RSA®Conference2018
San Francisco | April 16 – 20 | Moscone Center

NOW MATTERS

SESSION ID: GRC-W04

CREATING ORDER FROM CHAOS: METRICS THAT MATTER

James Lugabihl

Director, Execution Assurance-
Global Security Organization, ADP

Marta Palanques

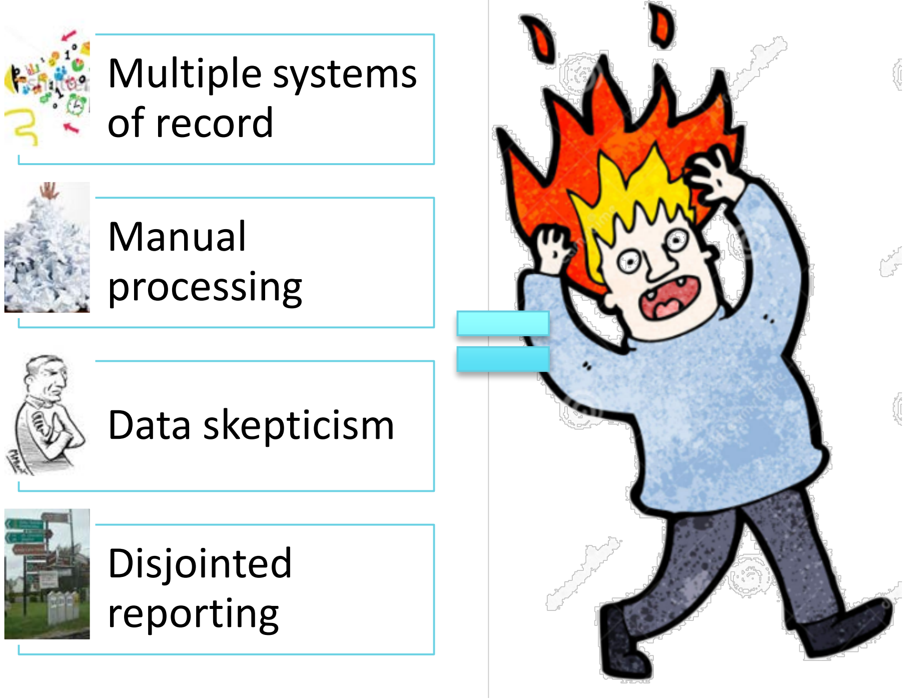
Security Lead Consultant, Execution Assurance-
Global Security Organization, ADP

Uncomfortable questions

The executive asks

- What controls need to be implemented?
- Where do those controls need to be implemented?
- Where do we allocate resources?
- How can investments be rearranged?

What you have available to answer



Multiple systems of record

Manual processing

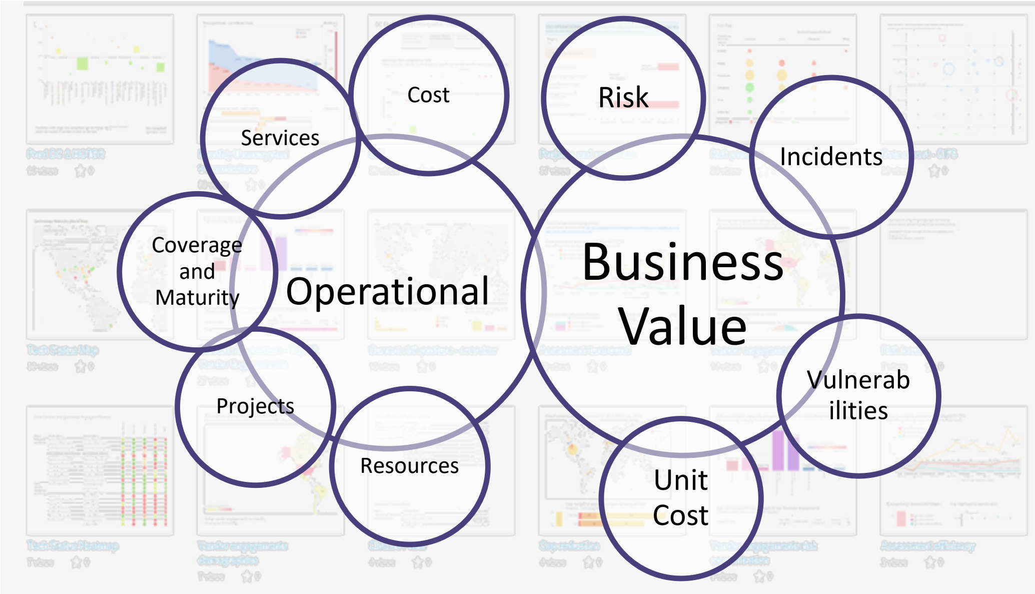
Data skepticism

Disjointed reporting

Our solution

Executive self service

- Self-service platform that enables security decision making
- Oriented to answer leadership questions
- Allows to intuitively navigate data leveraging conceptual relationships
- Uses data that is currently available in multiple environments



Retrospective

Where is our program today

- Reduced time to execute 3 previous manual reports by 70%
- Added 12 more services
- Currently using 6 data sources
- Monthly report on our key goals and risk areas
- 140 users, 54 of which are active

What did it take

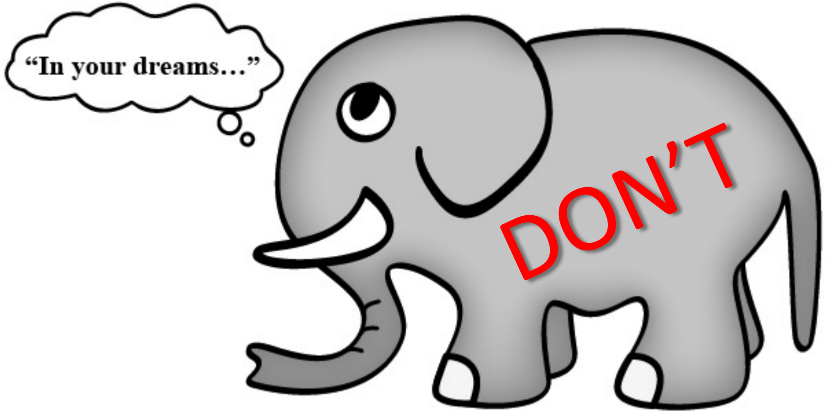
- 18 months
- 3 resources
- Approximately 3,000 work hours to build

What to expect

- A pragmatic 5-step approach to implement metrics
- Survival tips
- Ideas on integration with risk framework
- Visualization techniques for your audience

Where to start

How do you eat an elephant?

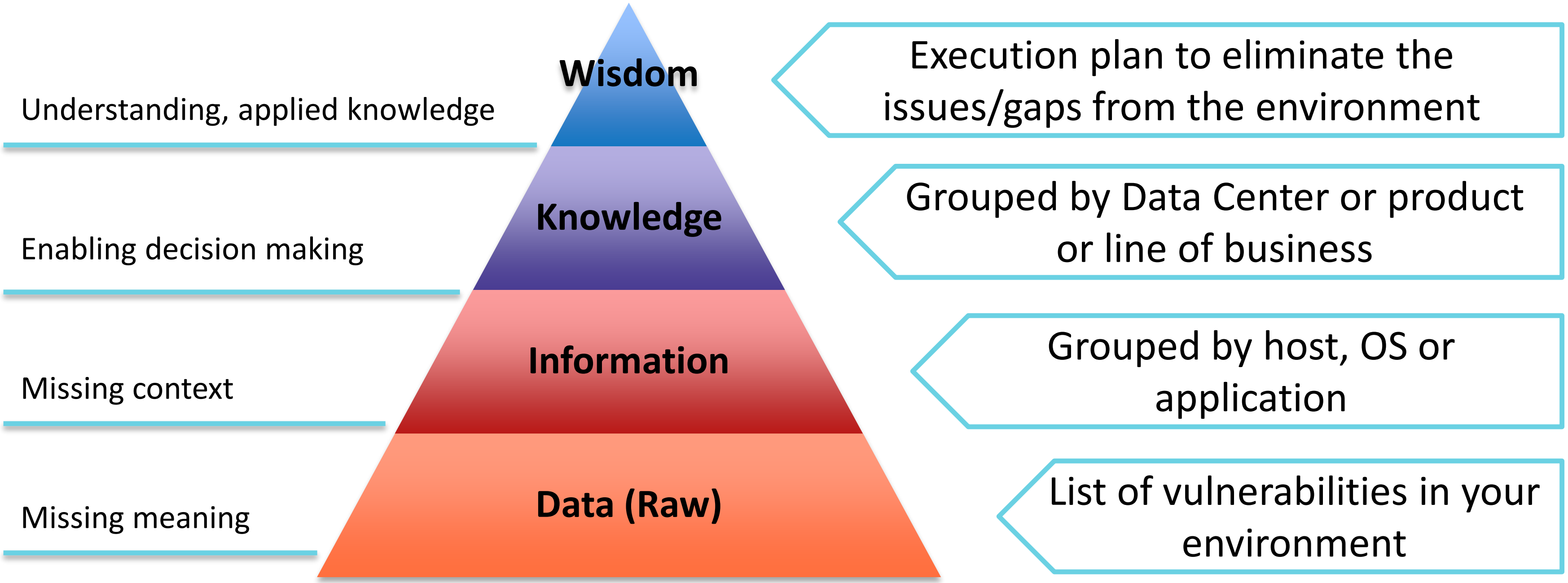


Stick to your goal!!!

- Accelerate decision making
- Ensure we're doing the right things the right way
- Achieve more with less: identify focus areas ("low hanging fruit")

Survival tip #1

Application of the DIKW pyramid



Understanding, applied knowledge

Enabling decision making

Missing context

Missing meaning

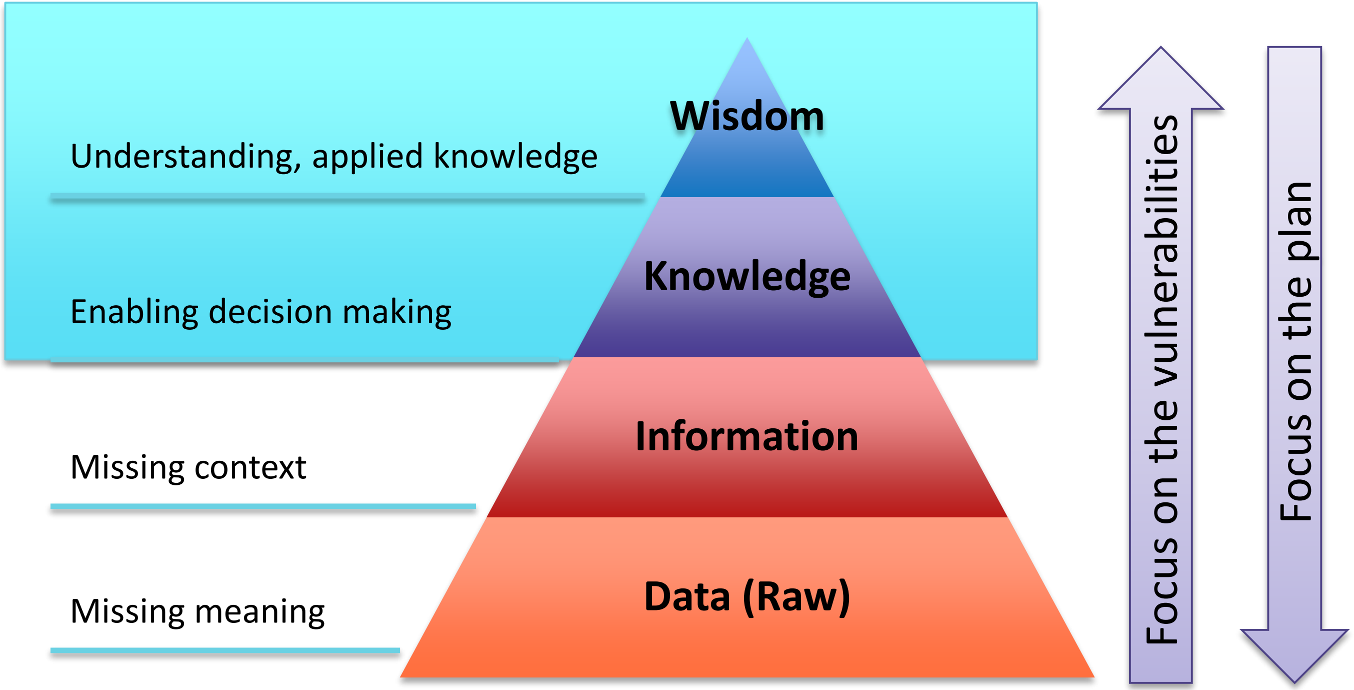
Execution plan to eliminate the issues/gaps from the environment

Grouped by Data Center or product or line of business

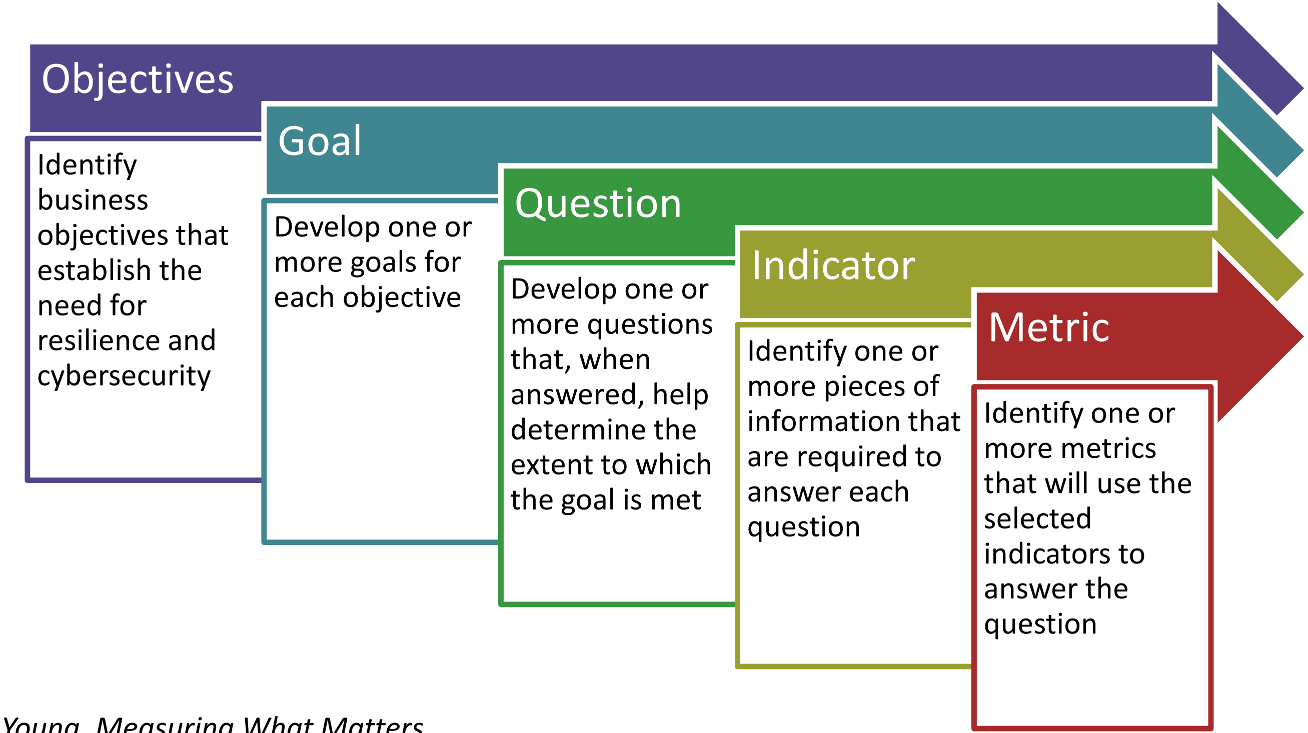
Grouped by host, OS or application

List of vulnerabilities in your environment

Our philosophy



Step 1 – define your requirements



Objectives

Identify business objectives that establish the need for resilience and cybersecurity

Goal

Develop one or more goals for each objective

Question

Develop one or more questions that, when answered, help determine the extent to which the goal is met

Indicator

Identify one or more pieces of information that are required to answer each question

Metric

Identify one or more metrics that will use the selected indicators to answer the question

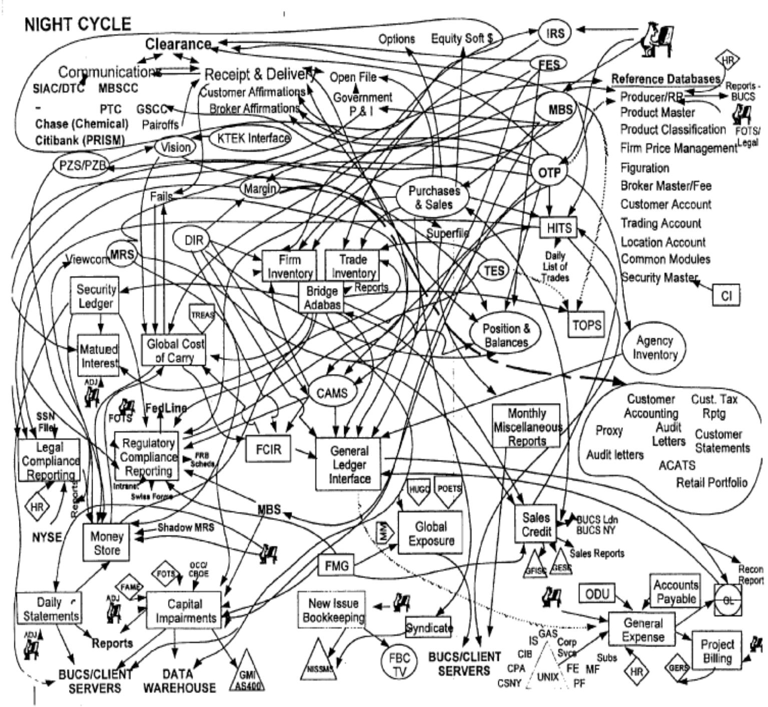
Source: Lisa Young, Measuring What Matters

Places to find "Goals"

- Security strategy
- Risk Register
- Audit/Controls
- Policies
- Executive's questions

Survival tip #2

Step 2 - Searching for data sources



Potential sources

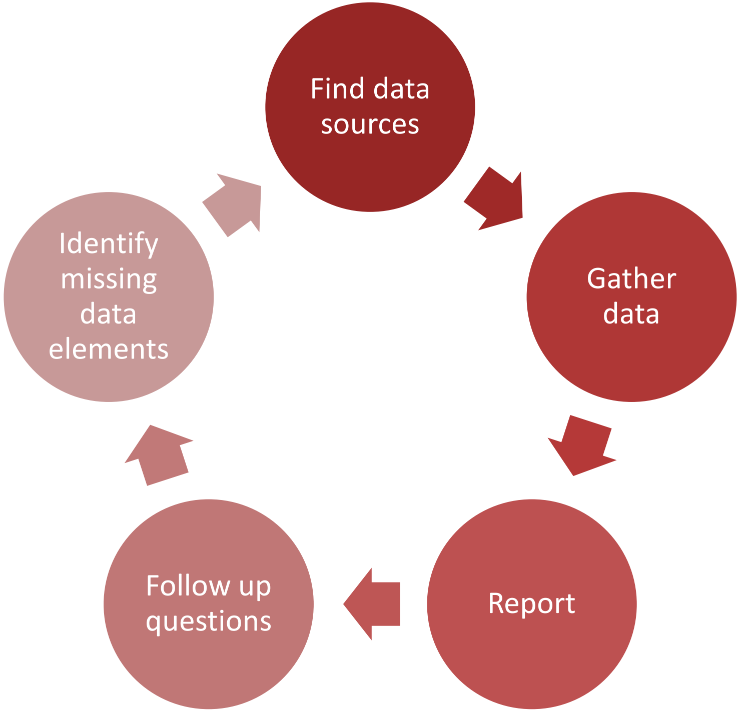
- Process bi-products
- Technologies assets interact with
- Peripheral processes
- External sources

- **Don't need an inventory**

Step 3 - Choosing your data source

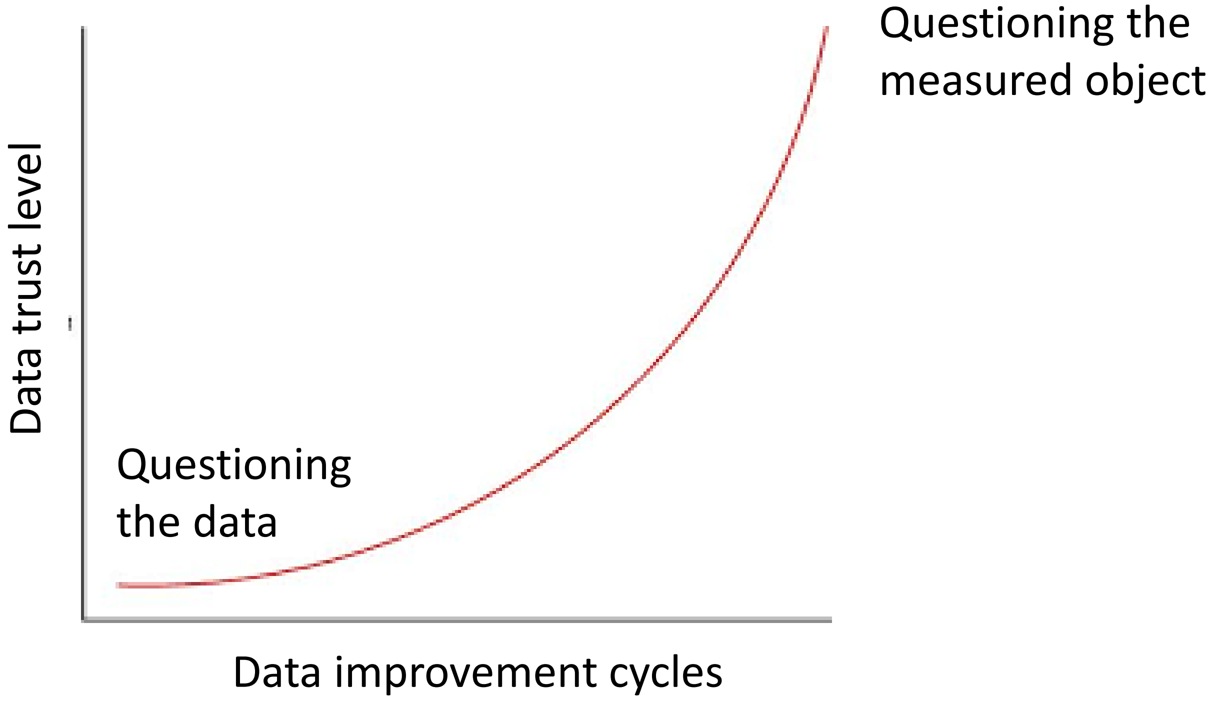
- Aspects to consider
  - Automatic vs manual
  - Ownership/source
  - Does it align with other sources? Use a common dictionary?
  - Completeness
  - Data variability
  - Refresh frequency
  - Does it contain stale/old data

Progressive data improvement



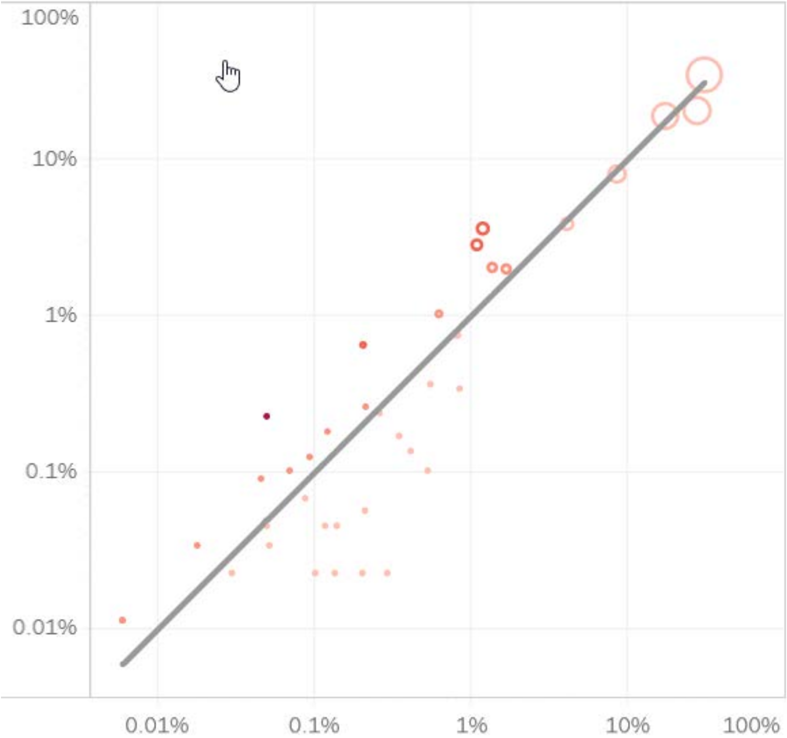
Survival tip #3

Trust curve


Questioning the measured object
Data trust level
Questioning the data
Data improvement cycles

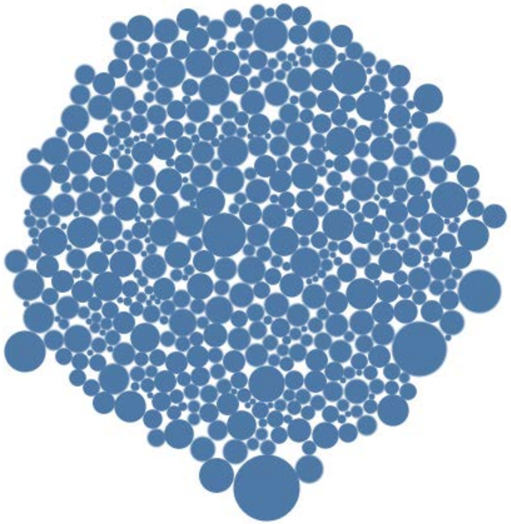
Step 4 - Analyze

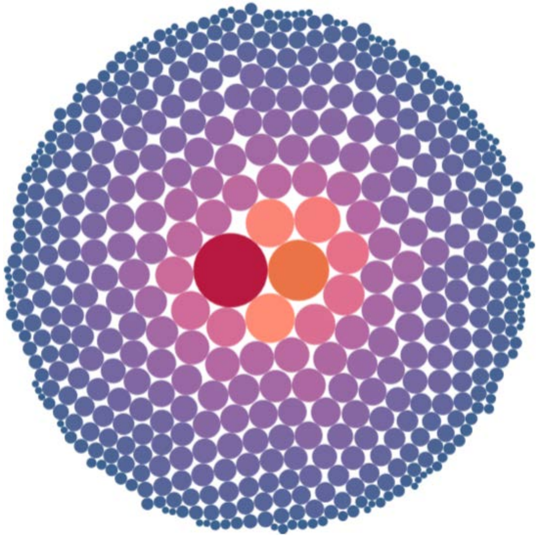
- Don’t need tools
- Needs to be repeatable
- Agreed upon approach
- Analyze deeper than needs to be presented
- Complexity of metrics



Step 5 – Communicate / Present

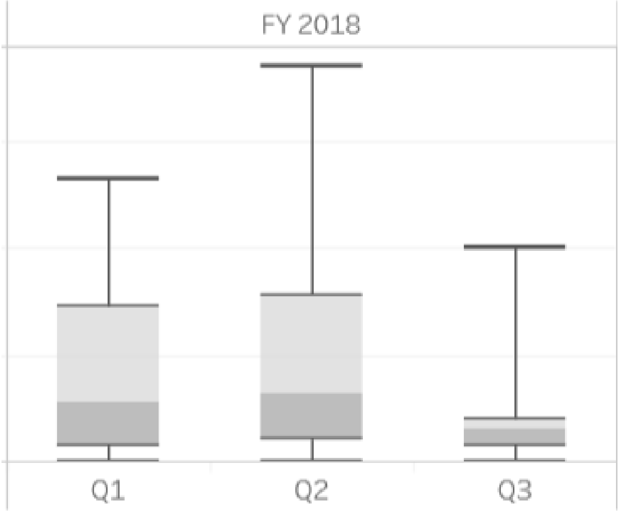
Draw attention to the most relevant items

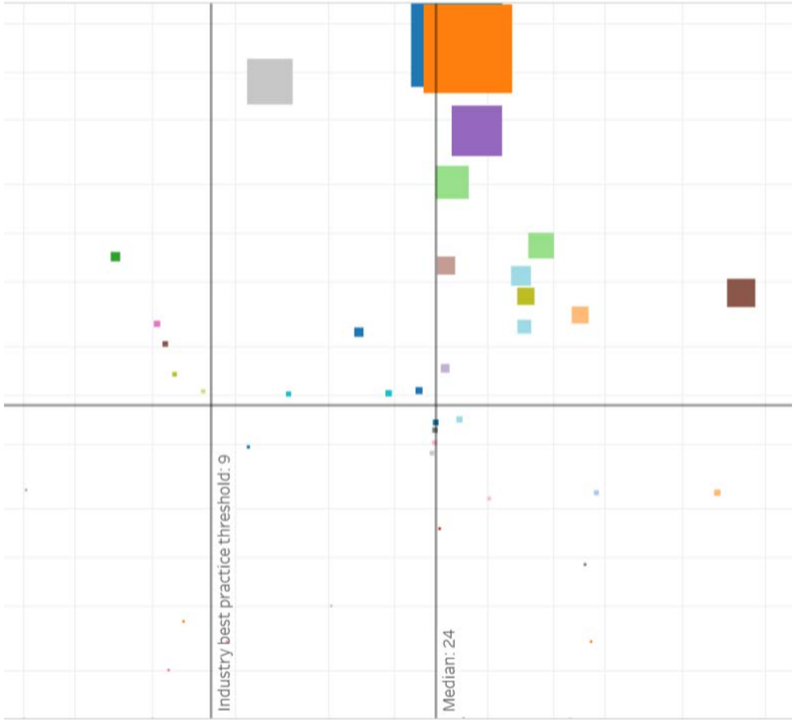




Step 5 – Communicate / Present

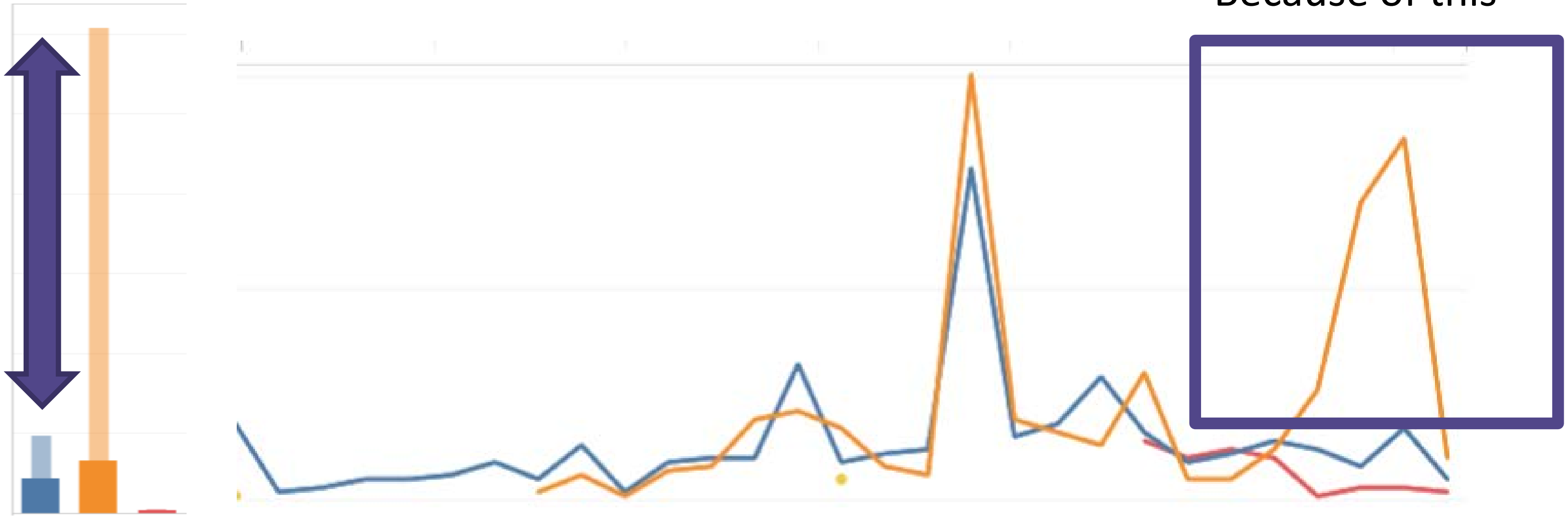
Use familiar formats and charts





Step 5 – Communicate / Present

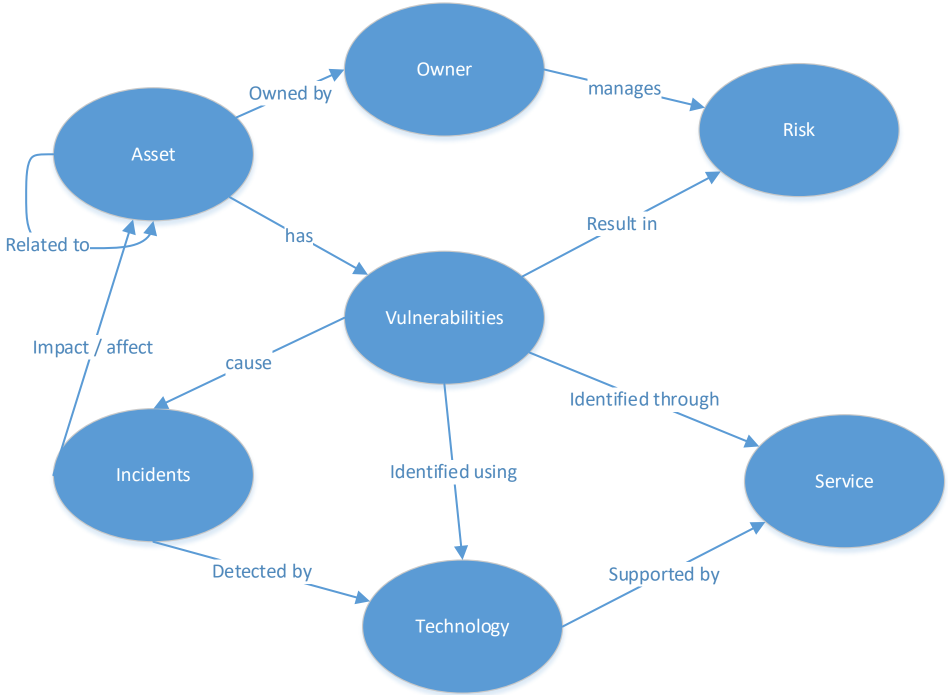
Repeated colors and patterns



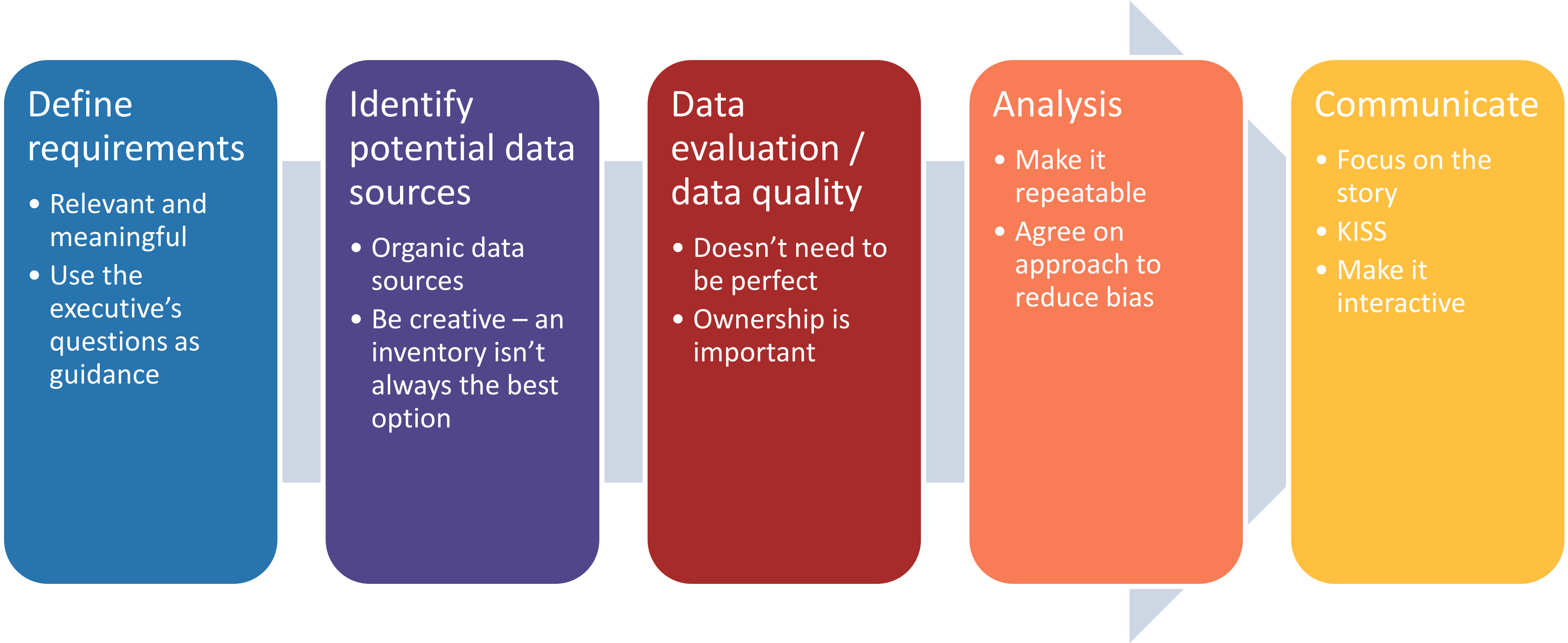
Why?

Because of this

Relationship between data sources



Recap on 5 steps



Define requirements

- Relevant and meaningful
- Use the executive's questions as guidance

Identify potential data sources

- Organic data sources
- Be creative – an inventory isn't always the best option

Data evaluation / data quality

- Doesn't need to be perfect
- Ownership is important

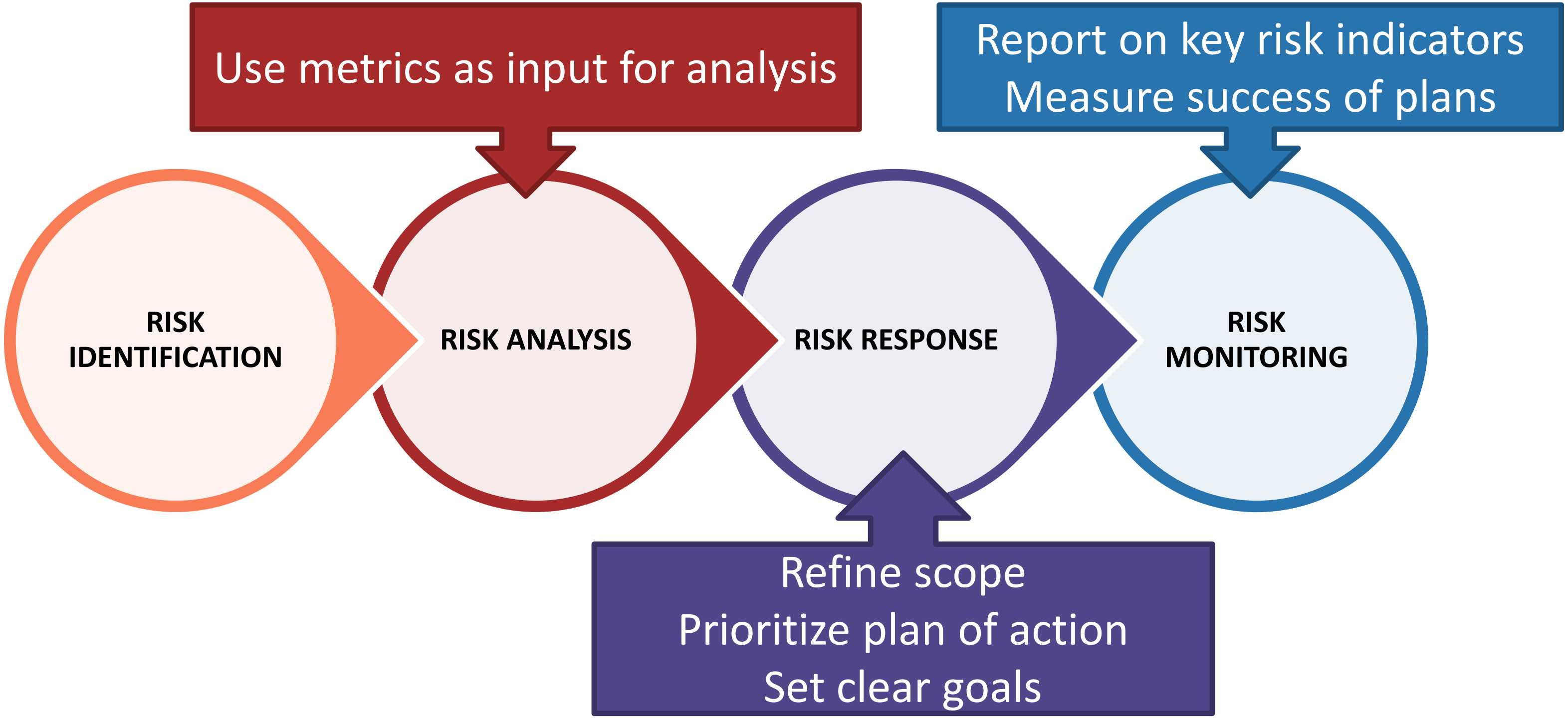
Analysis

- Make it repeatable
- Agree on approach to reduce bias

Communicate

- Focus on the story
- KISS
- Make it interactive

Integration with Risk framework



Use metrics as input for analysis

Report on key risk indicators
Measure success of plans

Refine scope
Prioritize plan of action
Set clear goals

What is next

- Continue adding more data points and reports
- Leverage reports to drive change in the organization (and measure that change)
- Leverage metrics as inputs to FAIR analysis
- Reduce operational overhead of maintenance

Apply it

Next week you should:

- Identify one of your organizational goals

In the first three months following this presentation you should:

- Define your reporting requirements for that goal
- List potential data sources for your metrics, obtain a sample and compare them to select one

Within six months you should:

- Use the data to answer the following questions:
  - Is my organization achieving this goal?
  - If not, what should I focus on first to get closer to it?

References and Resources

- Lisa Young, Measuring what matters; https://www.rsaconference.com/writable/presentations/file_upload/grc-r05_measuring_what_matters.pdf

Any questions?

James Lugabihl

James.Lugabihl@adp.com

Marta Palanques

Marta.Palanques@adp.com