ISC2 East Bay
Who's Accountable Anyway?

Sarah Clarke

Infospectives Ltd

Director ForHumanity (Not for profit AI audit solutions)

Infospectives™

FOCUS for TODAY

- Constructive Accountability
- Sustainable Risk Triage
- Visualizing Residual Risk
- Keeping it Rolling

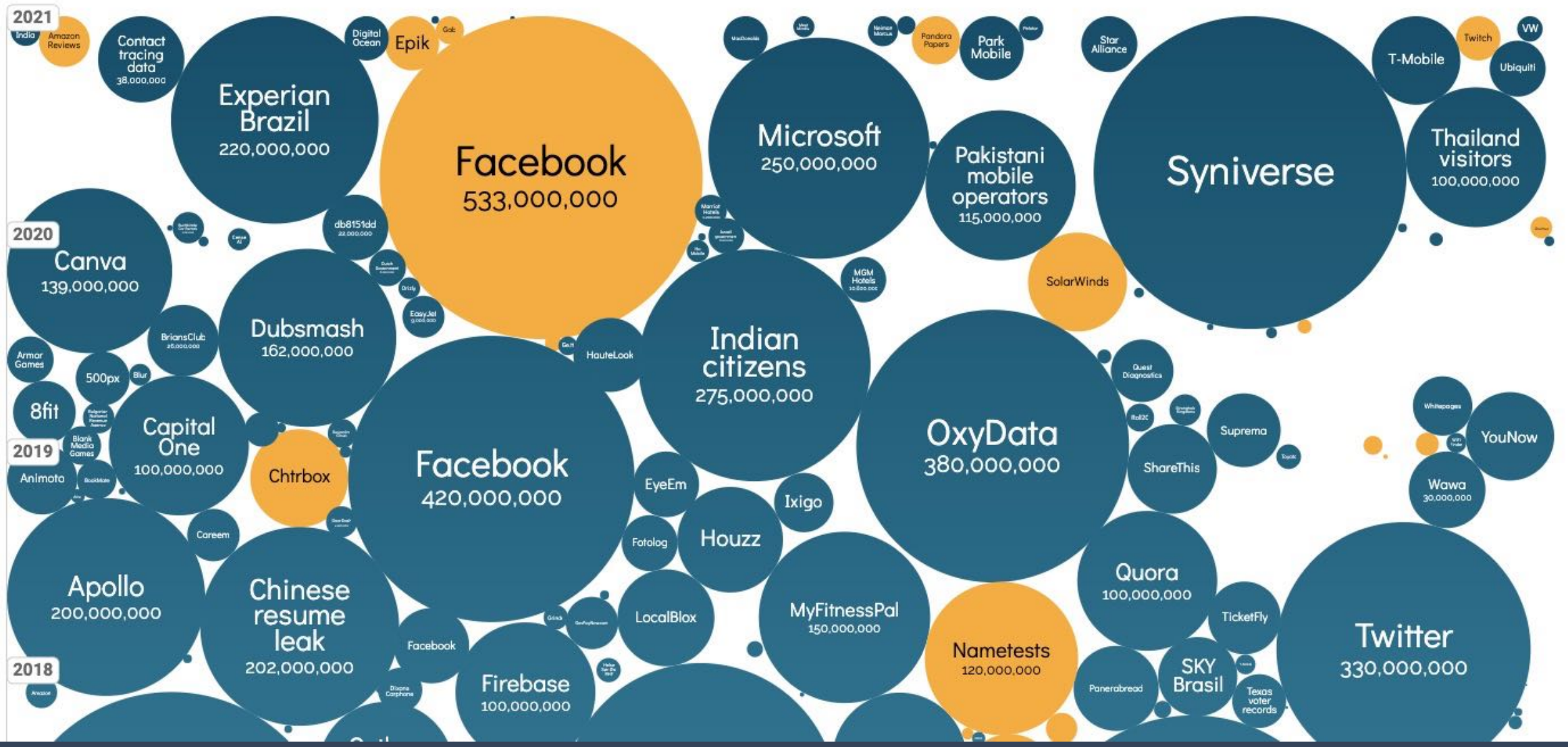
Infospectives™

World's Biggest Data Breaches & Hacks

Selected events over 30,000 records

UPDATED: Oct 2021 [Information Is Beautiful LINK]

size: records lost **filter**



What can go wrong?

WILL KNIGHT BUSINESS 01.12.2021 08:00 AM

Job Screening Service Halts Facial Analysis of Applicants

But it's still using intonation and behavior to assist with hiring decisions.

Source

Lemonade
@Lemonade_Inc

So, we deleted this awful thread which caused more confusion than anything else.

TL;DR: We do not use, and we're not trying to build AI that uses physical or personal features to deny claims (phrenology/physiognomy) (1/4)

3:45 PM · May 26, 2021 · Twitter Web App

Source

Study finds that few major AI research papers consider negative impacts

Kyle Wiggers
@Kyle_L_Wiggers

July 1, 2021 7:20 AM

Source

Accountability in a nutshell:

Accountability for risks must be FORMALLY assigned to stakeholders who have influence and means to effect change…

…stakeholders must REMAIN accountable until processing for specified purposes ceases, or the role is formally handed over…

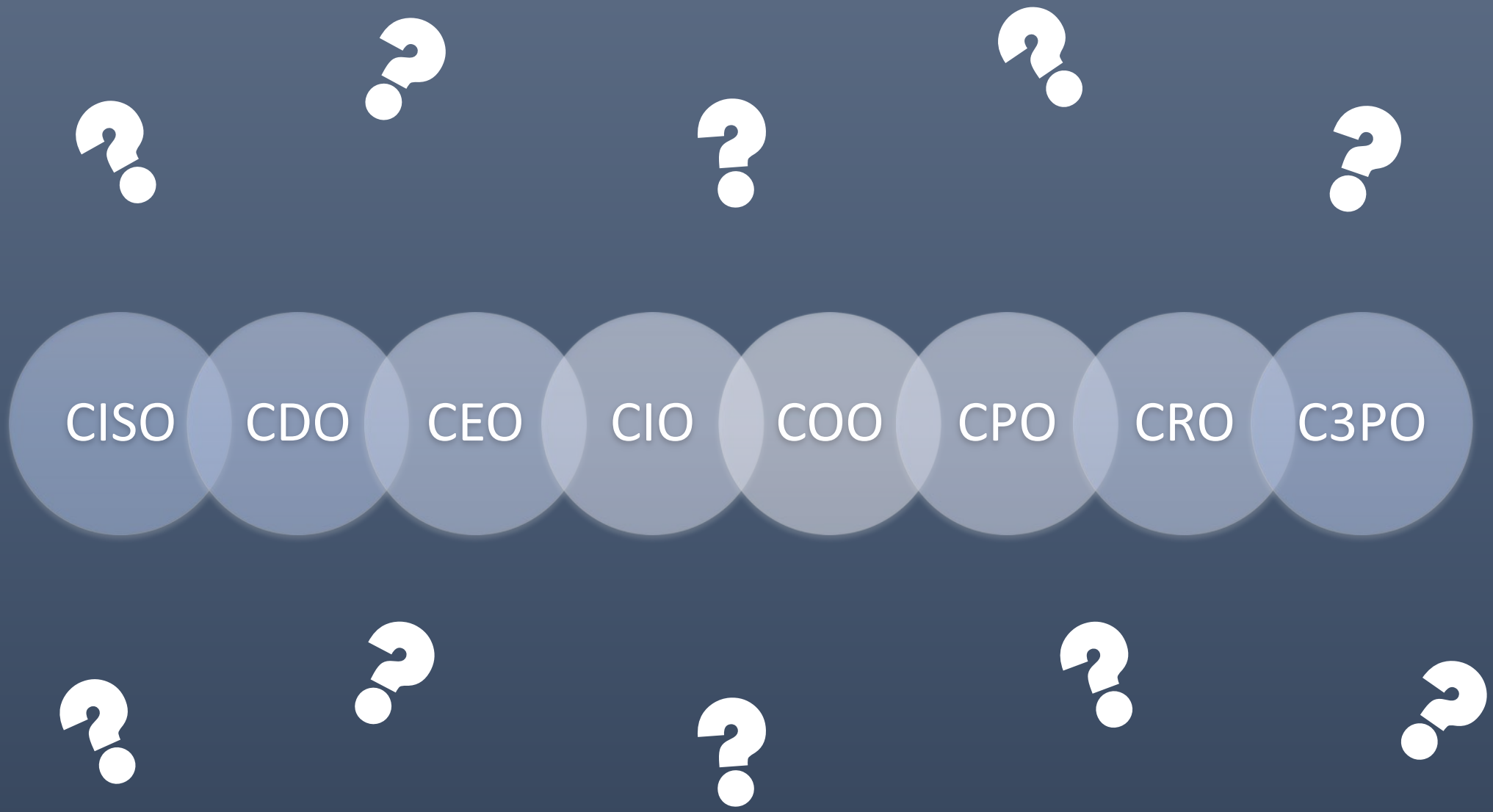
…SPECIALISTS are accountable for providing clear information about requirements, risks, and blockages…

STAKEHOLDERS are accountable for providing sufficient time, money, and support to make that work...

…because NO-ONE should be accountable for something that they can't influence, or don't understand.

4D – Multiple Accountability Dimensions

- Delegation & Demarcation
- Descoping
- Doing & Documenting
- Durability



Delegation & Demarcation

It can’t go too low

Nothing works in silos

Lack of engagement is a risk

Don’t ignore the supply chain

RACI	CISO	Security Ops	DPO	Data Protection Ops	Privacy Manager	IT Business Partner	Project Sponsor	SRM / Category Manager	CPO / Procurement Mgmt	Legal	Vendor	Risk Ops/Mgmt	Business Risk Owner	Executive Risk Owner
Approve risk criteria and thresholds for triage and assessment														
Deal with commercial/contractual objections to due diligence														
Answering intake / triage questions														
Update triage activity (annual audit)														
Facilitate assessment and remediation meetings with vendor														
Handle/escalate engagement blockages														
Conduct security and privacy compliance and risk assessments														
Report on compliance and risk status														
Ensure evidence is delivered to support findings														
Provide security/privacy SME input to support agreeing remediation														
Coordinate ongoing governance														
Provide security/privacy SME input into ongoing governance														
Oversee progress with remediation														
Re-assess residual risk after remediation														
Provide control status and risk input for risk acceptance														
Provide business and service specific detail for risk acceptance														
Identify business risk owners														
Accept risks														
Own residual risk of a breach while blockages / risks persist														

A two part story with KRIs

Engagement KRIs

Assessment Progress against target

Engagement Progress

Blockages

Remediation KRIs

Risk status by % entities

Risk status by % compliant controls

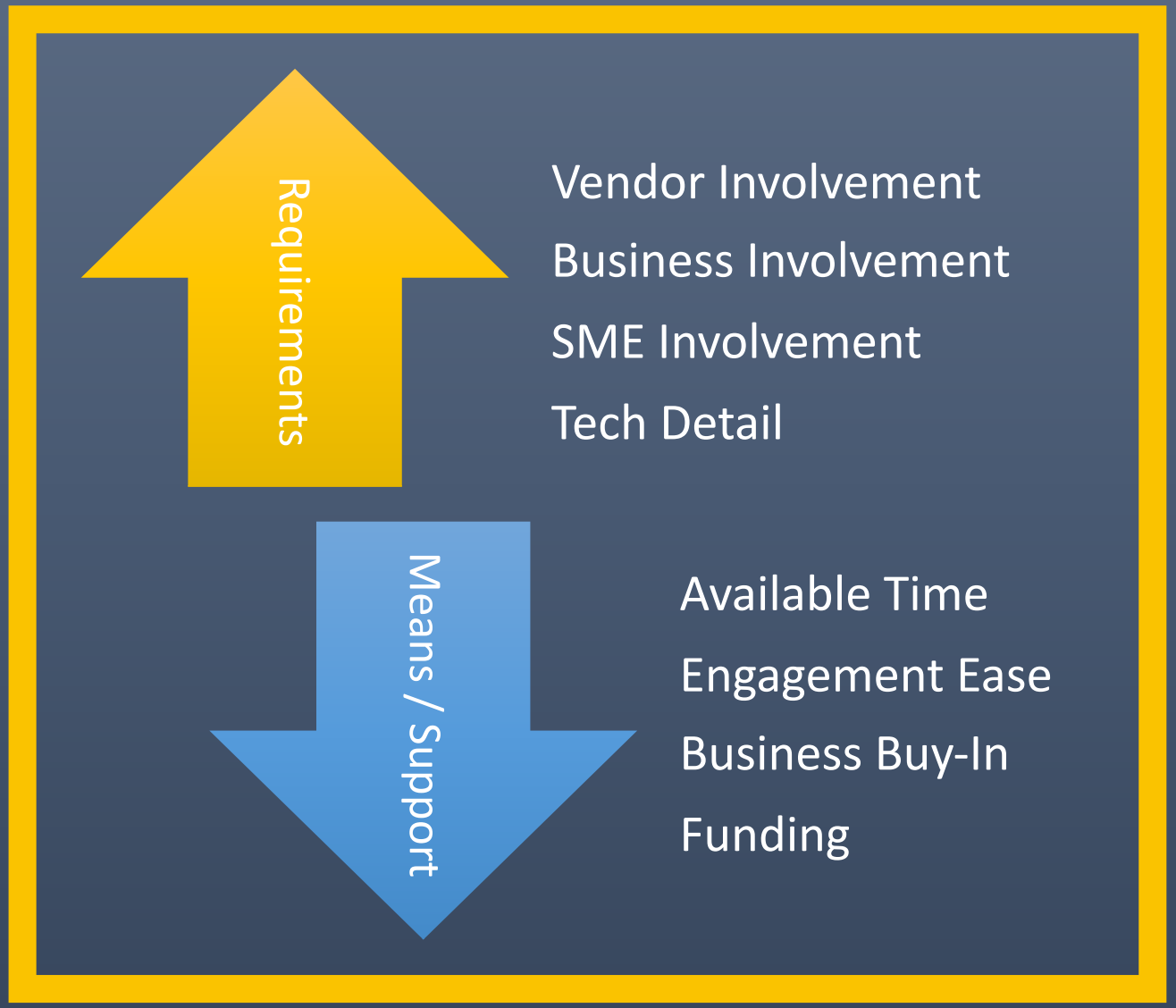
Risk status by control theme

The GRC Paradox:

We can't assess everything

We can't prioritize without assessing risk

We can't assess risk without prioritizing



Descoping

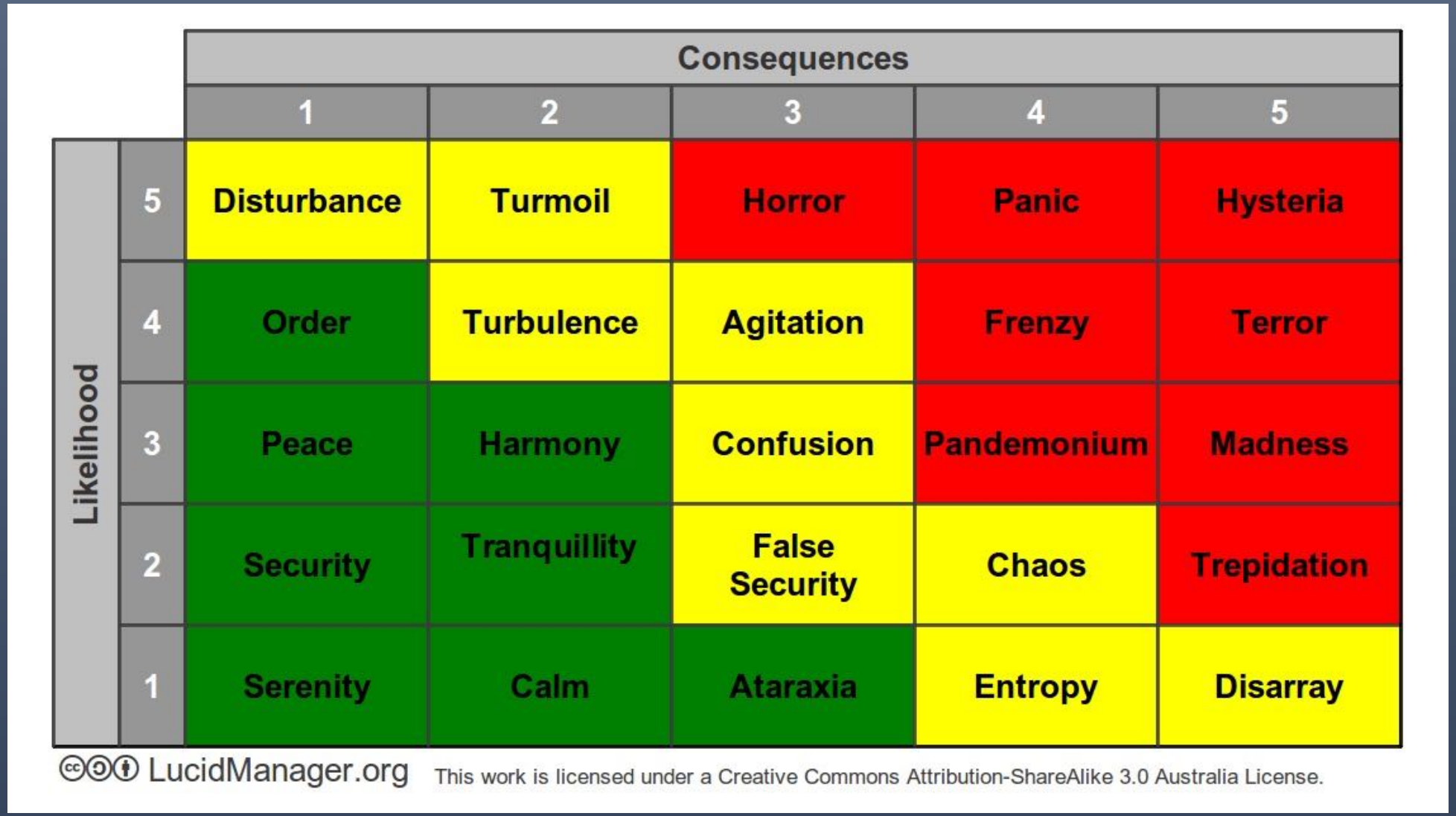
You can’t do it all

Move it all left

Agree how much is enough

Document all decisions

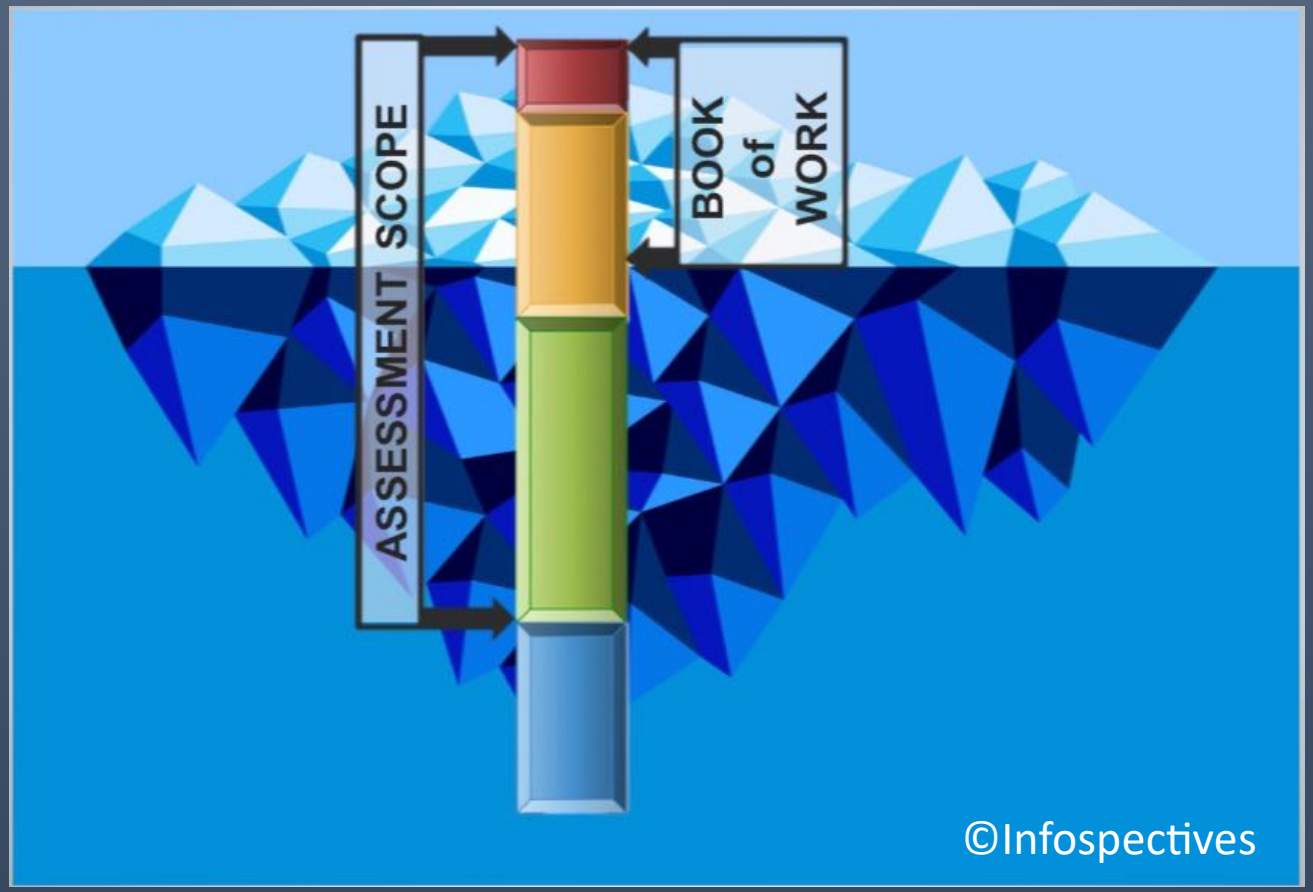
Traditional risk assessment doesn't scale



Likelihood	Consequences 1	2	3	4	5
5	Disturbance	Turmoil	Horror	Panic	Hysteria
4	Order	Turbulence	Agitation	Frenzy	Terror
3	Peace	Harmony	Confusion	Pandemonium	Madness
2	Security	Tranquillity	False Security	Chaos	Trepidation
1	Serenity	Calm	Ataraxia	Entropy	Disarray

Risk-based prioritization

- Up front planning for depth and timing
- Risk based context for de-scoping
- Evidence to support options to flex time or resource



In wider risk management context

Where is effort currently focused?

Are there bottlenecks elsewhere in the governance supply chain?

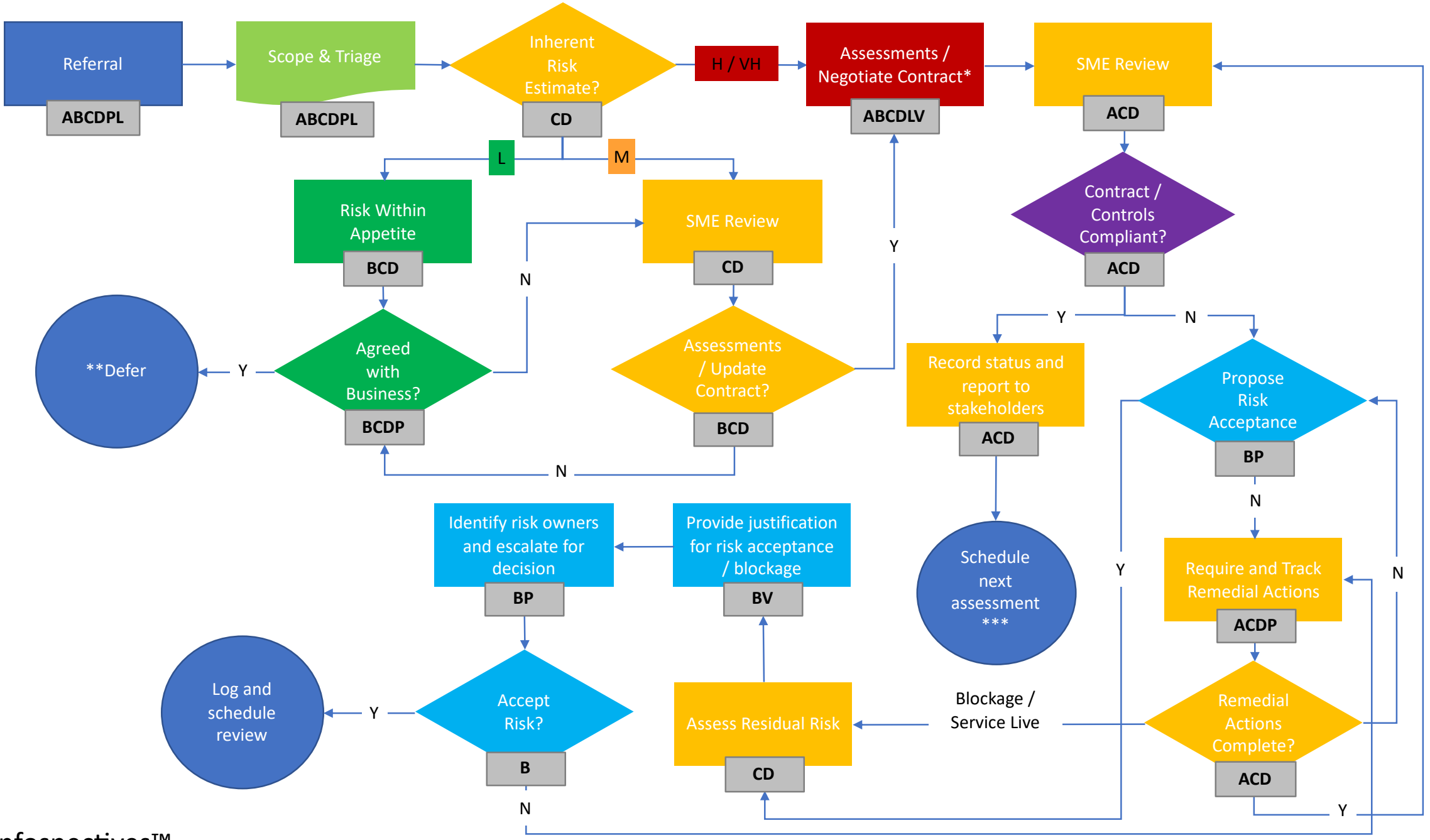
Potential for Humane Risk Management

Potential to do well

Committing to do well

Preparing well

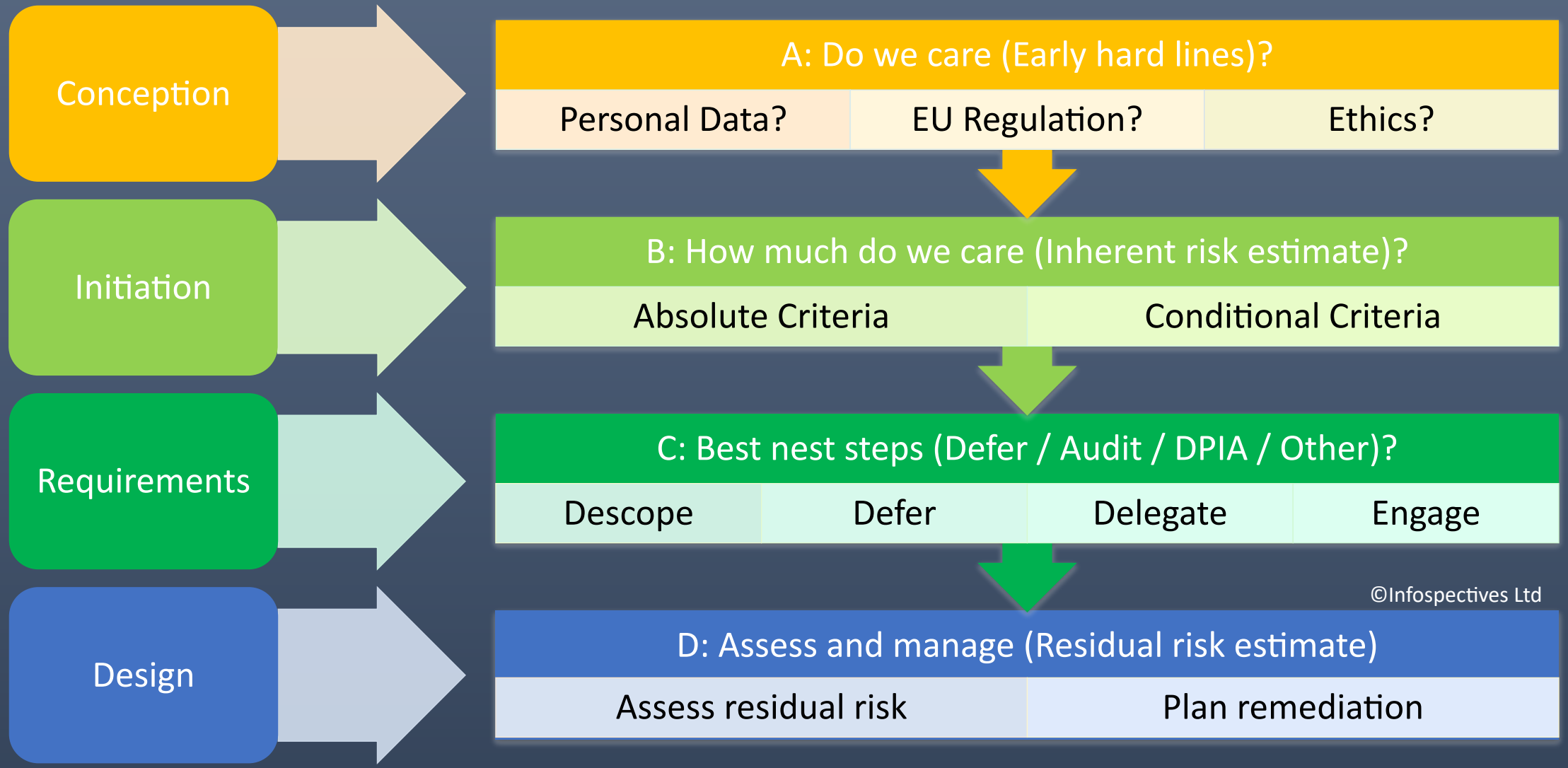
Doing well



Infospectives™

A – Applications / Infrastructure, B - Business, C – Cybersecurity, D – Data Protection / Privacy, L – Legal, P – Procurement, V - Vendor

Scope and Triage - Right questions, right people, right time



Inherent risk estimation / triage

Absolute – Policy / Law / Regulation "Must"

(No Brainers)

- EU AI Regulation High Risk criteria
- EU WP29 WP248 High Risk criteria
- Secret company data
- Most sensitive personal data.
- Most vulnerable people / environments
- High probability of reuse
- Highest complexity
- High risk supply chain
- Known data bias
- Novel technology with unknown implications

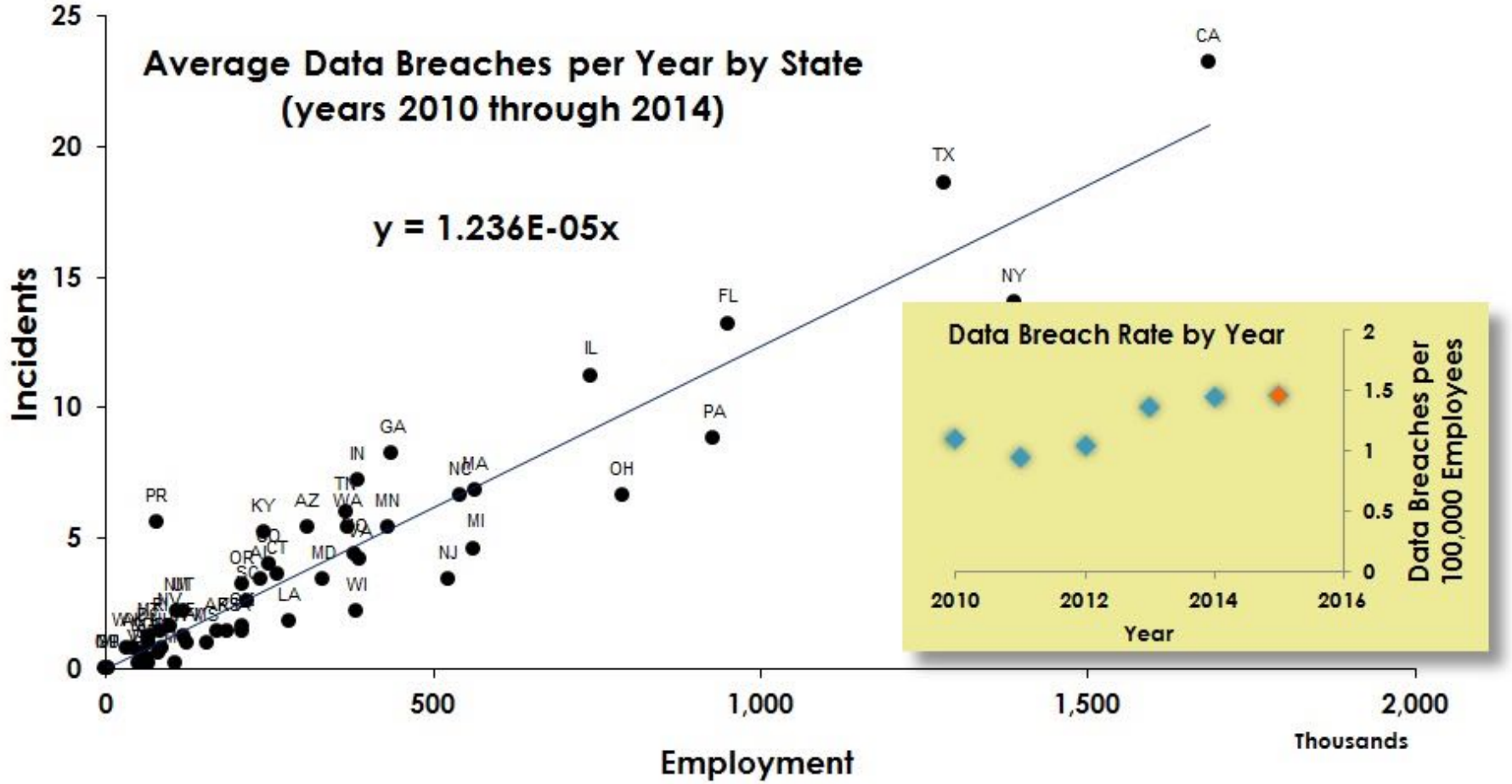
Conditional – Policy / Law / Regulation "Should"

(Tie Breakers)

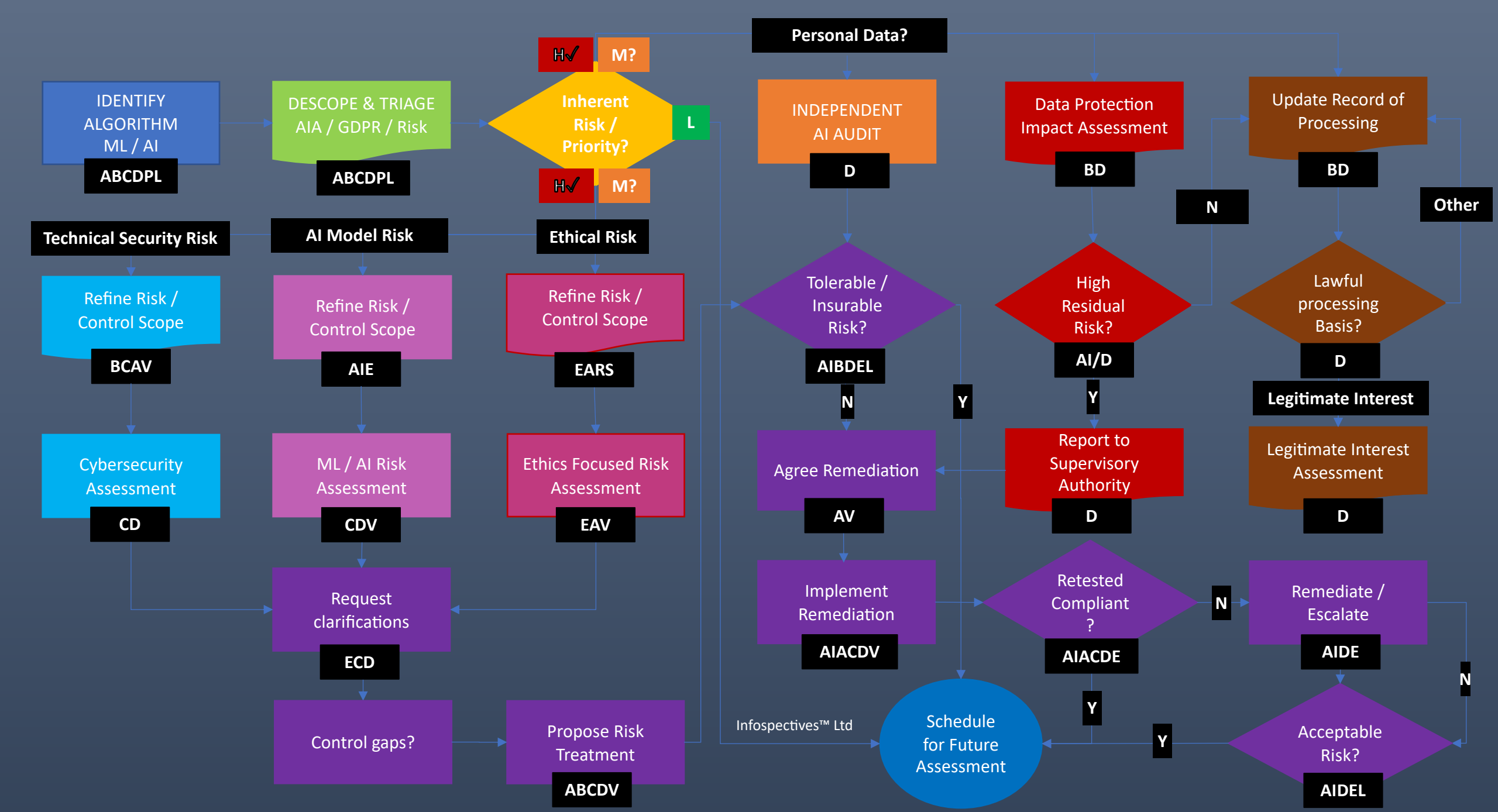
- Location in AI Supply Chain
- Data quantity / throughput
- Other specific legal / regulatory requirements
- Dependence on other third parties
- Potentially impacted systems
- Vendor size / maturity
- Internal governance maturity
- Potential for persistent bias
- Availability of specialists
- Delivery or contract renewal date

Example: New Insights from Empirically Derived Factors

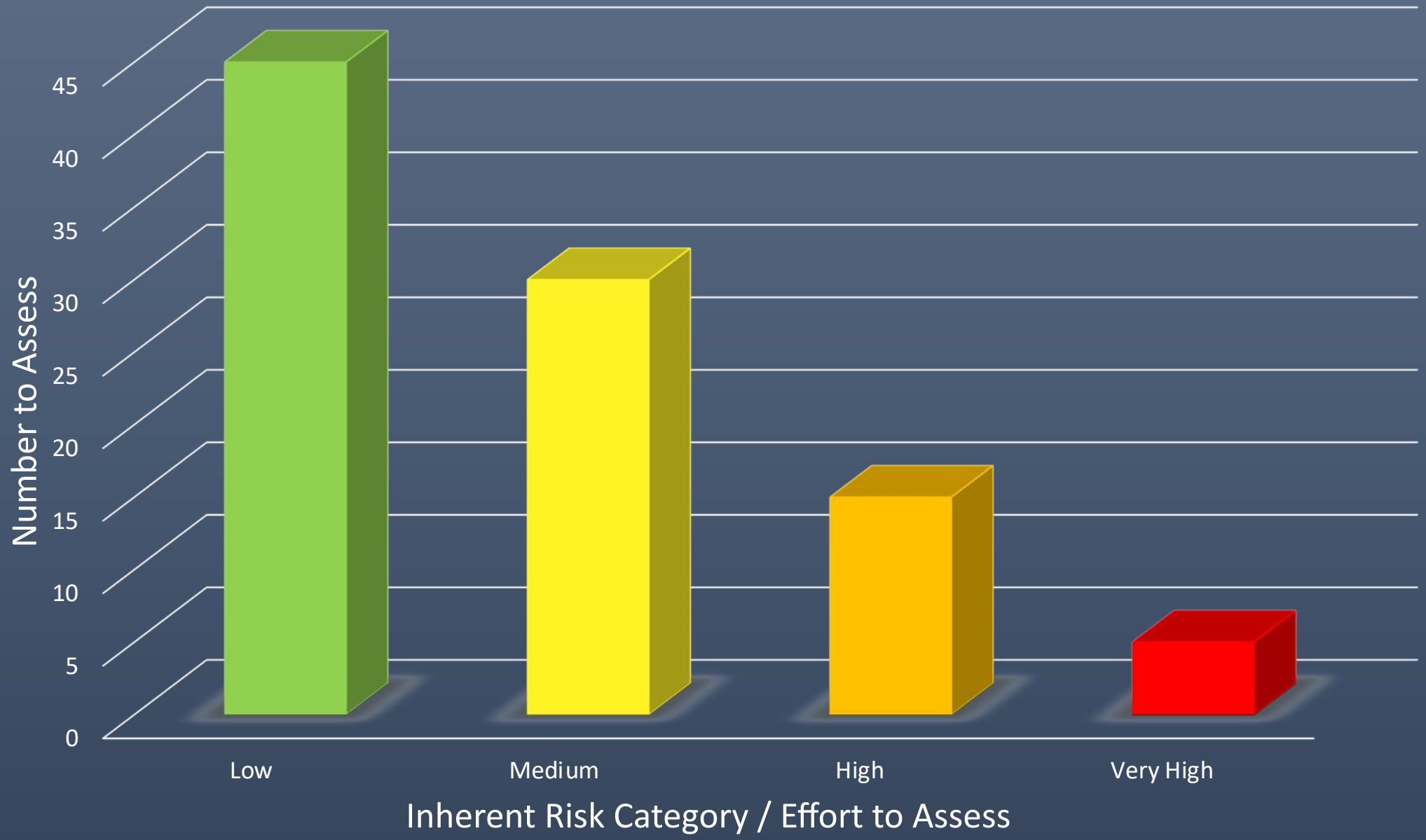
Number of employees is a predictor of data breach rate.



Reference: *Probability of a Data Breach in the Healthcare Industry,* Chuck Chan, Spencer Graves and Thomas Lee, VivoSecurity Inc., 2014



AI – AI Risk Stakeholders, A – Applications / Infrastructure, B - Business, C – Cybersecurity, D – Data Protection / Privacy, E – Ethics Officer, L – Legal, P – Procurement, V - Vendor


Number to Assess
45
40
35
30
25
20
15
10
5
0
Low
Medium
High
Very High
Inherent Risk Category / Effort to Assess

Make every question count

- Map answers to planning decisions
- Keep it simple
- Make sure you can analyse
- Test priorities and logic with stakeholders
- Record their risk appetite
- Define and sign off common exceptions

Doing & Documenting

- Prioritize next steps
- Keep it simple
- Re-use your inherent risk
- Non-compliance does not equal risk

Being afraid isn’t the same as being at risk…

…being at risk isn’t the same as being at proximate or intolerable risk

Me c.2013

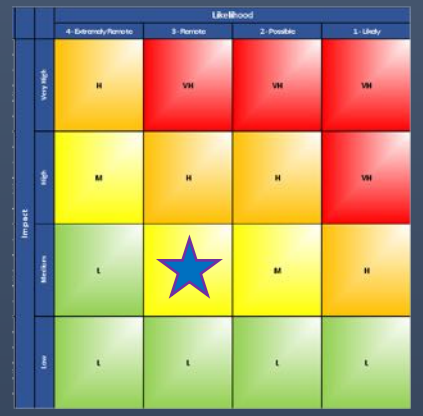
From Initial Inherent Risk Estimate to Residual Risk

Initial Inherent Risk Estimate → **Validated Inherent Risk Estimate** → **Controls Assessment** → **Residual Risk** → **Mitigated or Accepted Risk**

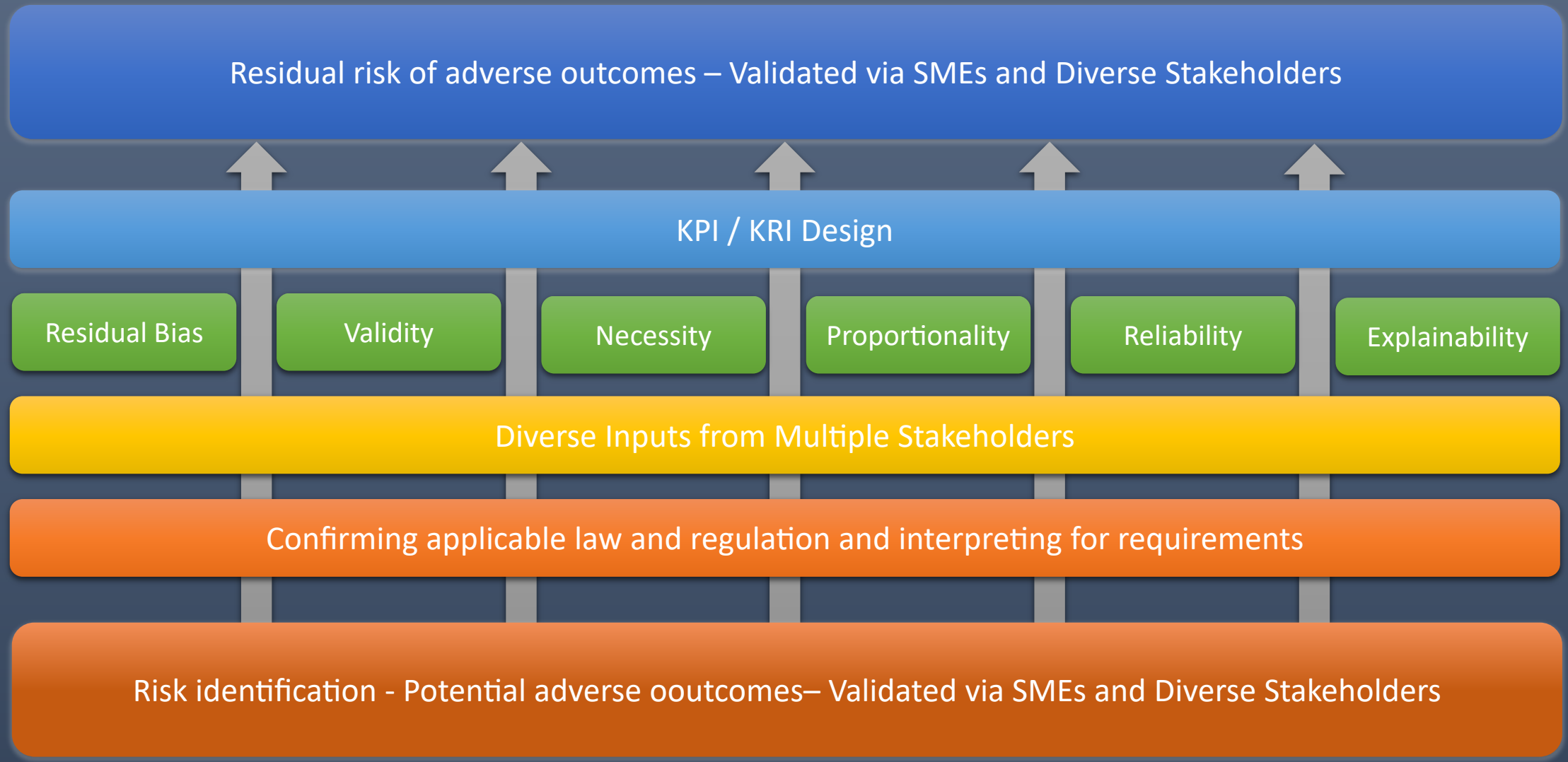
LEGS / REGS

POLICIES / STANDARDS

TECHNICAL / ETHICAL PROCEDURAL / DATA



Ethics Risk Analysis



Describe and Visualise Residual Risk – Impact / Probability?

Traditional Risk Matrix

Tiered impact

- Financial (fraud / fine)
- Reputation (Customer Confidence / market share / share price
- Portion of impacted customers (informs notification costs)
- Level of impact on individuals (harms and loss of freedoms)

Tiered probability

- 4 (Unlikely) to 1 (Probable
- Annual Loss Expectancy

Impact	Likelihood			
	4 - Extremely Remote	3 - Remote	2 - Possible	1 - Likely
Very High	H	VH	VH	VH
High	M	H	H	VH
Medium	L	M	M	H
Low	L	L	L	L

Describe Residual Risk – Hybrid Qualitative / Quantitative?

VCIO ”Energy Labels”

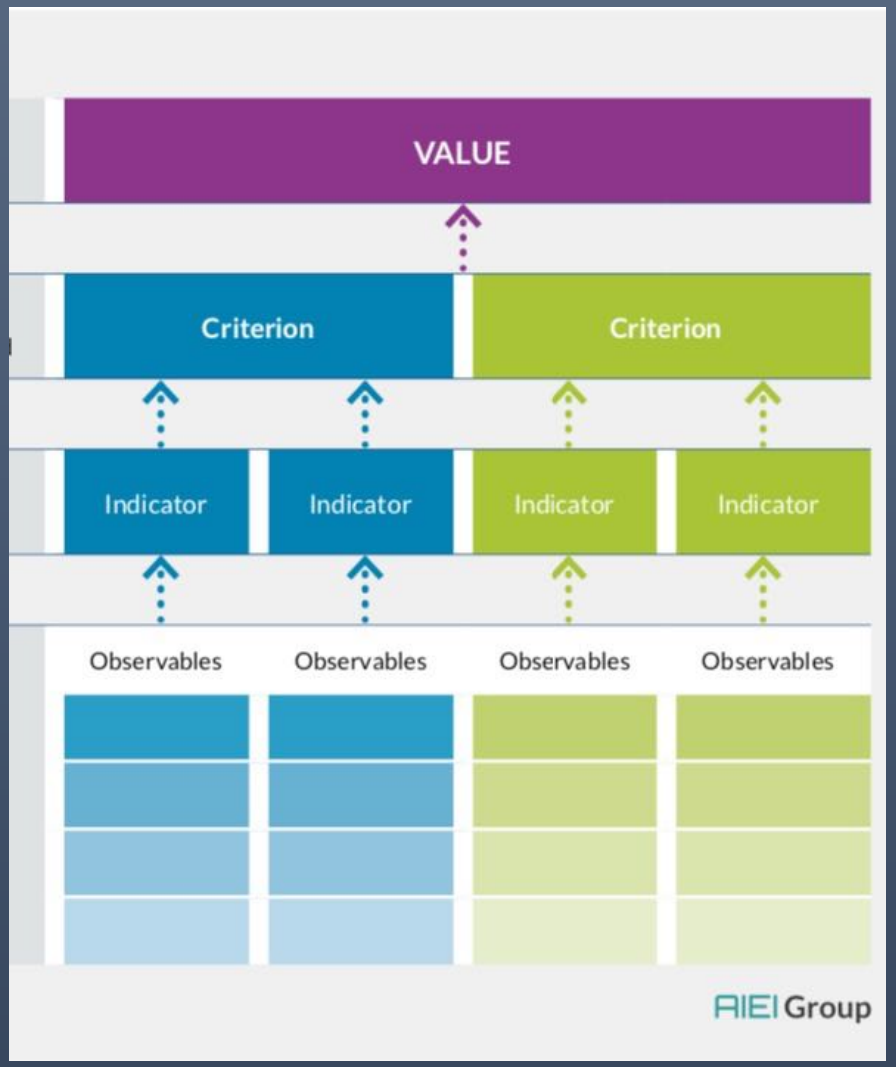
Values:

- Transparency
- Accountability
- Privacy
- Justice
- Reliability
- Environmental Sustainability

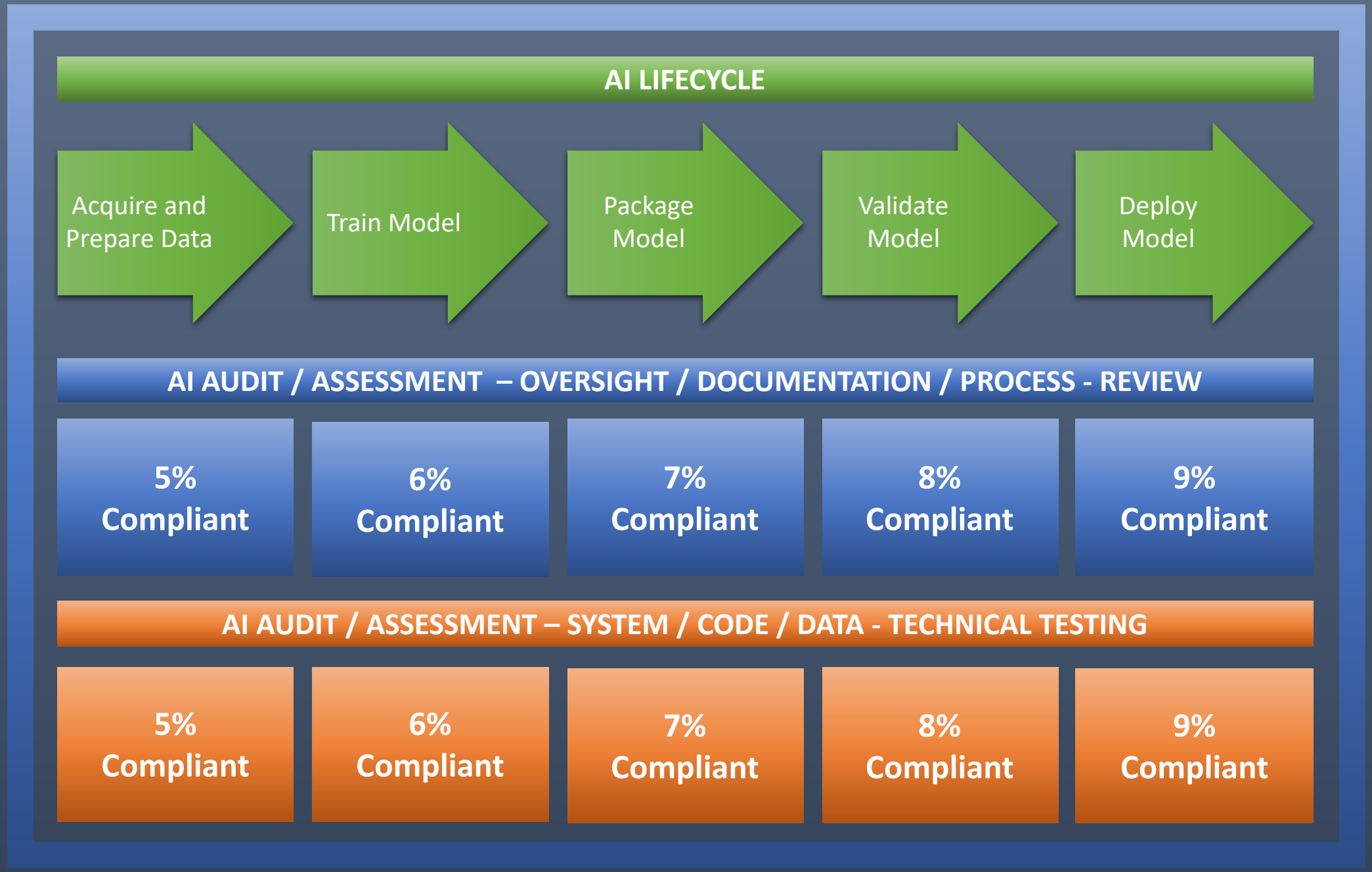
Criteria

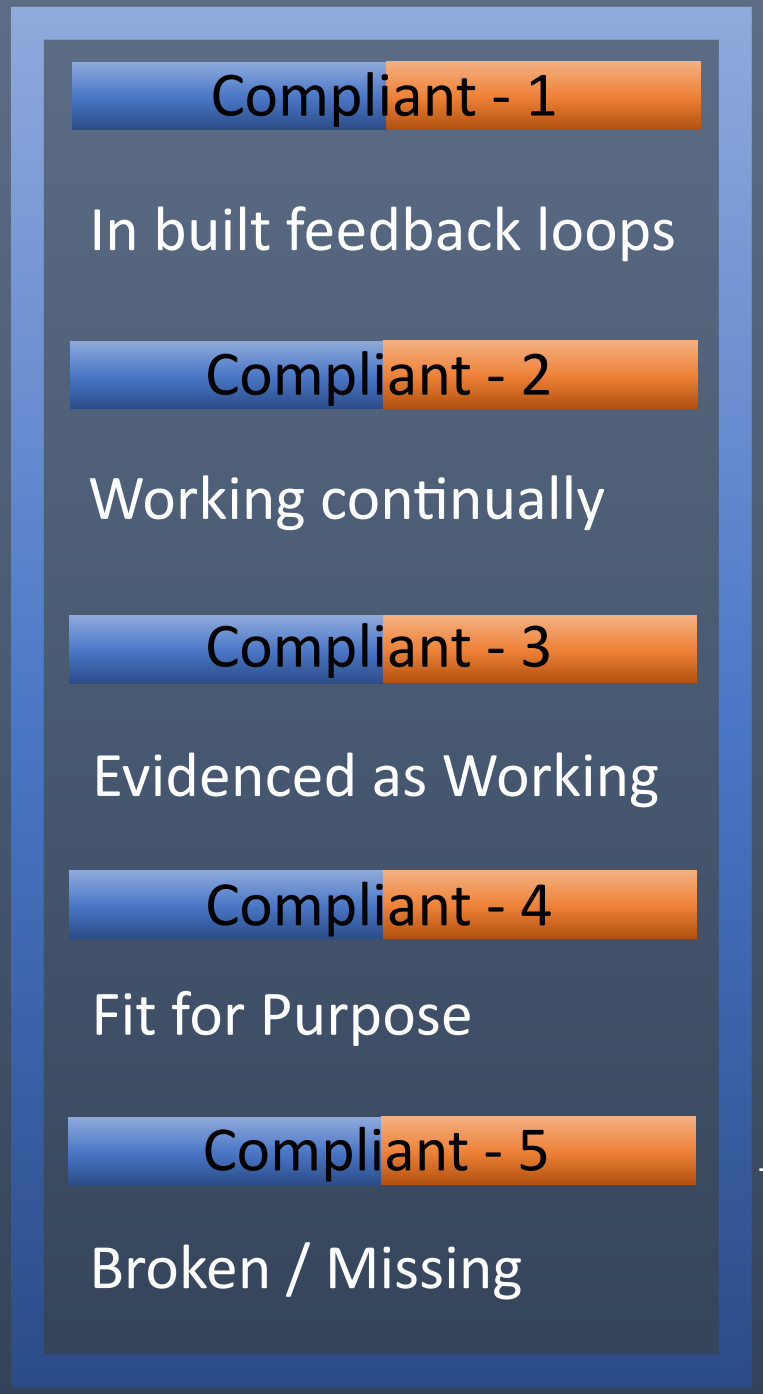
Indicators

Observables



Source: Krafft, Hauer, 2020: From Principles to Practice - An interdisciplinary framework to operationalise AI ethics



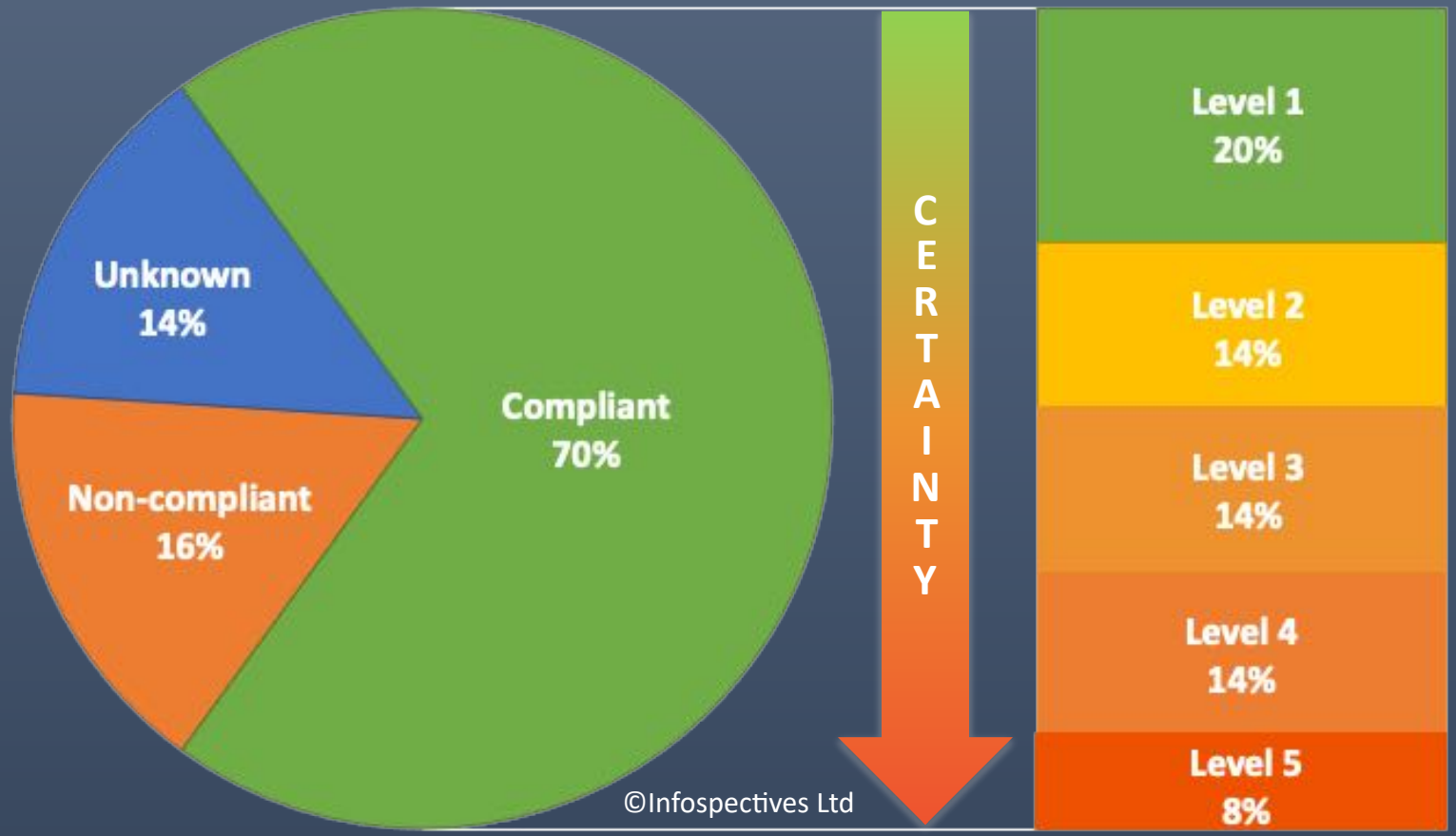


How compliant is compliant?

- How confident are you about reported compliance?
- Which portion of your AI lifecycle does the risk mitigation value apply to?
- Which subset of controls were tested?
- What portion of your inherent risk does that mitigate?

Resolve unacceptable uncertainty now, or plan to respond later

- **64%** of controls with unacceptable uncertainty
- Contractually limit liability?
- Insure?
- Government backed liability limitation?
- Expert, prompt, responsive post-market monitoring and incident / dispute resolution?



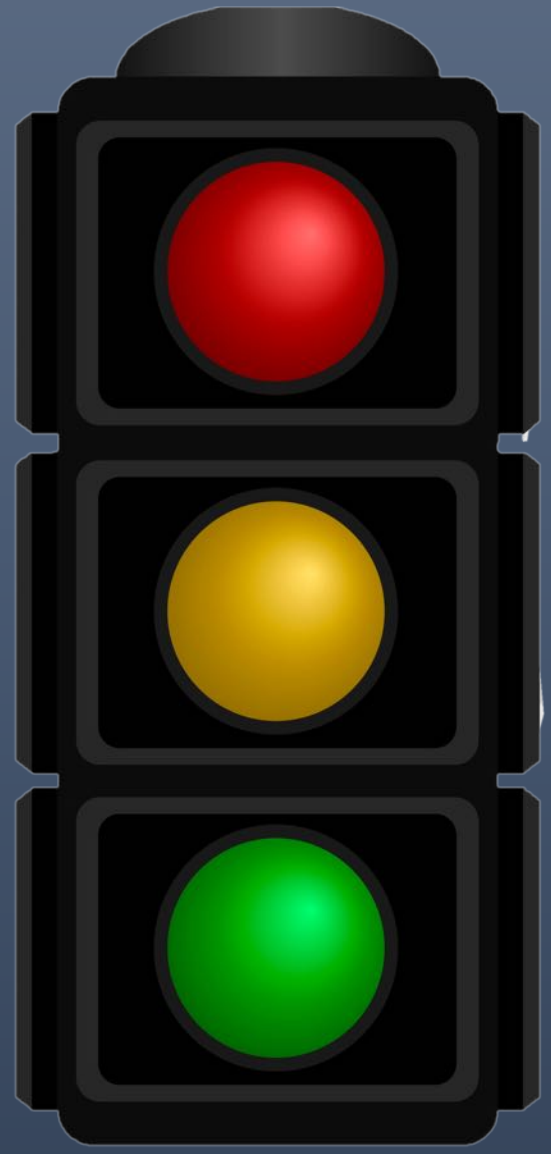
Combine maturity and inherent risk for options to flex

HIGH inherent risk + Low maturity / capability = Stop, deep dive, mature / fix / reduce risk. Ensure MEDIUM / LOW before progressing. Re-triage frequently.

MEDIUM inherent risk + Low maturity / capability = Pause for validation, if remains MEDIUM, re-triage after changes, mature / fix before releasing

LOW inherent risk + Low maturity / capability = Proceed, re-triage after change to ensure risk remains LOW, maturing in parallel

Ethically tolerable justification for exception?



Copyright: lekichik

Durability
(for next time)

It’s a rolling process

Map what you do and share

Model your resources

Rinse and repeat

We need more investment in translation and means to ease assessment

Our future won't be lost to the singularity…

…it will be lost to undervalued GRC mundanity, siloed scrutiny, excessive faith vs reproducibility, and absence of constructive accountability