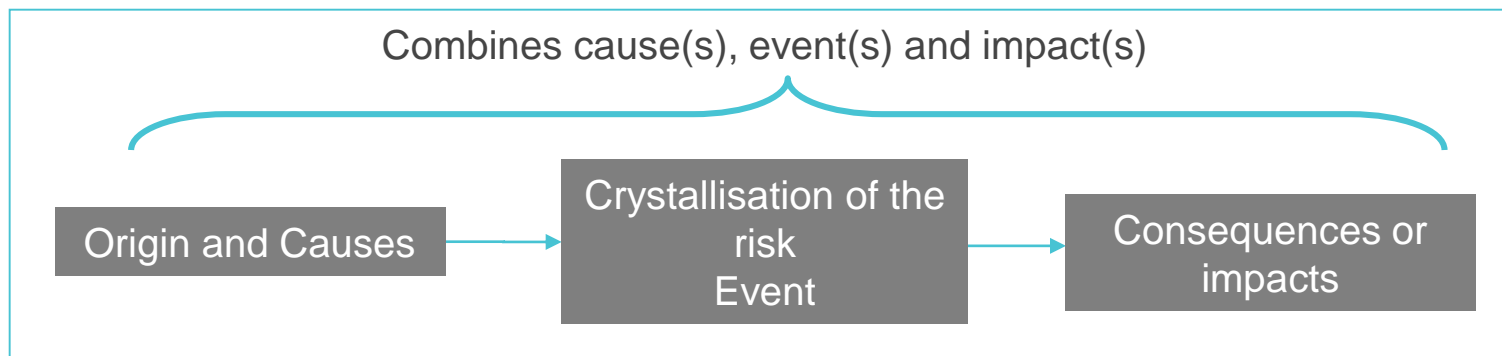# KEY RISK INDICATORS: METRICS OF RISK DRIVERS

What are risk drivers?

- Risk Drivers
- Causal factors
- Risk factors
- .. Are all synonymous of:
  - What causes an incident
  - What increases the risk of adverse consequences

Combines cause(s), event(s) and impact(s)

Origin and Causes	→	Crystallisation of the risk Event	→	Consequences or impacts

Classifying KRIs

Indicator Type	Description
Exposure Indicators	Any significant change in the nature of the business environment and in its exposure to critical stakeholders or critical resources. Flag any change in the risk exposure.
Stress Indicators	Any significant rise in the use of resources by the business, whether human or material. Flag any risk rising from overloaded humans or machines.
Causal Indicators	Metrics capturing the drivers of key risks to the business; *the cause of the cause* of incidents. The core of preventive KRIs.
Failure Indicators	Poor performance and failing controls are strong risk drivers. Failed KPIs and failed KCIs.

Risk Drivers from the business environment:
Exposures and *Vulnerabilities*

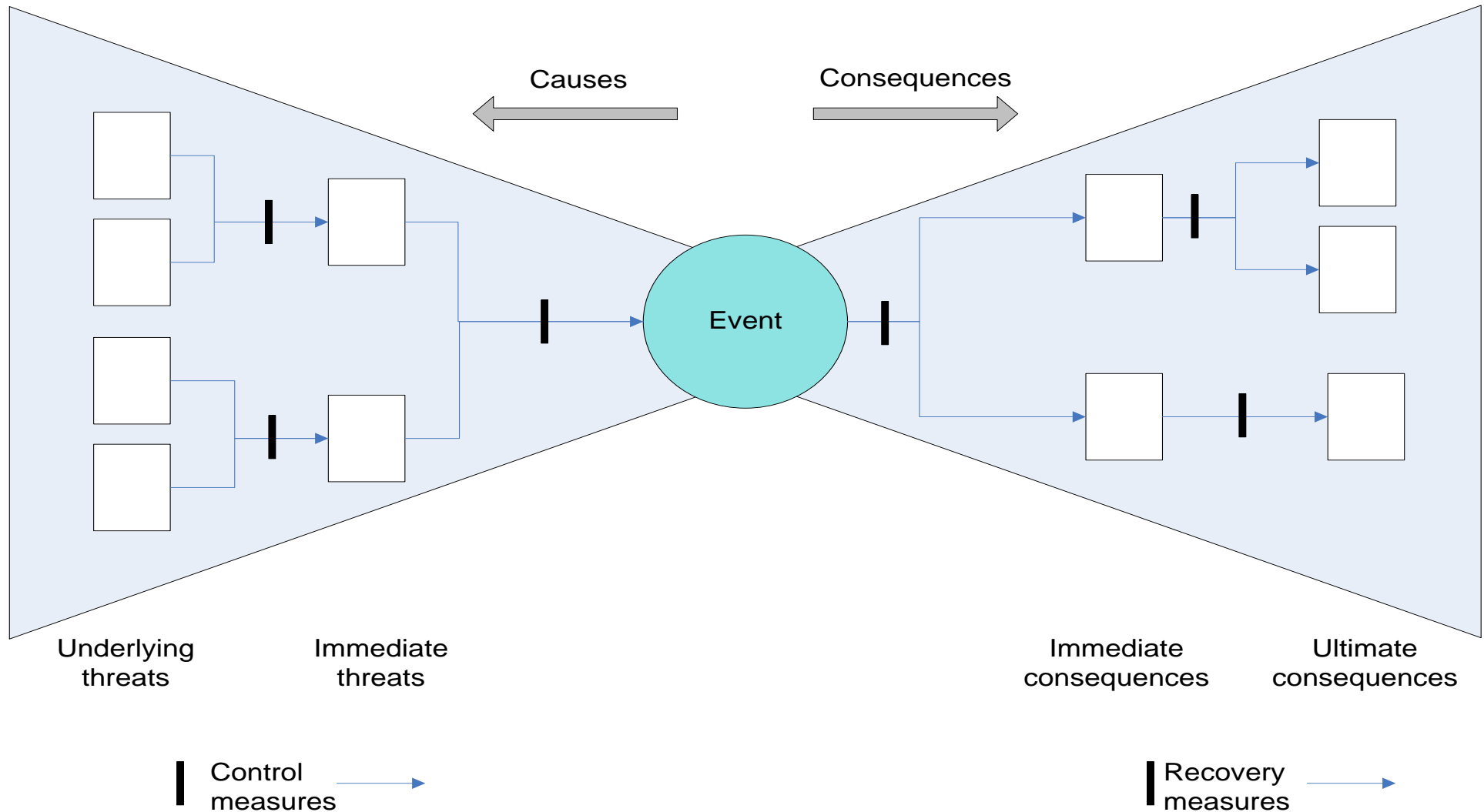| Exposures	Vulnerabilities
• Key distribution channels • Main clients • Main suppliers and third parties • Critical systems • Regulatory exposure • Main drivers of revenues, drivers of value • Brand value • ...	• Weakest links • Fragile systems • Revenue channels at risk • Systems or processes not integrated • Parts of the business resistant to risk management • Small, unmonitored operations or people • Unmaintained systems • BCP due for testing or updates • ...

Cause of the cause: the bow tie

Causes

Consequences

Event

Underlying threats

Immediate threats

Immediate consequences

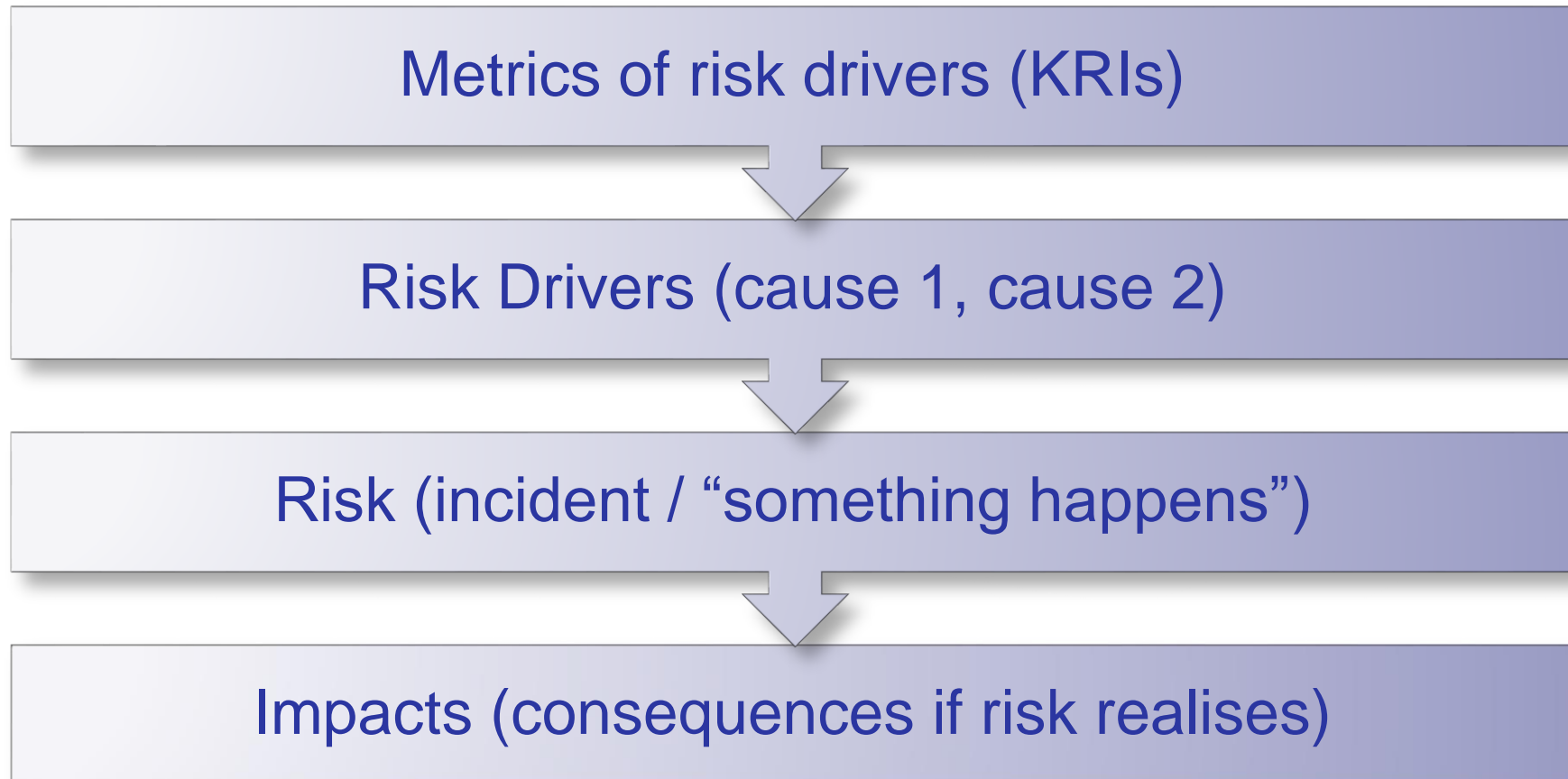Ultimate consequences

Control measures

Recovery measures

KRIs & Risk Drivers – Examples

- Human Resources
  - Impacts: knowledge loss / business disruption / financial impacts
  - Risks: abrupt loss / resignation of key staff
  - Risk drivers - of impact
    - Concentration of information of key people
  - Risk drivers – of likelihood
    - Of resignation: Bad boss / Bad pay
  - Metrics around risk drivers (KRI)
    - KRI Bad pay: Pay gap compared to market rate
    - KRI Bad boss: results of 360 review, of satisfaction / engagement survey
    (Rather than: "staff turnover")
    - KRI Info concentration: # key staff without trained alternate

KRI – Definition Structure

Metrics of risk drivers (KRIs)

Risk Drivers (cause 1, cause 2)

Risk (incident / "something happens")

Impacts (consequences if risk realises)

KRI, KPI, KCI? - Failure indicators

- **Key Risk Indicators**: *announcing troubles ahead*

  - Preventive KRIs: addressing risks (leading), not events (lagging)

- **Key Performance Indicators**: *shaping behaviours*

- **Key Control Indicators**: *measuring control effectiveness*

- However, indicators depend on context

  - Failed KPIs can constitute KRIs

    - Example: IT response time

  - Failed KPIs in a control function are altogether KPI, KCIs, KRIs

    - Example: pending confirmations in Back office of trading activities

Selection and Monitoring Phases

Selection Phase

- Initial step of a process: credit attribution, investment decision, supplier selection...
- Most of the process steps are controls, some of them are key :client history & documentation, due diligence on partners and suppliers, etc.
- **KRIs are mostly failed KCIs**

Monitoring Phase

- Life of a contract after initial decision: life of a credit, a project, a supplier, an IT system...
- Most of the process steps are time monitoring (interest payment schedule, project deliverables on time) and quality controls (client financial situation, vendor quality, investment return, etc.
- **KRIs are mostly failed KPIs**

Risk and Predictability: Aggregating colours

Are two oranges worth a red?

Are two greens and a red worse than three oranges?

- Risk data are often (always?) not additive nor linear
- It all depends on:
  – The intensity of the risk drivers/ the predictability of the KRI
  – The threshold definition
- **If strong predictive KRIs apply the "*weakest link*" rating**
- **If weak predictive KRIs: apply the "*majority*" rating**
- Examples:
  – Weakest link: the worst colour is the overall rating: all red if the driver is drunk: don't get in the car
  – Majority: the most common colour is the overall rating: in HR KRIs typically (overtime + low engagement + uncompetitive pay = turnover and fraud)

# Post Validation of KRIs – a Simple Case

- In case of an event, check the colours of the related KRIs
  - If they were green: they are probably useless
  - If they were amber / red: was there any action taken

- Conversely, check the situation after indicators turn red / amber:
  - Has is led to events?
  - If not, it can mean either:
    - KRIs are inappropriate, or too strict, or you just got lucky
   - Action was taken to avoid incidents, in that case, KRIs play their role fully.

Pre & Post validation – data driven

- Identify the risk drivers

  - A change in the value of KRI change has an incidence on the occurrence of events

- Identify the relevant threshold, if any

  - No specific threshold: linear relationship

  - Specific threshold: inflexion point (e.g. hockey stick effect in human error once overcapacity is reached)
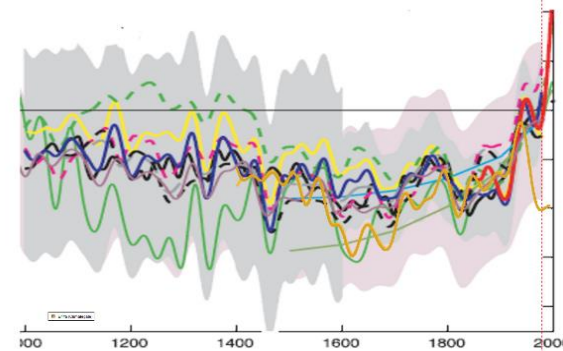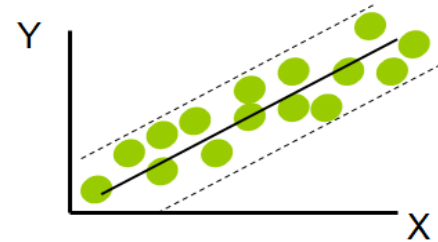
Pre & Post validation – data driven

- Multiple inflexion points – example:
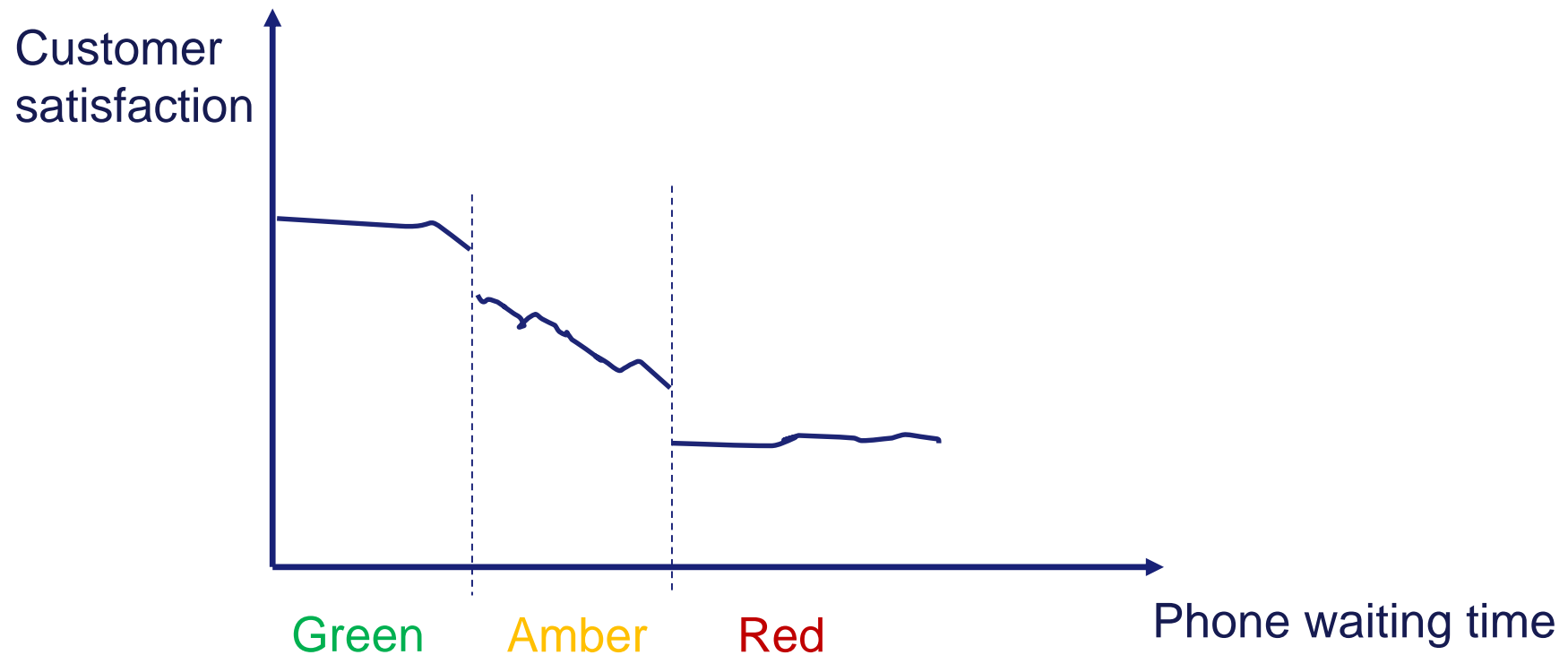
Summary: Effective KRI Features

1. Early warning devices
   - Signal changes in risk: increase in probability or in impact, *before* the risk materialises

2. Must address risks, not events
   - KRI are metrics capturing risk drivers
   - Or proxies of these risk drivers
   - "Lagging" indicators are instead, incidents reports

3. Specific to each activity:
   - Specific to each risks, and to specific weaknesses and culture of different institutions
   - One size does not fit all

4. Best identified via data analysis and experience
   - Business experience complements lack of data
   - Data analysis: to confirm business intuition, and uncover other effects

Summary: Effective KRI Features

5. May need heavy data collection

   – Trade-off to operate between the value of information collected and its cost of collection

   – Better if automated

6. Must be easy to use and timely

   – Should match the cycle of the activity: from real time (eg IT) to one-off (eg exposures), depending on the risk and the business cycle

7. Must help business decision

   – The rules of reporting apply to KRIs: only keep reports that do influence business decisions

8. Thresholds linked to risk appetite

   – Typically, lower threshold for core business (low risk), but not always

   – 100% (or about) target reliability does not mean 100% for all indicators; but only so collectively

9. Must be back tested for validity

   – *How do you know it works?* An essential question in risk management