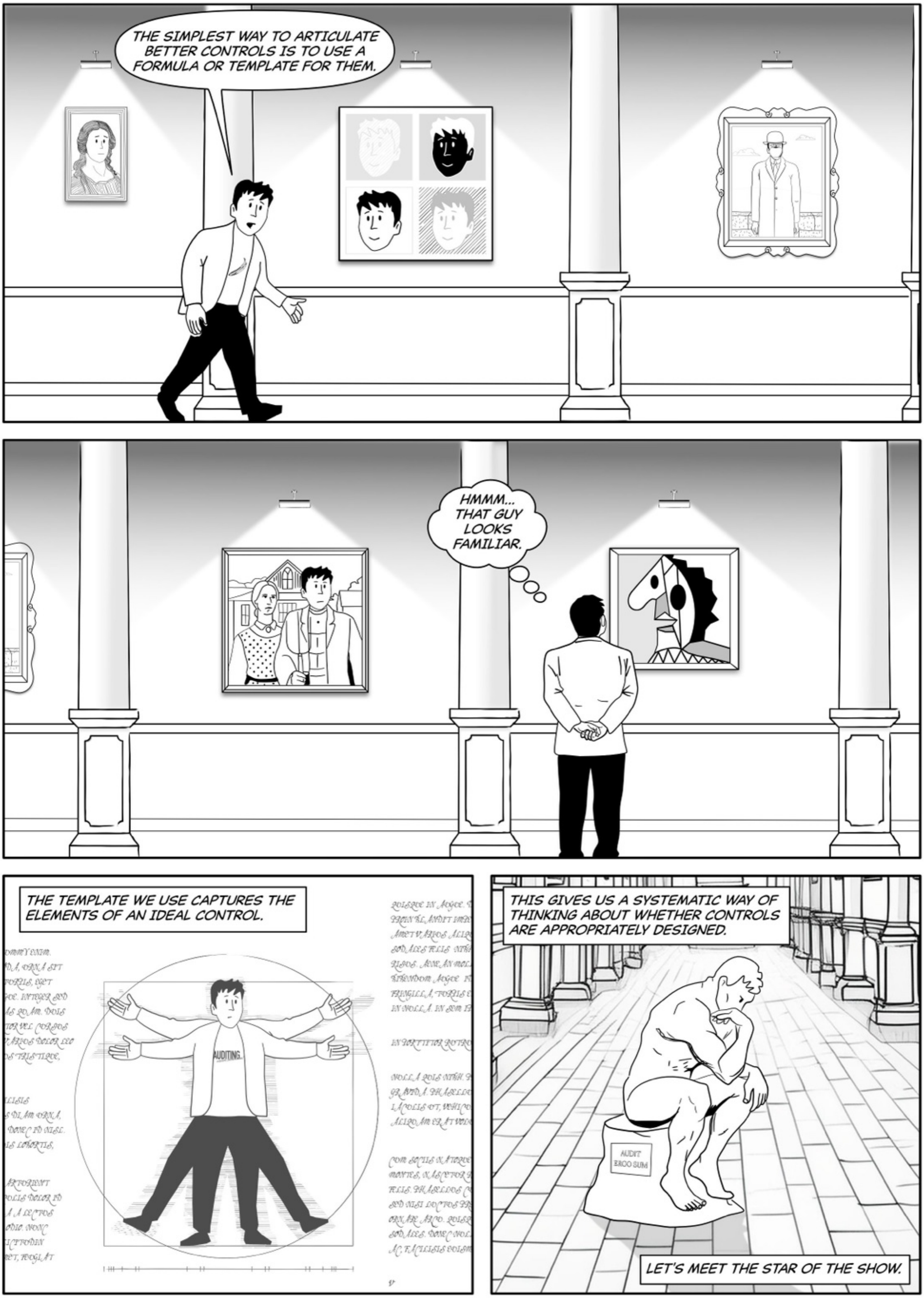

WE CAN ALSO ARRANGE THE CONTROL TYPES INTO A HIERARCHY, LIKE THIS.
Control Hierarchy
Monitoring
Preventative
Detective
Directive
MONITORING CONTROLS ARE 'HIGHER' CONTROLS THAN PREVENTATIVE, WHICH ARE HIGHER THAN DETECTIVE.
C
H
MONITORING CONTROLS TELL MANAGEMENT WHETHER OTHER, 'LOWER' CONTROLS ARE OPERATING EFFECTIVELY...
QA REVIEWS, MI ON THE EFFECTIVENESS OF FRAUD CHECKS AND SYSTEM CAPACITY CHECKS ARE SOME EXAMPLES OF MONITORING CONTROLS.
THEY'RE POWERFUL BECAUSE THEY GIVE MGT AN OVERVIEW OF THE CONTROL ENVIRONMENT, FREEING UP TIME TO FOCUS ELSEWHERE.
10
30
50
70
MPH
90
110
130
0017210
SO, THAT'S THE TOP OF OUR HIERARCHY. NOW, LET'S TALK ABOUT THE BOTTOM OF IT.
Monitoring
Preventative
Detective
Directive
IN OTHER WORDS, IT'S NOT ENOUGH TO JUST SAY THAT THERE IS MI RELATED TO SAME AREA AS OUR SELECTED RISK.
ACTIVE CHECKS
MANAGEMENT INFORMATION
MONITORING CONTROLS
BUT, WE NEED TO BE SURE THAT A CONTROL IS A MONITORING CONTROL - TO COUNT, THERE MUST BE AN ACTIVE CHECK OF THE OPERATION OF ANOTHER CONTROL.

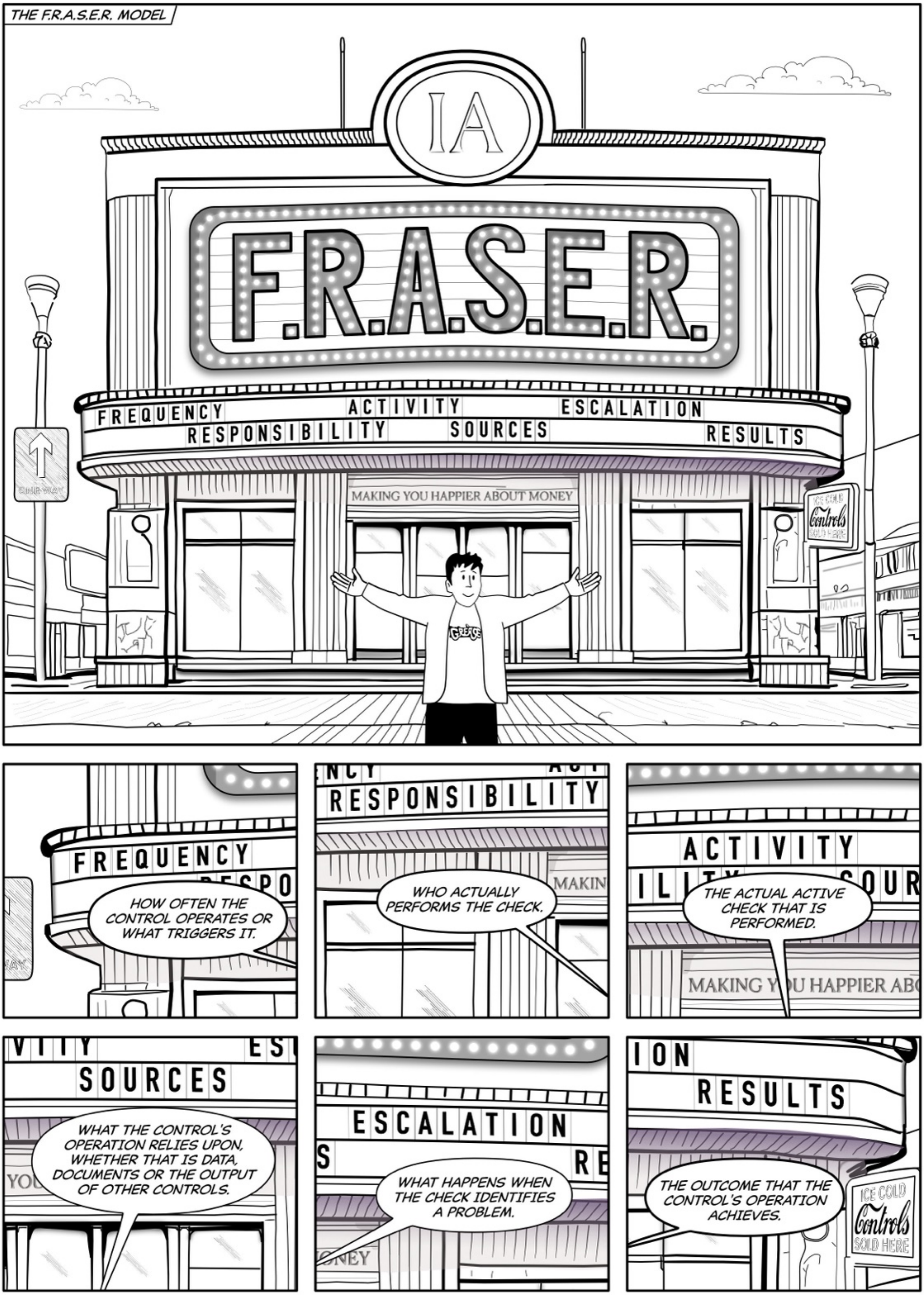

ARE DIRECTIVE MEASURES CONTROLS?
HERE'S THE THING ABOUT DIRECTIVE CONTROLS...
THEY AREN'T ACTUALLY CONTROLS AT ALL.
WHILST POLICIES AND PROCEDURES ARE VALUABLE TO HOW WE **APPROACH** CONTROLS, THEY DON'T IN THEMSELVES MEET THE 'ACTIVE CHECK' THRESHOLD FOR A CONTROL.
TELLING SOMEONE TO DO SOMETHING ISN'T A GUARANTEE OF THEM ACTUALLY DOING IT.
30
GIVE WAY
IF IT WAS, WE'D ONLY NEED A POLICY THAT SAID 'EVERYONE DO THEIR JOB PERFECTLY AND NEVER MAKE ANY MISTAKES' AND US AUDITORS WOULD ALL BE OUT OF A JOB!
Welcome to Internal Audit Population: 0
CLOSING DOWN SALE KELLY'S GOLF WAREHOUSE
IF ALL OF THIS MAKES YOU THINK WE'RE GOING TO IGNORE POLICIES, PROCEDURES AND THE LIKE - FEAR NOT!
WE'LL SEE LATER HOW WE CAN STILL INCLUDE POLICIES IN OUR CONTROL WHEN WE TALK ABOUT CONTROL SOURCE INFORMATION.
Diversion ENDS

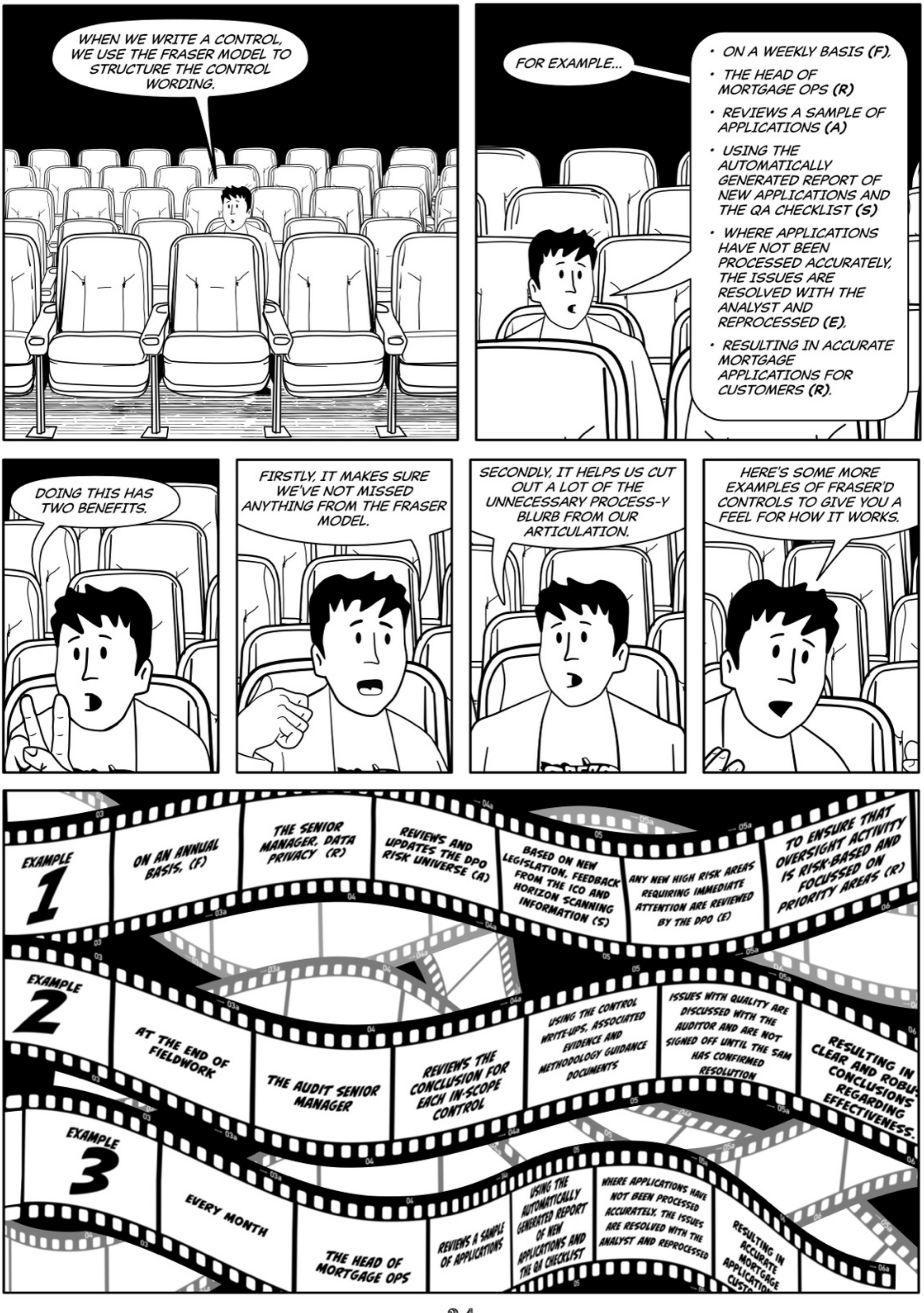

BACK TO OUR DEFINITION OF 'KEY CONTROLS'. HERE'S THE SECOND EXTENSION...
SCRATCH *SCRATCH*
A key control is the HIGHEST control that ultimately mitigates a selected risk, or that is necessary for other key controls to operate effectively.
THIS EXTENSION IS IMPORTANT BECAUSE IT MAKES US TO LOOK FOR THE **STRONGEST** CONTROL FOR OUR RISK.
WHEN WE ARE THINKING ABOUT THE CONTROLS WE NEED ON AN AUDIT, WE SHOULD BE VERY CLEAR WHETHER A HIGHER CONTROL EXISTS OR SHOULD EXIST.
THE REASONING BEHIND THIS IS CLOSELY LINKED TO OUR CHOICE OF RISK - DIRECT OR OVERSIGHT.
Monitoring
IF WE CHOSE AN OVERSIGHT RISK FOR OUR AUDIT, WE'D NORMALLY LOOK FOR A MONITORING CONTROL - OUR RISK IS LIKELY TO BE FOCUSSED ON A TOP-DOWN VIEW AND WE'D THEREFORE EXPECT THE CONTROL TO MATCH THAT. (THIS ISN'T TO SAY THAT WE WILL ALWAYS FIND ONE, OF COURSE).
Preventative
IF WE CHOSE A DIRECT RISK, WE SHOULD ALSO TRY TO MATCH THE CONTROL TO THE WORDING OF THAT - IF OUR RISK IS ABOUT PREVENTING SOMETHING HAPPENING, WE'D EXPECT THERE TO BE A PREVENTATIVE CONTROL.
Detective
IN SOME CIRCUMSTANCES DETECTIVE CONTROLS CAN MITIGATE RISKS THAT ARE ABOUT PREVENTING SOMETHING. HOWEVER, THE FULL CONTROL HAS TO OPERATE QUICKER THAN THE HORIZON THAT THE RISK CAN MATERIALISE. FOR EXAMPLE, IF WE HAVE A RISK ABOUT STOPPING SYSTEMS GETTING OVERLOADED, A DETECTIVE CONTROL THAT ALERTS IN REAL-TIME, BUT WHERE REMEDIAL ACTION TAKES A WEEK ISN'T GOING TO WORK.
Directive
THIS PROCESS OF MATCHING THE CONTROL TO OUR RISK SEEMS OBVIOUS WHEN IT'S WRITTEN DOWN LIKE THIS.
HOWEVER, THE PROCESS OF ASKING OURSELVES WHETHER THERE IS - OR SHOULD BE - A HIGHER CONTROL FOR OUR RISK CAN BE VERY POWERFUL IN ESTABLISHING WHETHER WE HAVE AN DESIGN ADEQUACY OBSERVATION.

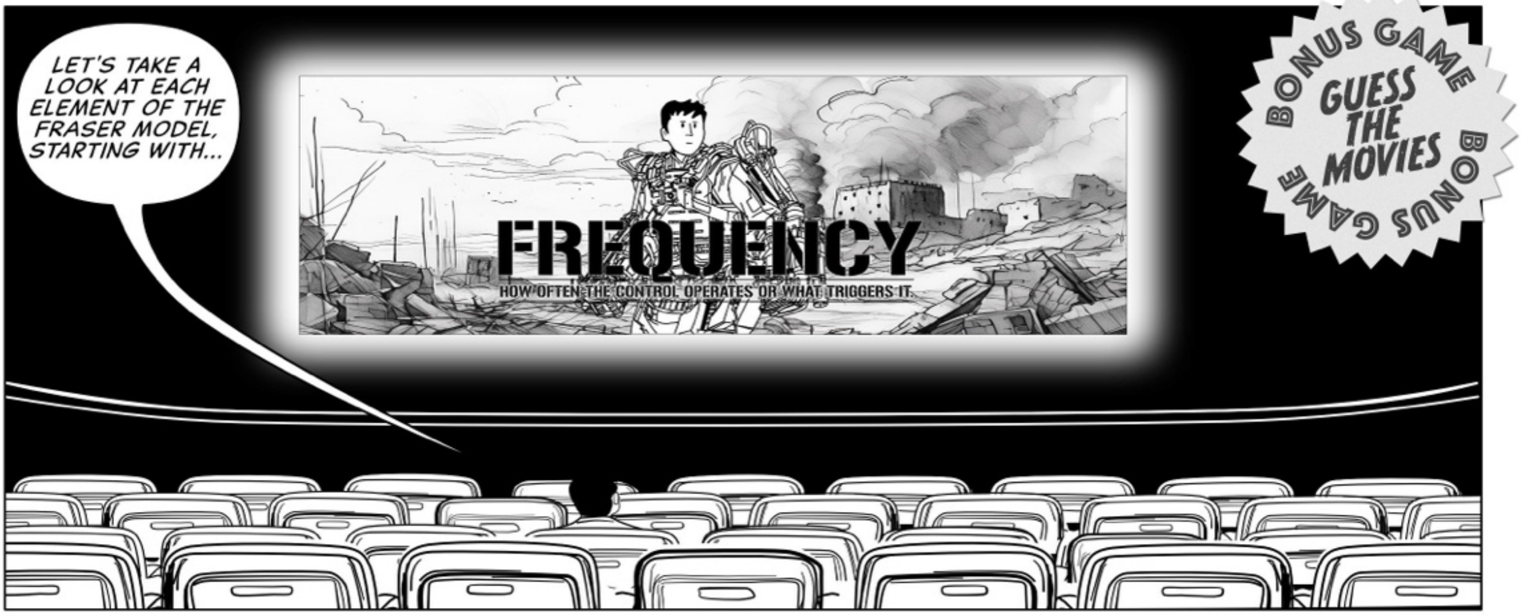
WRITING GREAT CONTROLS

THE PREVIOUS SECTION LOOKED AT WHAT CONTROLS AND HOW THEY RELATE TO THE RISKS WE WRITE AND TO EACH OTHER.
THIS SECTION GETS INTO HOW WE ACTUALLY ARTICULATE CONTROLS TO GIVE AS STRONG AND UNAMBIGUOUS AN OPINION AS WE CAN.
THERE IS AN ART TO THIS, SO WE'LL ALSO GO OVER LOTS OF EXAMPLES TO HELP MAKE THIS REAL.


THE SIMPLEST WAY TO ARTICULATE BETTER CONTROLS IS TO USE A FORMULA OR TEMPLATE FOR THEM.
HMMM... THAT GUY LOOKS FAMILIAR.
THE TEMPLATE WE USE CAPTURES THE ELEMENTS OF AN IDEAL CONTROL.
AUDITING
THIS GIVES US A SYSTEMATIC WAY OF THINKING ABOUT WHETHER CONTROLS ARE APPROPRIATELY DESIGNED.
AUDIT ERGO SUM
LET'S MEET THE STAR OF THE SHOW.


THE F.R.A.S.E.R. MODEL
IA
F.R.A.S.E.R.
FREQUENCY
ACTIVITY
ESCALATION
RESPONSIBILITY
SOURCES
RESULTS
ONE WAY
MAKING YOU HAPPIER ABOUT MONEY
ICE COLD Controls SOLD HERE
GREASE
FREQUENCY
HOW OFTEN THE CONTROL OPERATES OR WHAT TRIGGERS IT.
RESPONSIBILITY
WHO ACTUALLY PERFORMS THE CHECK.
ACTIVITY
THE ACTUAL ACTIVE CHECK THAT IS PERFORMED.
SOURCES
WHAT THE CONTROL'S OPERATION RELIES UPON, WHETHER THAT IS DATA, DOCUMENTS OR THE OUTPUT OF OTHER CONTROLS.
ESCALATION
WHAT HAPPENS WHEN THE CHECK IDENTIFIES A PROBLEM.
RESULTS
THE OUTCOME THAT THE CONTROL'S OPERATION ACHIEVES.
ICE COLD Controls SOLD HERE


WHEN WE WRITE A CONTROL, WE USE THE FRASER MODEL TO STRUCTURE THE CONTROL WORDING.
FOR EXAMPLE...
• ON A WEEKLY BASIS (F),
• THE HEAD OF MORTGAGE OPS (R)
• REVIEWS A SAMPLE OF APPLICATIONS (A)
• USING THE AUTOMATICALLY GENERATED REPORT OF NEW APPLICATIONS AND THE QA CHECKLIST (S)
• WHERE APPLICATIONS HAVE NOT BEEN PROCESSED ACCURATELY, THE ISSUES ARE RESOLVED WITH THE ANALYST AND REPROCESSED (E),
• RESULTING IN ACCURATE MORTGAGE APPLICATIONS FOR CUSTOMERS (R).
DOING THIS HAS TWO BENEFITS.
FIRSTLY, IT MAKES SURE WE'VE NOT MISSED ANYTHING FROM THE FRASER MODEL.
SECONDLY, IT HELPS US CUT OUT A LOT OF THE UNNECESSARY PROCESS-Y BLURB FROM OUR ARTICULATION.
HERE'S SOME MORE EXAMPLES OF FRASER'D CONTROLS TO GIVE YOU A FEEL FOR HOW IT WORKS.
EXAMPLE 1
ON AN ANNUAL BASIS, (F)
THE SENIOR MANAGER, DATA PRIVACY (R)
REVIEWS AND UPDATES THE DPO RISK UNIVERSE (A)
BASED ON NEW LEGISLATION, FEEDBACK FROM THE ICO AND HORIZON SCANNING INFORMATION (S)
ANY NEW HIGH RISK AREAS REQUIRING IMMEDIATE ATTENTION ARE REVIEWED BY THE DPO (E)
TO ENSURE THAT OVERSIGHT ACTIVITY IS RISK-BASED AND FOCUSSED ON PRIORITY AREAS (R)
EXAMPLE 2
AT THE END OF FIELDWORK
THE AUDIT SENIOR MANAGER
REVIEWS THE CONCLUSION FOR EACH IN-SCOPE CONTROL
USING THE CONTROL WRITE-UPS, ASSOCIATED EVIDENCE AND METHODOLOGY GUIDANCE DOCUMENTS
ISSUES WITH QUALITY ARE DISCUSSED WITH THE AUDITOR AND ARE NOT SIGNED OFF UNTIL THE SAM HAS CONFIRMED RESOLUTION
RESULTING IN CLEAR AND ROBU CONCLUSIONS REGARDING EFFECTIVENESS.
EXAMPLE 3
EVERY MONTH
THE HEAD OF MORTGAGE OPS
REVIEWS A SAMPLE OF APPLICATIONS
USING THE AUTOMATICALLY GENERATED REPORT OF NEW APPLICATIONS AND THE QA CHECKLIST
WHERE APPLICATIONS HAVE NOT BEEN PROCESSED ACCURATELY, THE ISSUES ARE RESOLVED WITH THE ANALYST AND REPROCESSED
RESULTING IN ACCURATE MORTGAGE APPLICATION CUSTO

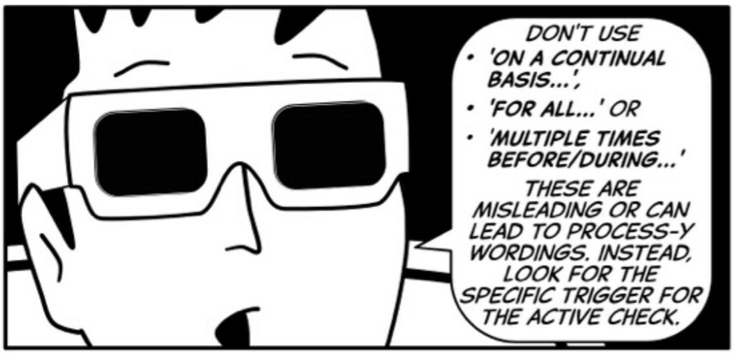

LET'S TAKE A LOOK AT EACH ELEMENT OF THE FRASER MODEL, STARTING WITH...
FREQUENCY
HOW OFTEN THE CONTROL OPERATES OR WHAT TRIGGERS IT.
BONUS GAME GUESS THE MOVIES BONUS GAME

WHILST SOME CONTROLS HAVE A VERY OBVIOUS FREQUENCY - A WEEKLY CHECK, AN ANNUAL REVIEW - BUT SOME ARE TRIGGERED BY SOMETHING: AN ACTION BY A CUSTOMER OR COLLEAGUE, REACHING A PARTICULAR STAGE IN A PROCESS, OR AS THE RESULT OF ANOTHER CONTROL OPERATING.

IT'S IMPORTANT THAT WE ACCURATELY CAPTURE THE FREQUENCY FOR EACH CONTROL FOR TWO REASONS: FIRSTLY, IT GIVES US A WAY OF ASSESSING THE TIMELINESS OF THE CONTROL. SECONDLY, IT IS A KEY PART OF DETERMINING OUR SAMPLE SIZE FOR EFFECTIVENESS TESTING LATER IN THE AUDIT.

DO'S & DON'TS

DO CAREFULLY PICK THE RIGHT KIND OF FREQUENCY STATEMENT **- TIME-BASED OR A TRIGGER.** IF YOU PICK A TRIGGER, BE SURE THAT IT WILL ALWAYS CAUSE THE CONTROL TO OPERATE.


DON'T USE
• 'ON A CONTINUAL BASIS...',
• 'FOR ALL...' OR
• 'MULTIPLE TIMES BEFORE/DURING...'
THESE ARE MISLEADING OR CAN LEAD TO PROCESS-Y WORDINGS. INSTEAD, LOOK FOR THE SPECIFIC TRIGGER FOR THE ACTIVE CHECK.

REMEMBER THAT **THE FREQUENCY IS HOW OFTEN OR WHEN THE ACTIVE CHECK YOU DESCRIBE IN THE ACTIVITY SECTION OF THE CONTROL HAPPENS** - DON'T CONFUSE THIS WITH THE FREQUENCY OF BROADER PROCESSES OR OTHER, SUPPORTING CONTROLS.

EXAMPLES

✓ "ON A WEEKLY BASIS..."

✓ "ONCE A YEAR..."

✓ "WHEN A CUSTOMER SUBMITS A COMPLAINT VIA THE APP..."

✓ "AS PART OF THE GO/NO-GO DECISION MEETING..."

✓ "PRIOR TO APPROVAL OF THE MORTGAGE APPLICATION..."

✖ **"ON A CONTINUAL BASIS..."**
OFTEN USED FOR CONTROLS WHERE SOMEONE IS MONITORING SOMETHING AS PART OF THEIR JOB OR WHERE AN AUTOMATIC ALERT GETS RAISED. HOWEVER, IT ONLY REALLY WORKS FOR CERTAIN TYPES OF FULLY AUTOMATED CONTROLS AND THE ACTUAL CONTROL IS USUALLY THE **RESPONSE** TO THE TRIGGER TO THE ALERT. AS SUCH, IT IS USUALLY BE BETTER TO USE A TRIGGER INSTEAD, SUCH AS "WHEN AN ALERT IS RAISED BY THE SYSTEM..."

✖ **"ON AN AD HOC BASIS..."**
AGAIN, THIS WOULD BE BETTER ARTICULATED AS THE TRIGGER FOR THE AD HOC REVIEW SO THAT WE'RE CLEAR ON WHAT THRESHOLD CAUSES THE REVIEW.

✖ **"FOR ALL PROJECTS..."** OR **"FOR ALL APPLICATIONS..."**
USUALLY USED WHEN WE'RE TRYING TO ARTICULATE A MANDATORY STEP IN A PROCESS. HOWEVER, IT DOESN'T REALLY NAIL DOWN **WHEN** THE CONTROL OPERATES AND ISN'T THEREFORE FOCUSSED ENOUGH.

✖ **"MULTIPLE TIMES BEFORE GO-LIVE..."** OR **"AT EACH MEETING..."**
THESE ARE WELL-INTENDED FUZZYING OF THE FREQUENCY - WHERE THERE ARE MULTIPLE ITERATIONS OF REVIEW. HOWEVER, THESE ARE REALLY DESCRIBING A PROCESS AND ALSO MAKE THINGS MUCH HARDER TO TEST (BECAUSE YOU END UP HAVING TO TEST EVERY INSTANCE OF THE MEETING). INSTEAD, YOU SHOULD FOCUS YOUR FREQUENCY WORDING ON THE KEY INSTANCE OF THE CONTROL OPERATING, WHICH IS USUALLY THE FINAL ONE BEFORE THE DECISION POINT. THIS HELPS REMOVE THE AMBIGUITY ABOUT WHETHER THE CONTROL ACTUALLY ACHIEVES ITS OBJECTIVE OR NOT (SEE THE 'RESULTS' SECTION LATER FOR MORE ON THIS).

Responsibility
WHO ACTUALLY PERFORMS THE CHECK.
'RESPONSIBILITY' IS ABOUT CLEARLY DEFINING WHO ACTUALLY PERFORMS THE CONTROL...
IDENTIFYING THE RESPONSIBLE PERSON, PEOPLE OR SYSTEM (FOR AUTOMATED CHECKS) IS A PRE-REQUISITE FOR IT BEING ACTIVE: IF WE CAN'T WHO IS DOING THE CHECK, WE CAN'T SAY IT IS ACTUALLY HAPPENING.

DO'S AND DON'TS

- ✓ **DO USE THE ROLE OF THE COLLEAGUE** THAT PERFORMS THE CHECK. IF THE PEOPLE DOING THE CHECK DON'T HAVE A USEFUL JOB TITLE - FOR EXAMPLE, JUST 'MANAGER, OPERATIONS' - IT'S OK TO MAKE SOMETHING UP THAT DESCRIBES THE LEVEL AND NATURE OF THEIR ROLE, SUCH AS 'THE MORTGAGE OPERATIONS ANALYST...' . THIS IS BETTER THAN 'MORTGAGE OPERATIONS CHECKS...' BECAUSE IT IS MORE PRECISE AND AVOIDS ANY POTENTIAL SEGREGATION OF DUTIES QUESTIONS LATER IF THE SAME TEAM RELY ON THE CONTROL.

- ✓ **IF THE CONTROL IS OPERATED BY MULTIPLE PEOPLE, OUR ARTICULATION SHOULD CONCISELY STATE WHO CAN DO IT.** THIS MIGHT BE A SIMPLE EITHER/OR ('THE PROGRAMME SPONSOR OR THE PRODUCT OWNER...') OR IT MIGHT BE COLLEAGUES ON A PRE-DETERMINED LIST ('THE PROGRAMME SPONSOR OF THE DELEGATES APPROVED VIA...').

- ✖ **IF THE CONTROL IS OPERATED BY A COMMITTEE, DON'T LIST THE MEMBERS IN THE CONTROL DESCRIPTION** - IN OUR WALKTHROUGH WRITE-UP, WE CAN CONFIRM WHO THE COMMITTEE MEMBERS ARE (AND THAT THEY ARE THE RIGHT PEOPLE TO BE OPERATING THE CONTROL).

- ✖ **WHERE CONTROLS ARE FULLY AUTOMATED, WE SHOULD NAME THE SYSTEM** THAT DOES THE CHECK (E.G. 'THE BPPM MONITORING TOOL...').

EXAMPLES

- ✓ "THE HEAD OF MORTGAGE OPERATIONS..."
- ✓ "THE SECURITY OPERATIONS ANALYST..."
- ✓ "THE PROJECT CONTROL BOARD MEMBERS..."
- ✓ "A SECOND FRAUD OPERATIONS TEAM MEMBER..." (FOR INSTANCES WHERE THE CONTROL IS A PEER REVIEW WITHIN A TEAM)
- ✓ "THE MORTGAGE APPLICATION WEBFORMS..." (WHERE A CONTROL IS OPERATED BY A SYSTEM)
- ✖ "JIMMY FRANK..." WE SHOULDN'T USE NAMES IN CONTROL DESCRIPTIONS AS IT MAKES IT HARD TO UNDERSTAND, AND MEANS THAT ANY REVIEWER HAS TO KNOW WHO THE NAMED INDIVIDUAL IS TO BE ABLE TO ASSESS WHETHER THEY ARE AN APPROPRIATE PERSON TO OPERATE THE CONTROL.
- ✖ "THE TEAM LEAD AND THE ANALYST..." THIS IS USUALLY USED WHERE A REVIEW HAPPENS BY A MORE SENIOR PERSON. IN THESE CASES, THE ACTIVE CHECK IS BEING PERFORMED BY THE MORE SENIOR PERSON (BECAUSE THEY ARE MAKING ANY DECISIONS REQUIRED), SO WE CAN JUST USE 'THE TEAM LEAD'.

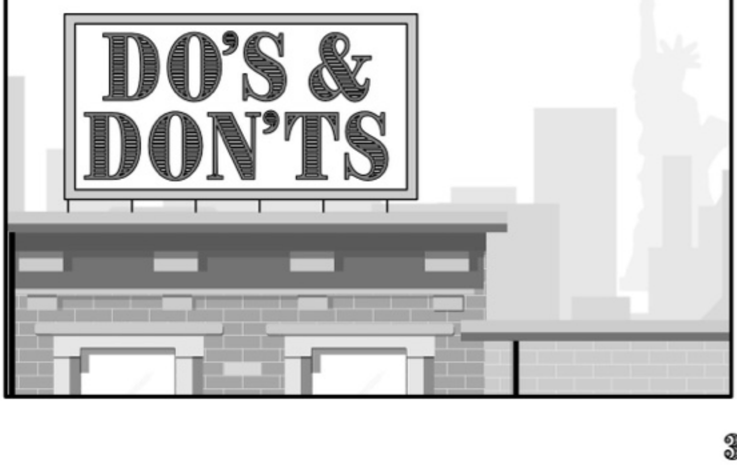
NOW WE'RE IN TO THE HEART OF THE FRASER MODEL.
THE WORDS WE USE FOR THE ACTIVITY MUST DESCRIBE AN ACTIVE CHECK.
IF WE GOT OUR FREQUENCY AND RESPONSIBILITY WORDS RIGHT, THE ACTIVITY SHOULD NATURALLY FOLLOW.
Internal Audit's
ACTIVITY!
The active check that is performed.

√ ***DO*** *REMEMBER THAT AN ALERT OR EXCEPTION BEING RAISED ISN'T IN ITSELF A CHECK: THE ACTIVITY FOR THOSE IS THE* ***RESPONSE*** *TO THE ALERT (THIS IS WHY A LOT OF 'AUTOMATED' CONTROLS ARE ACTUALLY NOT AUTOMATED - THE TRIGGER IS AUTOMATED, BUT THE ACTUAL CONTROL OFTEN REQUIRES A HUMAN FOLLOW-UP).*

✖ ***DON'T*** *INCLUDE LOTS OF MINOR DETAIL ABOUT THE FINER WORKINGS OF THE CHECK IN THE CONTROL WORDING. THESE CAN BE INCLUDED IN OUR WALKTHROUGH WRITE-UP.*

√ ***DO*** *MAKE SURE THE CHECK IS ACTIVE.*

√ ***DO*** *TRY TO STICK TO A SINGLE ACTIVITY IN EACH CONTROL, UNLESS THERE ARE SEVERAL INSTANCES OF THE SAME ACTIVE CHECK THAT FIT TOGETHER. WE'LL SEE IN THE NEXT SECTION HOW WE CAN CHAIN CONTROLS TOGETHER. THE EXCEPTION TO THIS IS WHERE A CHECK VARIES DEPENDING ON AN INPUT (FOR EXAMPLE IF WE DO SOMETHING DIFFERENT FOR PERSONAL AND BUSINESS CUSTOMERS).*



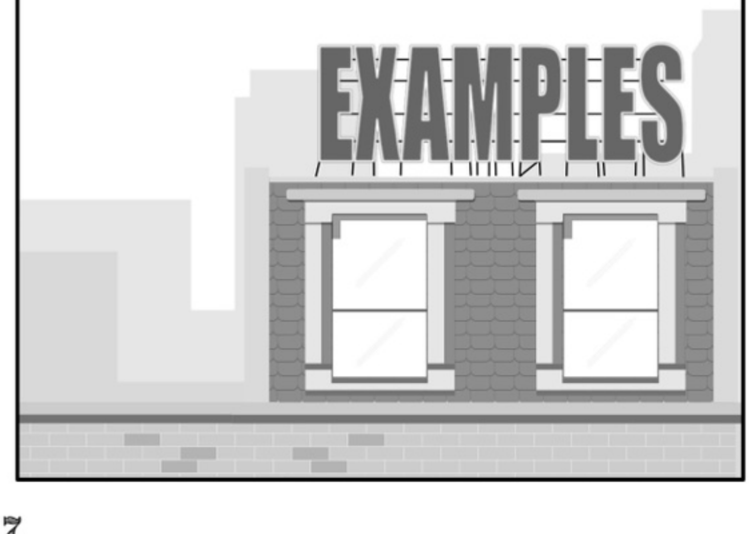
√ *"..REVIEWS THE BPPM ALERT AND FOLLOWS UP WITH THE SYSTEM OWNER AND THE USER THAT TRIGGERED THE ALERT"* ***VS...***

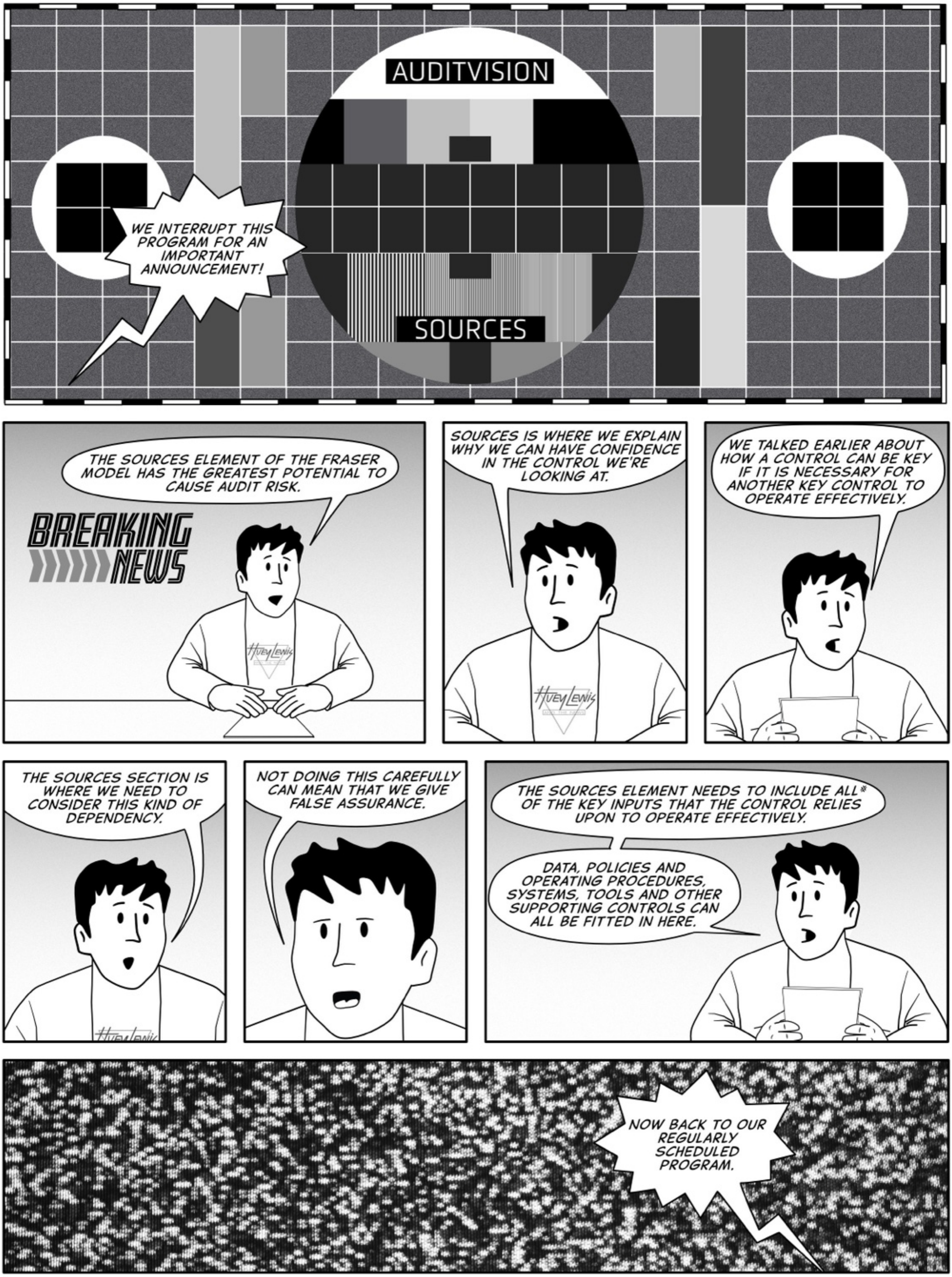
✖ *"...THE BPPM SYSTEM RAISES AN AUTOMATIC ALERT.."*

√ *"...CHECKS THAT THE CUSTOMER'S APPLICATION FORM INCLUDES ALL OF THE REQUIRED DETAILS AND MARKS IT AS COMPLETE..."*

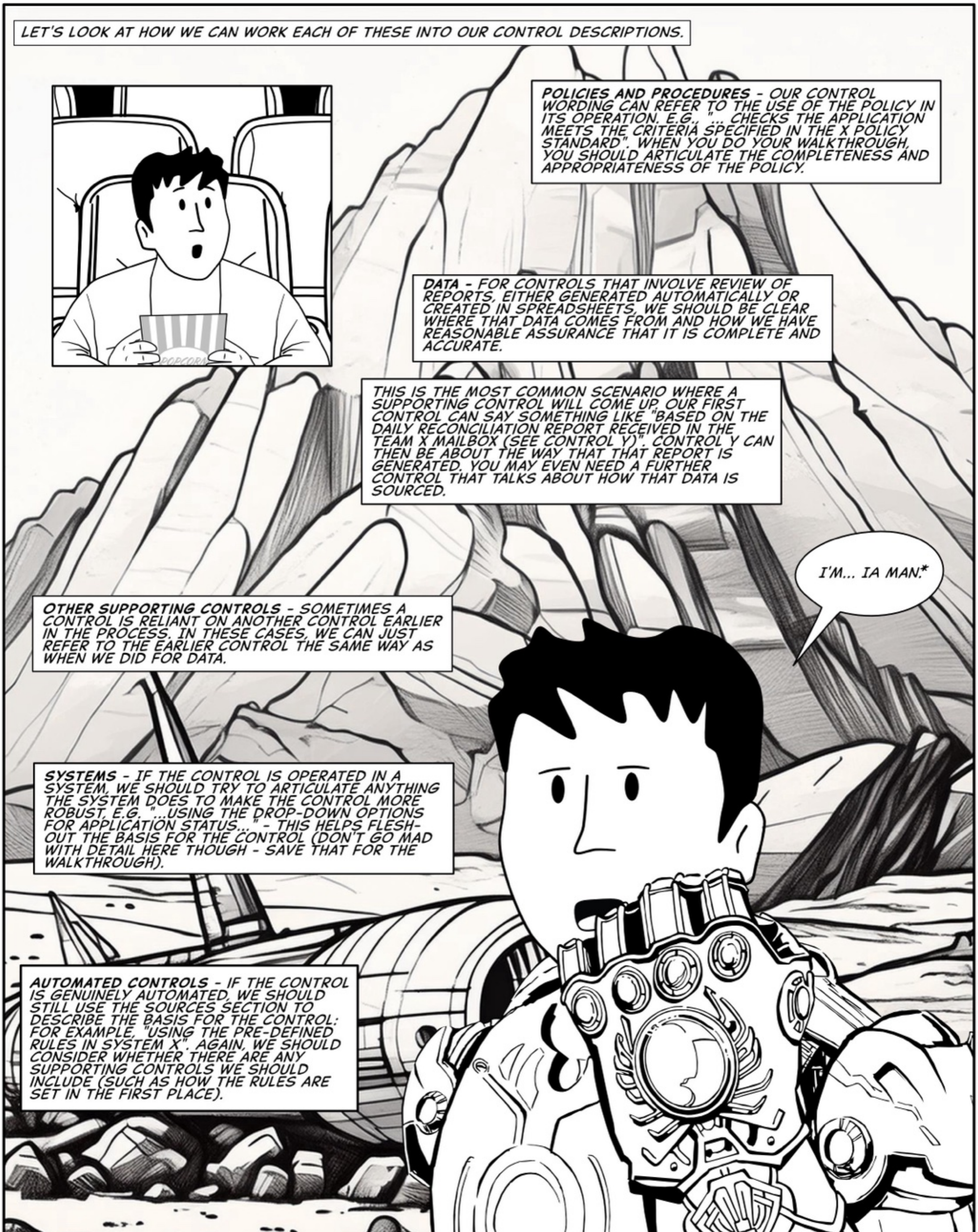
✖ *"...THE SERVICE INTRODUCTION MANAGER CHECKS THAT THE PROJECT HAS COMPLETED THE REQUIRED TEMPLATE TO INCLUDE FUNCTIONAL TESTING, SECURITY TESTING, SUPPORT MODEL DOCUMENTATION, ACCESS RIGHTS REVIEW AND SIGN OFF ETC ETC..."*

✖ *... THE MORTGAGE ANALYST CHECKS THE COMPLETENESS OF THE APPLICATION, MARKS IT COMPLETE AND PASSES THE FORM TO THE TEAM LEAD WHO COMPLETES THE AFFORDABILITY CHECK..."*




AUDITVISION
SOURCES
WE INTERRUPT THIS PROGRAM FOR AN IMPORTANT ANNOUNCEMENT!
BREAKING NEWS
THE SOURCES ELEMENT OF THE FRASER MODEL HAS THE GREATEST POTENTIAL TO CAUSE AUDIT RISK.
SOURCES IS WHERE WE EXPLAIN WHY WE CAN HAVE CONFIDENCE IN THE CONTROL WE'RE LOOKING AT.
WE TALKED EARLIER ABOUT HOW A CONTROL CAN BE KEY IF IT IS NECESSARY FOR ANOTHER KEY CONTROL TO OPERATE EFFECTIVELY.
THE SOURCES SECTION IS WHERE WE NEED TO CONSIDER THIS KIND OF DEPENDENCY.
NOT DOING THIS CAREFULLY CAN MEAN THAT WE GIVE FALSE ASSURANCE.
THE SOURCES ELEMENT NEEDS TO INCLUDE ALL* OF THE KEY INPUTS THAT THE CONTROL RELIES UPON TO OPERATE EFFECTIVELY.
DATA, POLICIES AND OPERATING PROCEDURES, SYSTEMS, TOOLS AND OTHER SUPPORTING CONTROLS CAN ALL BE FITTED IN HERE.
NOW BACK TO OUR REGULARLY SCHEDULED PROGRAM.

* - WE SAY 'ALL' BUT, AS WITH THE ACTIVITY ELEMENT, WE DON'T NEED A LONG EXHAUSTIVE LIST. SUMMARISING FOR CLARITY'S SAKE IS A GOOD IDEA. THE WALKTHROUGH WRITE-UP CAN CAPTURE ANY ADDITIONAL DETAIL.



LET'S LOOK AT HOW WE CAN WORK EACH OF THESE INTO OUR CONTROL DESCRIPTIONS.

POLICIES AND PROCEDURES - OUR CONTROL WORDING CAN REFER TO THE USE OF THE POLICY IN ITS OPERATION. E.G., "... CHECKS THE APPLICATION MEETS THE CRITERIA SPECIFIED IN THE X POLICY STANDARD". WHEN YOU DO YOUR WALKTHROUGH, YOU SHOULD ARTICULATE THE COMPLETENESS AND APPROPRIATENESS OF THE POLICY.

DATA - FOR CONTROLS THAT INVOLVE REVIEW OF REPORTS, EITHER GENERATED AUTOMATICALLY OR CREATED IN SPREADSHEETS, WE SHOULD BE CLEAR WHERE THAT DATA COMES FROM AND HOW WE HAVE REASONABLE ASSURANCE THAT IT IS COMPLETE AND ACCURATE.

THIS IS THE MOST COMMON SCENARIO WHERE A SUPPORTING CONTROL WILL COME UP. OUR FIRST CONTROL CAN SAY SOMETHING LIKE "BASED ON THE DAILY RECONCILIATION REPORT RECEIVED IN THE TEAM X MAILBOX (SEE CONTROL Y)". CONTROL Y CAN THEN BE ABOUT THE WAY THAT THAT REPORT IS GENERATED. YOU MAY EVEN NEED A FURTHER CONTROL THAT TALKS ABOUT HOW THAT DATA IS SOURCED.

OTHER SUPPORTING CONTROLS - SOMETIMES A CONTROL IS RELIANT ON ANOTHER CONTROL EARLIER IN THE PROCESS. IN THESE CASES, WE CAN JUST REFER TO THE EARLIER CONTROL THE SAME WAY AS WHEN WE DID FOR DATA.

SYSTEMS - IF THE CONTROL IS OPERATED IN A SYSTEM, WE SHOULD TRY TO ARTICULATE ANYTHING THE SYSTEM DOES TO MAKE THE CONTROL MORE ROBUST, E.G. "...USING THE DROP-DOWN OPTIONS FOR APPLICATION STATUS..." - THIS HELPS FLESH-OUT THE BASIS FOR THE CONTROL (DON'T GO MAD WITH DETAIL HERE THOUGH - SAVE THAT FOR THE WALKTHROUGH).

AUTOMATED CONTROLS - IF THE CONTROL IS GENUINELY AUTOMATED, WE SHOULD STILL USE THE SOURCES SECTION TO DESCRIBE THE BASIS FOR THE CONTROL: FOR EXAMPLE, "USING THE PRE-DEFINED RULES IN SYSTEM X". AGAIN, WE SHOULD CONSIDER WHETHER THERE ARE ANY SUPPORTING CONTROLS WE SHOULD INCLUDE (SUCH AS HOW THE RULES ARE SET IN THE FIRST PLACE).

* - YES, I KNOW - THIS IS A TERRIBLE JOKE, NOT TO MENTION MEANINGLESS IF YOU HAVEN'T SEEN THE FILM.

DO'S & DON'TS

✓ **DO REALLY THINK ABOUT WHAT THE CONTROL IS RELYING ON FOR ITS EFFECTIVE OPERATION.**

ASK YOURSELF WHAT WE WOULD EXPECT TO SEE FOR THIS CONTROL TO BE ROBUST AND EFFECTIVE.

⊗ **DON'T HOWEVER MAKE THE MISTAKE OF REQUIRING THE SOURCES FOR A CONTROL TO BE DESIGNED SOLELY TO BE EASY TO AUDIT.**

WE SHOULD EXPECT SOURCES TO BE REASONABLY COMPLETE AND TO COVER EVERYTHING THAT IS NECESSARY FOR THE CONTROL TO OPERATE. BUT, REQUIRING THE SOURCES TO COVER EVERY EVENTUALITY AND ANGLE AND FOR EVIDENCE TO BE NEATLY PACKAGED UP JUST FOR US TO AUDIT IS NOT NEEDED.

✓ **DO THINK ABOUT HOW POLICIES, STANDARDS AND PROCEDURES INFORM AND INFLUENCE THE CONTROL'S OPERATION.**

AND THINK ABOUT THE REVERSE SITUATION WHERE A POLICY OR STANDARD DOESN'T INFORM A CONTROL'S DESIGN BUT SHOULD.

✓ **DO USE YOUR TECHNOLOGY AND DATA ANALYTICS AUDIT COLLEAGUES' EXPERTISE TO DIG INTO HOW DATA AND SYSTEMS SUPPORT CONTROL OPERATION.**

THERE ARE VERY FEW PROCESSES IN THE ORGANISATION THAT RELY SOLELY ON PAPER TRAILS.

✓ **DO ADD EXTRA CONTROLS WHERE THEY ARE NEEDED AND BE CLEAR ABOUT WHICH ARE IN THE SCOPE OF YOUR AUDIT.**

TALK TO YOUR SAM OR HEAD OF AUDIT WHERE YOU THINK EXCLUSIONS ARE NEEDED.

✓ **DO MAKE SURE THAT YOU CLEARLY REFERENCE SYSTEMS AND REPORTS.**

IF A REPORT DOESN'T HAVE AN 'OFFICIAL' NAME, TRY TO THINK OF AN UNAMBIGUOUS, DESCRIPTIVE NAME FOR IT AND USE THAT CONSISTENTLY IN YOUR WORKPAPERS.

⊗ **DON'T FORGET THAT AUTOMATED CONTROLS ARE USUALLY BASED ON A SET OF RULES, CONFIGURATION OR SET-UP THAT DETERMINE WHAT THEY ARE TRIGGERED BY**

THESE ARE AS IMPORTANT AS THE AUTOMATED CHECK ITSELF AND YOU SHOULD THINK ABOUT INCLUDING THEM IN YOUR SCOPE.

⊗ **DON'T TRY AND CRAM LOADS OF DETAIL INTO THE SOURCES SECTION AND DON'T TURN IT INTO A LIST.**

IF THERE ARE LOTS OF SOURCES, DESCRIBE THEM AS BRIEFLY AND CONCISELY AS YOU CAN AND ADD THE DETAIL TO YOUR WALKTHROUGH WRITE-UP.

EXAMPLES

✓ **"...USING THE THRESHOLDS SET OUT IN THE CREDIT POLICY STANDARD..."**

MAKES CLEAR THE BASIS OF THE CHECKS AND MEANS OUR WALKTHROUGH CAN ARTICULATE WHETHER THE POLICY IS COMPLETE AND SUFFICIENT.

✓ **"...USING THE DATA RECORDED FOR THE INCIDENT IN SERVICENOW..." OR**

THESE ARE BOTH GOOD ENOUGH AS LONG AS WE'RE CLEAR WHETHER/HOW OUR AUDIT COVERS THE SUPPORTING CONTROLS OVER HOW THE DATA GOT TO THIS POINT.

✓ **... USING THE EXCEPTIONS IDENTIFIED BY THE WEEKLY REVIEW (SEE CONTROL 1)"**

SOME CONTROLS FLOW NATURALLY FROM ONE TO THE OTHER SO CAN JUST BE REFERENCED (JUST WATCH THAT EACH CONTROL GENUINELY IS A CONTROL AND NOT JUST STEPS IN A PROCESS.)

✓ **...THE REPORT IS FILTERED USING THE PRE-DEFINED RULES ENCODED IN THE CDM SYSTEM....**

MAKES CLEAR THE BASIS OF AN AUTOMATED CONTROL AND NAMES THE SYSTEM THAT PERFORMS THE CHECKS.

⊗ **"...USING THE REPORT RECEIVED IN THE TEAM MAILBOX EACH DAY."**

ON ITS OWN, THIS IS NOT CLEAR WHETHER WE'RE JUST TRUSTING THE REPORT TO BE COMPLETE AND CORRECT.

⊗ **"...USING THE THRESHOLDS SET OUT IN THE SECURITY POLICY STANDARD WHICH ARE DEFINED AS *MINIMUM PASSWORD LENGTH OF 8 CHARACTERS, PASSWORD EXPIRY OF BLAH BLAH BLAH...*"**

TOO LONG. THIS KIND OF DETAIL CAN BE ARTICULATED IN YOUR WALKTHROUGH WRITE-UP.

⊗ **"... BASED ON THE POLICIES AND PROCEDURES..."**

WHICH ONES? NEED TO BE SPECIFIC (WITHOUT BEING TOO VERBOSE).

⊗ **"... BASED ON THE INFORMATION RECEIVED FROM THE CUSTOMER..."**

THIS ENDS UP READING LIKE A JUDGEMENT CALL WITHOUT ANY REAL, PRE-DEFINED BASIS. IS THE CUSTOMER'S DATA CHECKED AGAINST ANYTHING? IS IT BEING CHECKED FOR COMPLETENESS, IN WHICH CASE, SAY THAT.

⊗ **"...BASED ON THE TEAM LEAD'S PROFESSIONAL JUDGEMENT..."**

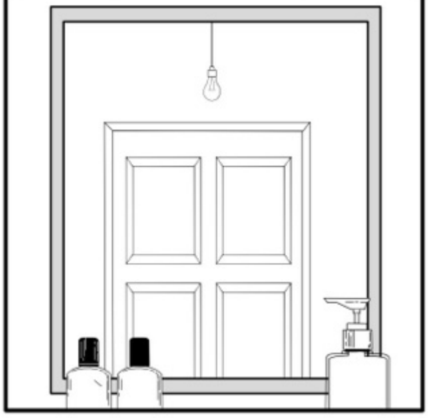
THERE ARE INSTANCES WHERE PROFESSIONAL JUDGEMENT IS KEY TO THE OPERATION OF A CONTROL, BUT WE SHOULD BE WARY OF WRITING CONTROLS WHERE THAT'S ALL THERE IS.

⊗ **... BASED ON THE COMPLETION OF THE INITIAL COMPLETENESS CHECK..."**

WITHOUT A REFERENCE TO ANOTHER CONTROL, THIS READS MORE LIKE A TRIGGER THAN A SOURCE (ITS A PRE-REQUISITE RATHER THAN AN INPUT). BE CLEAR IF THE PRECEDING STEP IS IN SCOPE OR NOT.

THE ACTIVITY ELEMENT OF THE FRASER MODEL COVERS THE ACTIVE CHECK WE'RE INTERESTED IN. BUT, SOMETIMES THAT CHECK FINDS THAT SOMETHING IS WRONG. THE ESCALATION ELEMENT COVERS HOW THIS GETS DEALT WITH.
Escalation
WHAT HAPPENS WHEN THE CHECK IDENTIFIES A PROBLEM
THIS IS KEY SO THAT THE CHECK HAS A PURPOSE: IF THE CHECK IDENTIFIES A PROBLEM, BUT DOESN'T AT LEAST ATTEMPT TO FIX IT, ITS NOT A VERY USEFUL CHECK!

IN SOME CASES, THE ESCALATION IS SIMPLE, E.G., AN ADDITIONAL REVIEW BY A MORE SENIOR COLLEAGUE.

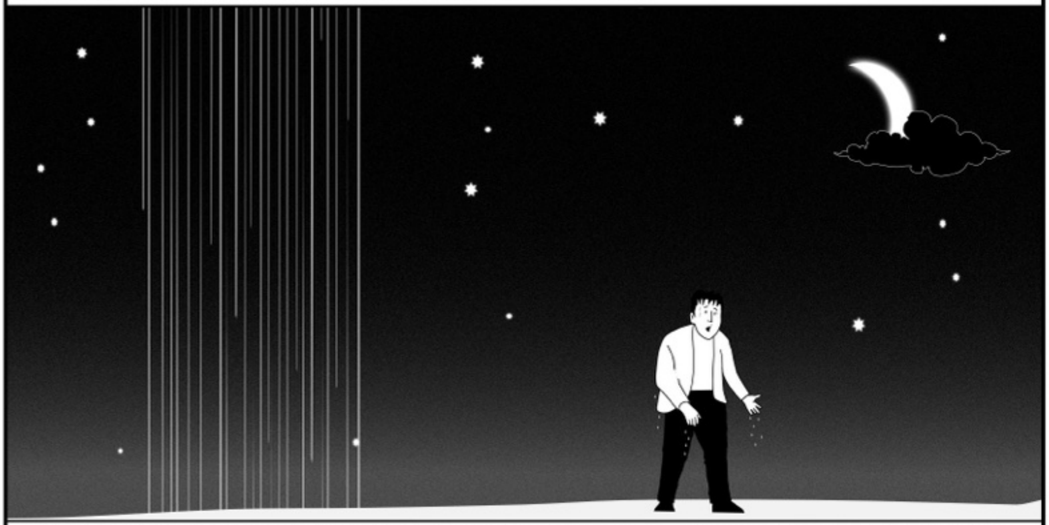


IN OTHER CASES HOWEVER, WE MAY NEED TO BE MORE NUANCED.

SOMETIMES, ITS EASIER TO SPLIT THE ESCALATION INTO A SEPARATE CONTROL ALTOGETHER.

THE VALUE OF THIS ELEMENT IS THAT IT LETS US SHOW THAT THE CONTROL ALWAYS 'TERMINATES'.

NOTE THAT THE ESCALATION ELEMENT IS SEPARATE FROM WHERE THE CONTROL WE'RE INTERESTED IN HAS BRANCHES FOR DIFFERENT SCENARIOS. THE ESCALATION WE'RE TALKING ABOUT HERE IS WHERE THE CHECK IDENTIFIES A PROBLEM...



...IF THERE ARE DIFFERENT PRODUCT TYPES OR ADDITIONAL STEPS WHEN THRESHOLDS ARE MET, THESE SHOULD BE INCLUDED IN THE ACTIVITY SECTION OR TREATED AS SEPARATE CONTROLS, DEPENDING ON HOW COMPLEX THEY ARE.

Do's & Don'ts

✓ DO REALLY THINK ABOUT HOW A PROBLEM WOULD BE DEALT WITH AND WHETHER THE CONTROL WILL BE ABLE TO PROPERLY CONCLUDE.

IF EVERYTHING STALLS WHEN A PROBLEM HAPPENS OR GOES ROUND IN AN INFINITE LOOP, IT MAY NOT BE ROBUST ENOUGH.

✖ DON'T CONFUSE MI DESCRIBING EXCEPTIONS WITH THE ACTIONS REQUIRED TO RESOLVE THEM.

THIS MAY WORK IF THE ISSUE IS RESOURCE AVAILABILITY IN A TEAM, BUT IF YOUR CONTROL IS ABOUT INDIVIDUAL APPLICATIONS OR PAYMENTS, BE CLEAR HOW AGGREGATED REPORTING HELPS WITH THE SPECIFIC EXCEPTIONS.

✖ DON'T JUST SAY THAT THE PROBLEM GOES TO A MORE SENIOR PERSON WITHOUT EXPLAINING WHAT THEY DO.

IF THEY APPROVE AN EXCEPTION OR CAN OVERRIDE SOME RESTRICTION IN A SYSTEM, SAY SO.

✖ DON'T TREAT ESCALATIONS AS AN ENDLESS CYCLE OF UPWARD DELEGATIONS.

IF THE PROBLEM CAN ONLY BE SOLVED BY SOMEONE AT THE TOP OF THE ORGANISATION, SAY SO. BUT...

✖ DON'T INCLUDE LONG CHAINS OF ESCALATION IN YOUR CONTROL WORDING

IF IT REQUIRES THE CEO TO RESOLVE A PROBLEM, DON'T LIST EVERYBODY IN BETWEEN.

✓ DO REMEMBER TO MATCH THE EVIDENCE OF ESCALATION TO THE NATURE OF THE ACTION REQUIRED.

THE QUESTION WE SHOULD ASK ABOUT SENIOR ESCALATIONS IS 'CAN WE REASONABLY SAY THAT THE DECISION-MAKER WAS ABLE TO MAKE THE RIGHT CALL BASED ON THE INFORMATION THEY HAD'? (AND, AS WE TALKED ABOUT IN THE ACTIVITY SECTION, IF THE DECISION IS SOLELY BASED ON JUDGEMENT, ARE WE COMFORTABLE THAT THAT IS OK?)

Examples

✓ "WHERE DETAILS ARE FOUND TO BE INCOMPLETE, THE ANALYST CONTACTS THE CUSTOMER TO OBTAIN THE DETAILS. THE APPLICATION IS PLACED ON HOLD IN SYSTEM X UNTIL THE INFORMATION IS RECEIVED. IF IT IS NOT RECEIVED WITHIN 30 DAYS, THE APPLICATION IS MARKED AS CANCELLED."

YES, THIS IS A MADE-UP EXAMPLE AND YOU MAY BE SCREAMING THAT WE COULDN'T DO THIS, BUT IT ILLUSTRATES THE IDEA OF THE CONTROL HAVING A CLEAR END-POINT.

✓ "PAYMENTS THAT ARE NOT AUTOMATICALLY PROCESSED WITHIN 63 SECONDS ARE AUTOMATICALLY ADDED TO THE EXCEPTION REPORT PRODUCED EACH DAY FOR PAYMENTS OPERATIONS (SEE CONTROL X)."

HERE WE LINK TO ANOTHER IN-SCOPE CONTROL. IF THAT CONTROL ENSURES THAT THE EXCEPTIONS ARE ALL WORKED THROUGH, WE DON'T NEED TO EXPLAIN THAT AGAIN HERE.

✖ "ACCESS ATTESTATIONS THAT AREN'T APPROVED AFTER 30 DAYS ARE ESCALATED TO THE REVIEWER'S PEOPLE LEADER."

THIS IS A VERY FREQUENT SITUATION BUT WHAT WE SHOULD TRY AND MAKE CLEAR IS WHAT HAPPENS THAT ENSURES THAT THE ATTESTATION IS ACTUALLY COMPLETED. DOES THE PEOPLE LEADER HAVE TO DO THE ATTESTATION OR ARE THEY JUST ASKED TO REMIND THE REVIEWER? WHAT HAPPENS IF THEY DON'T?

✖ "PURCHASE ORDERS WITH A VALUE OF MORE THAN £1M ARE ESCALATED TO THE CHIEF EXECUTIVE."

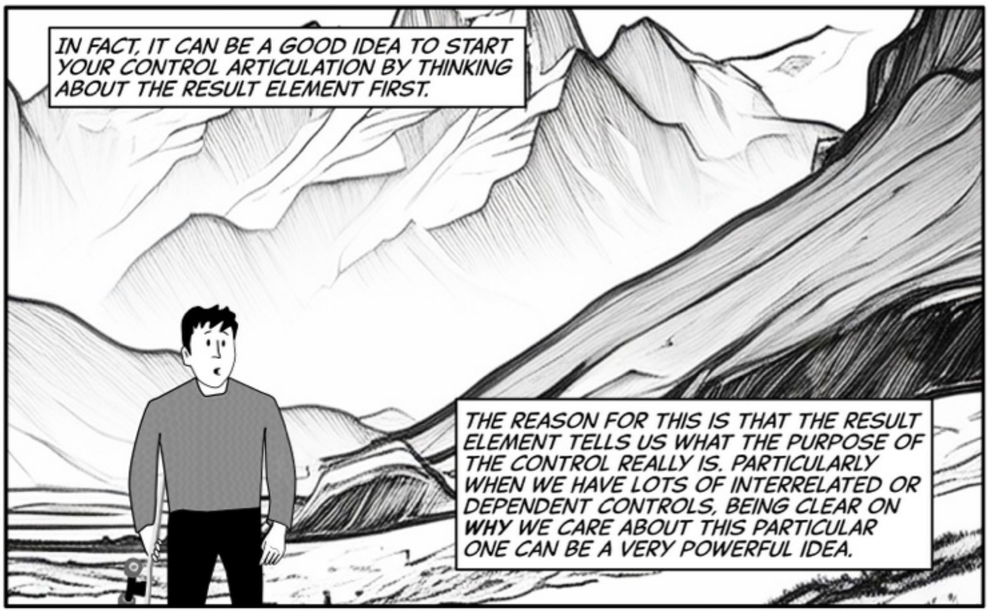
THIS ISN'T REALLY AN ESCALATION. THE PROCESS HAS THRESHOLDS THAT GOVERN WHO APPROVES POS AND OUR ACTIVITY OR SOURCES SECTIONS COULD EASILY ARTICULATE THESE (THE VALUE OF A PAYMENT OR PO IS NOT INHERENTLY A 'PROBLEM').

You Are Now Leaving Seahaven Island!
Are You Sure It's A Good Idea?

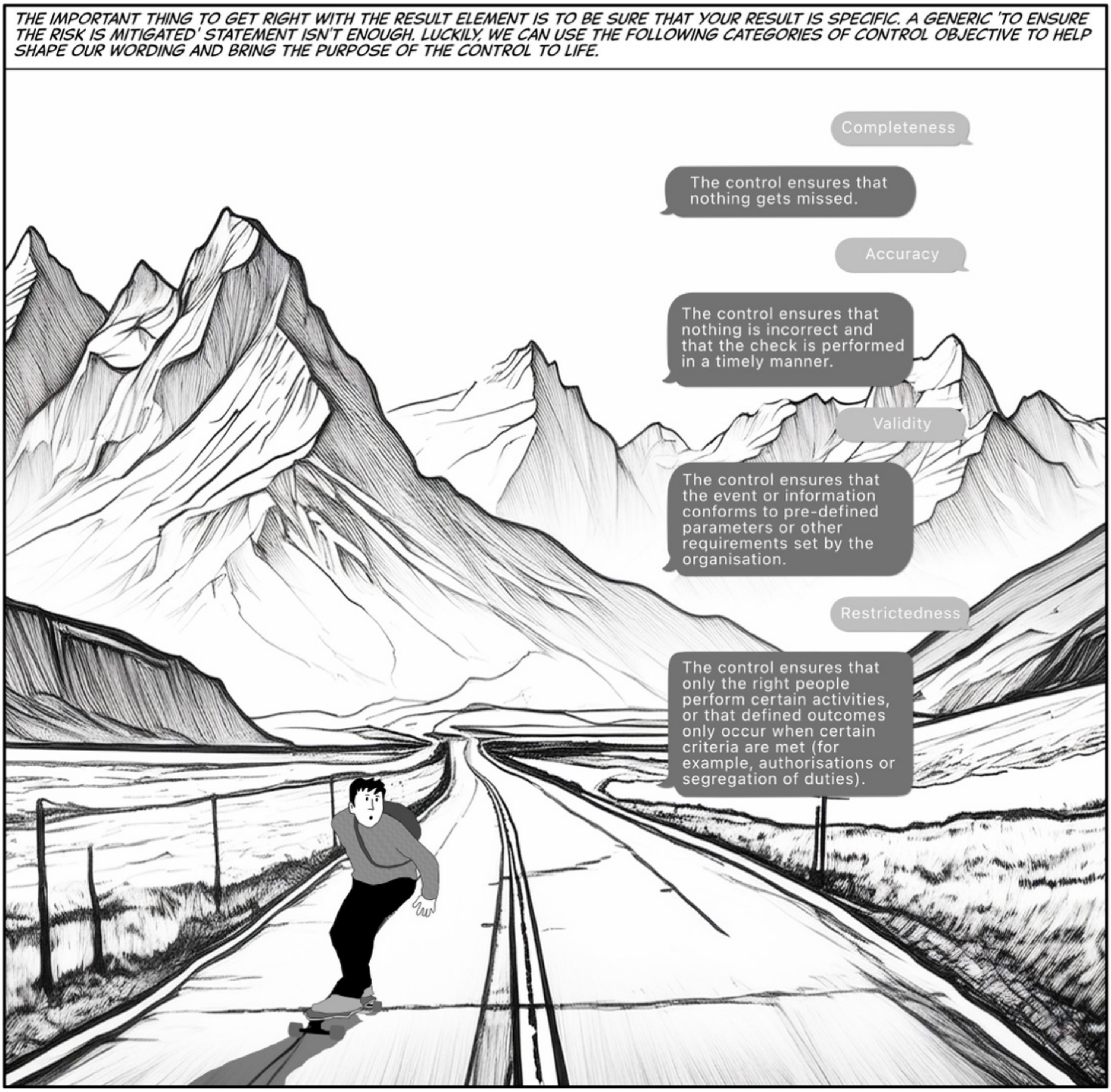
AND FINALLY...

THE RESULT ELEMENT IS SIMPLE TO UNDERSTAND, BUT IS A REALLY USEFUL TOOL FOR US TO USE.
RESULT
RISK & CONTROL BUILDING
FINAL ELEMENT
The outcome that the control's operation achieves.

AUTHOR'S NOTE - THIS SECTION IS BASED ON MY FAVOURITE MOVIE EVER.


IN FACT, IT CAN BE A GOOD IDEA TO START YOUR CONTROL ARTICULATION BY THINKING ABOUT THE RESULT ELEMENT FIRST.
THE REASON FOR THIS IS THAT THE RESULT ELEMENT TELLS US WHAT THE PURPOSE OF THE CONTROL REALLY IS. PARTICULARLY WHEN WE HAVE LOTS OF INTERRELATED OR DEPENDENT CONTROLS, BEING CLEAR ON **WHY** WE CARE ABOUT THIS PARTICULAR ONE CAN BE A VERY POWERFUL IDEA.

IF THIS MADE YOU SHOUT '**CONTROL OBJECTIVE!**', GIVE YOURSELF A GOLD STAR. THAT'S EXACTLY WHAT THIS IS.


THE IMPORTANT THING TO GET RIGHT WITH THE RESULT ELEMENT IS TO BE SURE THAT YOUR RESULT IS SPECIFIC. A GENERIC 'TO ENSURE THE RISK IS MITIGATED' STATEMENT ISN'T ENOUGH. LUCKILY, WE CAN USE THE FOLLOWING CATEGORIES OF CONTROL OBJECTIVE TO HELP SHAPE OUR WORDING AND BRING THE PURPOSE OF THE CONTROL TO LIFE.
Completeness
The control ensures that nothing gets missed.
Accuracy
The control ensures that nothing is incorrect and that the check is performed in a timely manner.
Validity
The control ensures that the event or information conforms to pre-defined parameters or other requirements set by the organisation.
Restrictedness
The control ensures that only the right people perform certain activities, or that defined outcomes only occur when certain criteria are met (for example, authorisations or segregation of duties).

Do's & Don'ts

✓ DO START WITH THE RESULT ELEMENT WHEN YOU'RE WRITING YOUR CONTROLS.

KNOWING WHY THE CONTROL EXISTS CAN GIVE YOU A LOT OF CLUES AS TO WHAT THE ACTIVE CHECK IS.

✓ DO MATCH THE RESULT TO THE CONTROL'S ACTIVITY.

DON'T MAKE THE RESULT TOO BROAD RELATIVE TO THE ACTIVITY - SUPPORTING CONTROLS IN PARTICULAR WILL OFTEN HAVE QUITE NARROW RESULT STATEMENTS.

✓ DO TRY AND USE THE FOUR CONTROL OBJECTIVES CATEGORIES TO MAKE SURE THAT YOUR RESULT IS ACTUALLY ACHIEVING SOMETHING.

COMPLETENESS, ACCURACY, VALIDITY AND RESTRICTEDNESS ARE POWERFUL ANCHORS FOR YOUR RESULT. IF YOU CAN'T RELATE THE CONTROL TO ONE OF THESE, ASK YOURSELF WHETHER THIS IS REALLY A KEY CONTROL.

✖ DON'T OVER-WRITE THE RESULT SECTION.

IT'S BETTER TO HAVE A SIMPLE, CLEARLY ARTICULATED RESULT THAN TO TRY AND COVER LOTS OF ANGLES. IF YOU REALLY THINK THE CONTROL COVERS MULTIPLE CONTROL OBJECTIVE TYPES, CONSIDER SPLITTING IT INTO SEPARATE CONTROLS THAT EACH COVER ONE (THIS WILL MAKE ASSESSING AND TESTING EVERYTHING SIMPLER TOO AS YOU'LL NOT NEED TO WRITE A CONCLUSION THAT COVERS MULTIPLE ANGLES).

✓ DON'T JUST REPEAT THE ACTIVITY IN YOUR RESULT ELEMENT.

THE ACTIVE CHECK IS NEVER AN END IN ITSELF.

✖ DON'T BE AFRAID TO CHALLENGE WHETHER A CONTROL IS REALLY NEEDED IF THE RESULT ELEMENT DOESN'T SOUND CONVINCING.

THERE ARE MANY ELEMENTS TO A PROCESS THAT WE COULD LOOK AT, BUT IF A PART OF IT ISN'T REALLY KEY, WE SHOULD EXCLUDE IT.

Examples

✓ "...TO ENSURE THAT THERE IS A COMPLETE LIST OF CHANGES THAT WILL BE SUBJECT TO THE SERVICE INTRODUCTION PROCESS."

CONCISE AND LIMITED TO THE SCOPE OF THE ACTIVITY.

✖ "...TO MITIGATE THE RISK OF FRAUD CONTROLS NOT OPERATING."

THIS DOESN'T TELL US WHY THE CONTROL EXISTS, BUT IS INSTEAD A KIND OF CIRCULAR REFERENCE.

✖ "......TO ENSURE THAT MORTGAGE APPLICATIONS ARE CHECKED BY A SENIOR MANAGER."

THIS IS JUST A REPEAT OF THE ACTIVITY AND, AGAIN, DOESN'T TELL US ***WHY*** *THE CONTROL HAS BEEN PUT IN PLACE.*

✓ "...TO ENSURE THAT MORTGAGE APPLICATIONS THAT ARE OUTSIDE RISK APPETITE ARE SUBJECT TO APPROPRIATE SENIOR REVIEW ."

THIS IS A MODIFIED VERSION OF THE PREVIOUS ONE, BUT FOCUSES ON WHY THE CONTROL EXISTS.

✖ "... TO ENSURE THAT FRAUD CHECKS ARE COMPLETED FOR ALL PAYMENTS."

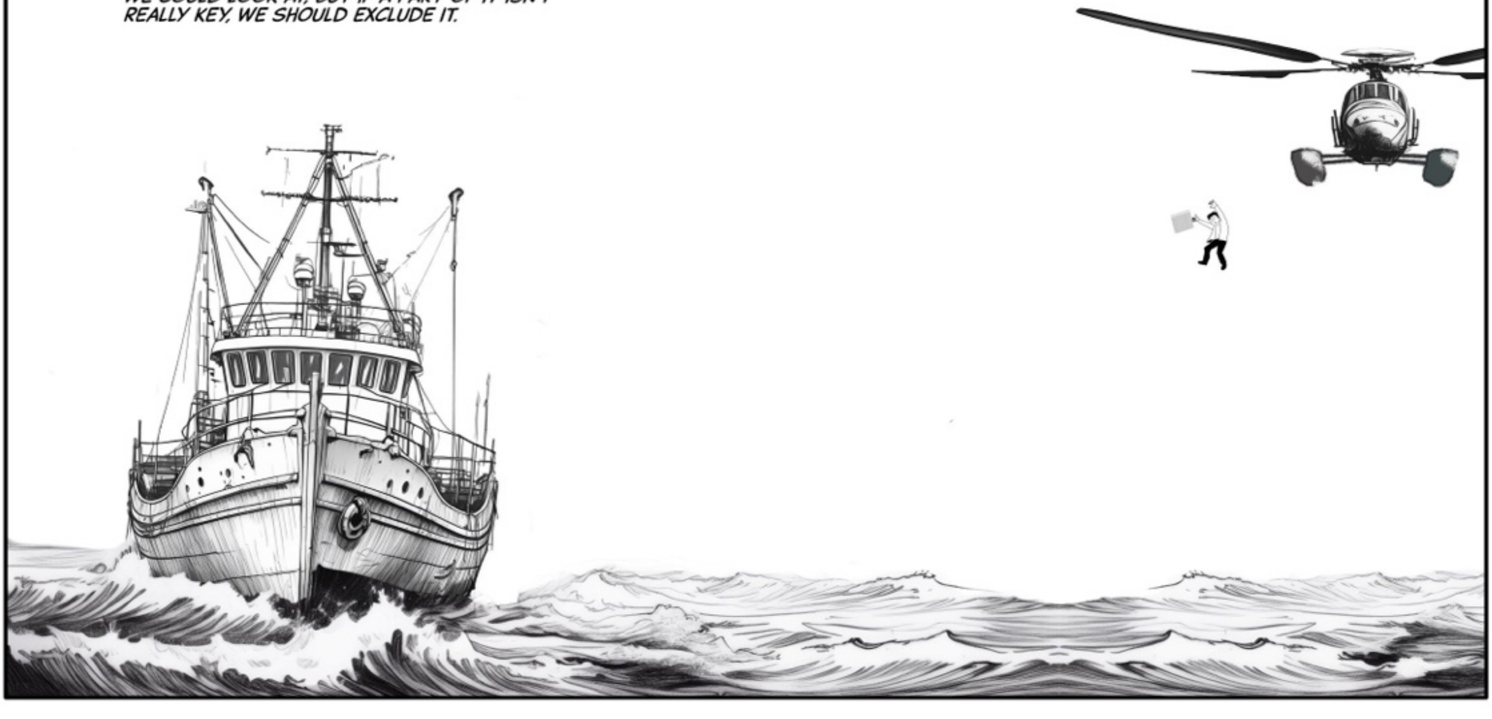
THIS IS FINE, AS LONG AS IT MATCHES THIS CONTROL'S ACTIVITY. IF THE ACTIVITY IS NARROWER, THE RESULT SHOULD MATCH THAT.

✓ "...TO ENSURE THAT THE MONTHLY TRANSACTIONAL FRAUD MI IS ACCURATE AND COMPLETE."

SOME RESULTS DO COVER MORE THAN ONE CONTROL OBJECTIVE, BUT DON'T TRY TOO HARD TO CRAM LOTS OF OBJECTIVES INTO YOUR RESULT STATEMENTS.

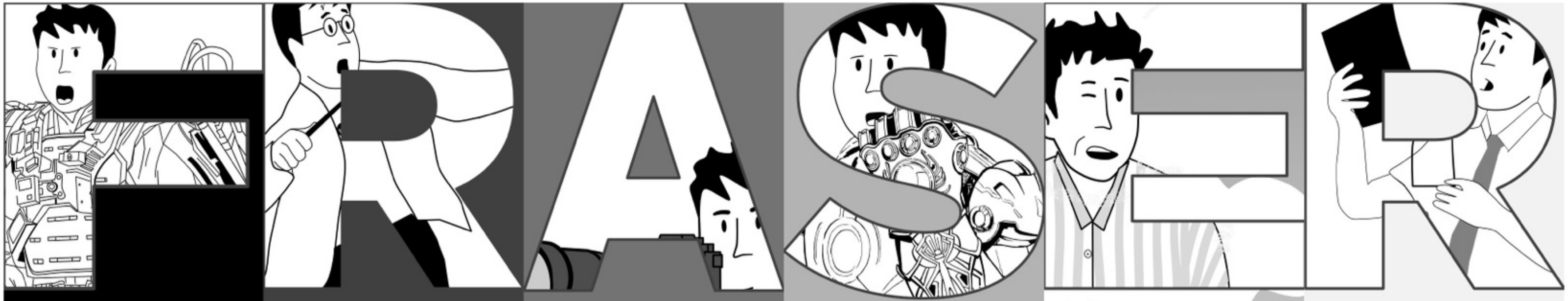
✖ "... TO ENSURE THAT THE DPO RISK UNIVERSE CONTAINS ALL APPLICABLE REGULATORY AND STATUTORY REQUIREMENTS, EMERGING REQUIREMENTS AND INTERNAL ISSUES, WITH EACH RISK ASSESSED AND PRIORITISED SO THAT THE ANNUAL ASSURANCE PLAN IS COMPLETE AND FULLY RESOURCED."

TOO. MANY. WORDS. A LOT OF THIS CAN BE CAPTURED ELSEWHERE AND THIS WORDING IS BOTH TOO VERBOSE AND HARD TO GET YOUR HEAD ROUND.



AAAAND, THAT'S A WRAP! OUR FRASER HIGHLIGHT REEL - AND OUR JOURNEY AS A WHOLE - IS FINISHED.
APPLYING THE IDEAS WE'VE TALKED THROUGH TAKES PRACTICE, AND YOU MAY FIND IT HARDER TO DO WITH SOME AUDITS.
WHAT I HOPE, HOWEVER IS THAT THIS GUIDE HAS HELPED YOU TO SEE RISK AND CONTROL MORE CLEARLY AND GIVEN YOU...
...A NEW PERSPECTIVE.

THE END



FREQUENCY

A time-based frequency or a trigger that causes the control to operate.

Avoid phrases like 'on a continual basis' or 'on an ad hoc basis'. Instead, work out what triggers the check. This might be something a customer does, reaching a certain point in a process or project, or when a pre-defined threshold is met.

Make sure that the frequency you pick relates to the check you describe in the activity section.

If a control operates on more than one occasion - for example, a review that happens several times before a project go-live - your frequency should normally be the final instance of it (e.g. 'prior to go-live'). Don't use 'multiple times before go-live' as this will complicate your test plan and walkthrough.

RESPONSIBILITY

The role, team or system that performs the check.

Focus on the role/title of the person performing the check. There is no need to include the names of individual people in your control descriptions.

If you are think you need more than person in this section, be clear whether this is because:

- there are multiple people that can do it (use their job titles unless the list is long),
- the control is actually performed by a group such as a project board or risk forum (just list the board/forum), or
- the check is performed by someone with someone else present such as a senior manager's review with a junior team member (focus on the checker).

For automated controls, just list the system name (and section/screen or menu if possible).

ACTIVITY

Active check. Active check. Active check.

Active check. Active. Check.

Ac-tive chec-k. Vérification active. Actieve controle. Aktive Prüfung. Controllo attivo.

.הקידב הליעפ 主动检查
Aktyvus patikrinimas. Gwiriad Gweithredol.

طشن صحف Aktywna kontrola. Seiceáil ghníomhach

... and remember that an alert being raised isn't in itself a control: there needs to be a response as well.

SOURCES

The inputs required for the control to operate.

Use the sources section to capture what inputs the control needs to operate effectively.

Policies, data, systems, other controls and professional judgement can all feature in the sources section.

Where the sources for a control are themselves reliant on other sources, consider whether you need additional supporting controls in the scope of your audit. Don't walk by supporting controls without really considering whether they are necessary for your main controls to operate.

If you think additional sources that should be in place are missing in practice, be sure that they are really necessary and not just to make it easy to audit.

ESCALATION

How the control deals with any problems that the activity identifies.

Escalation is distinct from controls where different approaches apply to different product types, customers etc.

The goal with the escalation section is to try and show that the control has a clear end-point and doesn't just leave a lot of items incomplete.

Don't confuse something just being reported with action being taken to address the problem - if we tell someone more senior but they don't **do** anything, it's not a good escalation.

If the escalation is complex or is reliant on its own sources, consider whether it would be easier to split it into a separate control.

RESULT

The control's objective: why it was put in place.

Make the result section specific to the activity, not the wider risk.

Try to work one of the four control group categories into your results section: Completeness, accuracy, validity and restrictedness.

Don't just rewrite the activity in the result section: the control isn't an end in itself.

Don't over-write the result section: your goal is to be clear what the control should achieve so that you can judge its adequacy, and to give you a basis for your operating effectiveness testing.