



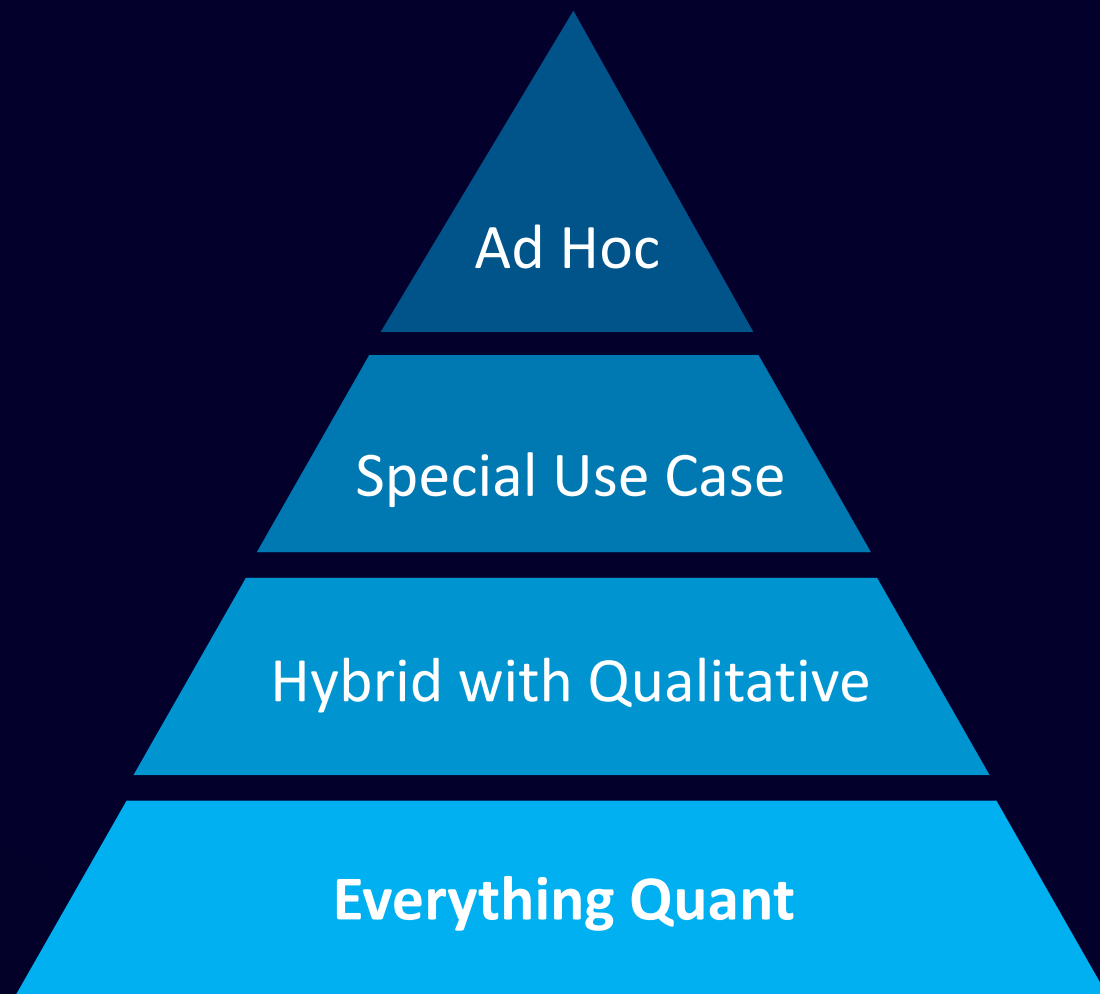
Building a quantitative Cyber Risk Program Based on FAIR

02.24.2024

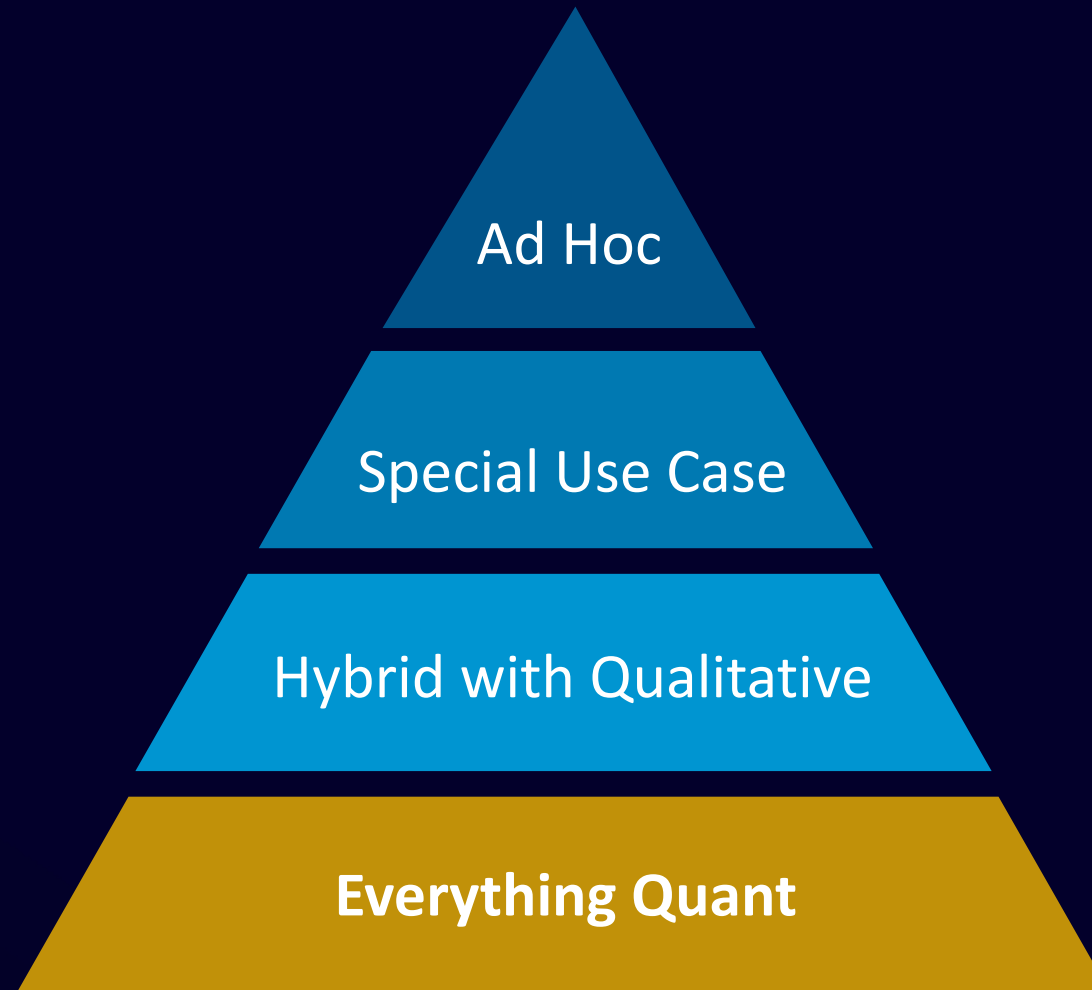
Tyler Britton
Cyber Risk Quant Manager, Dropbox



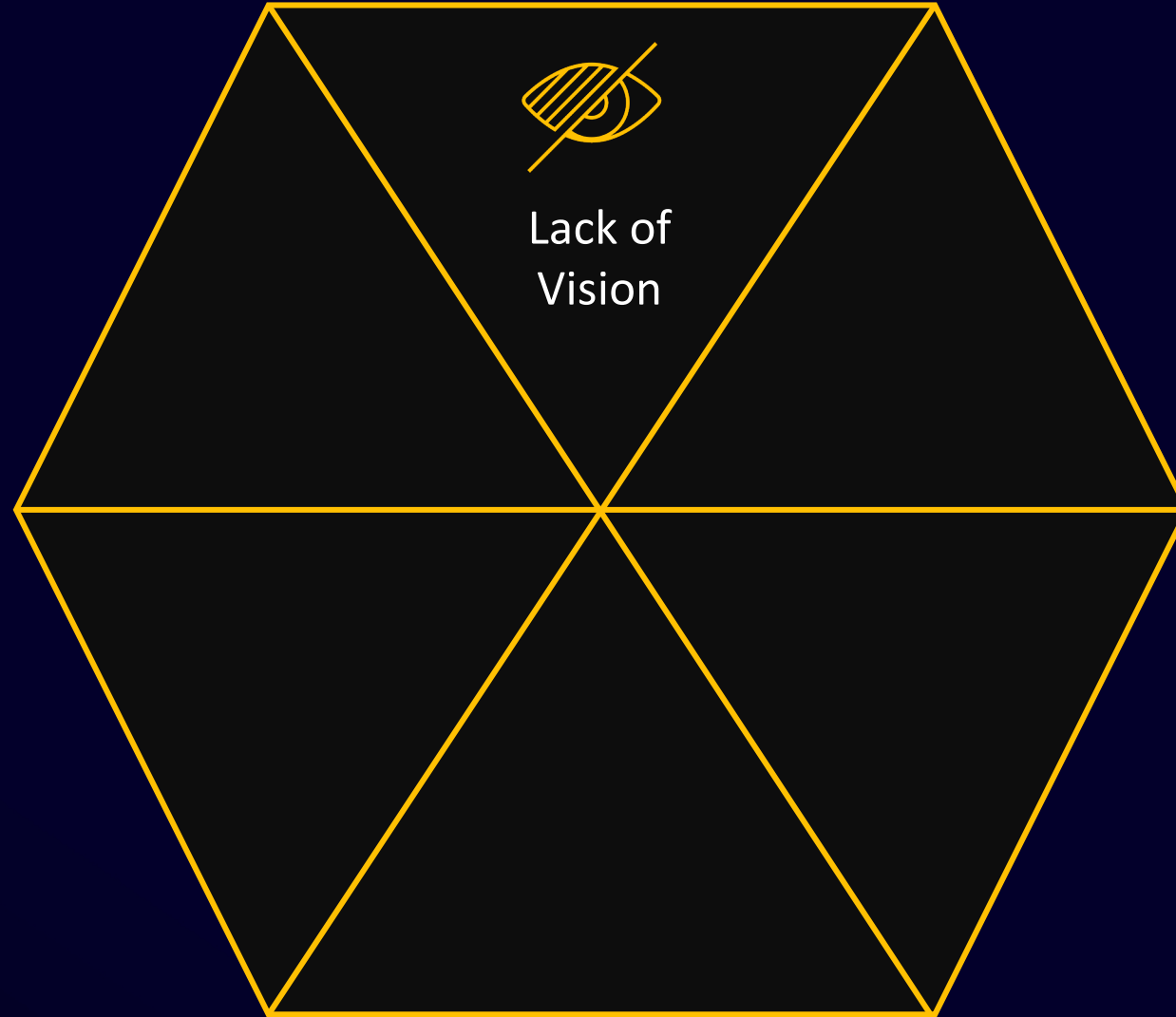
What is a CRQ (FAIR) Program?



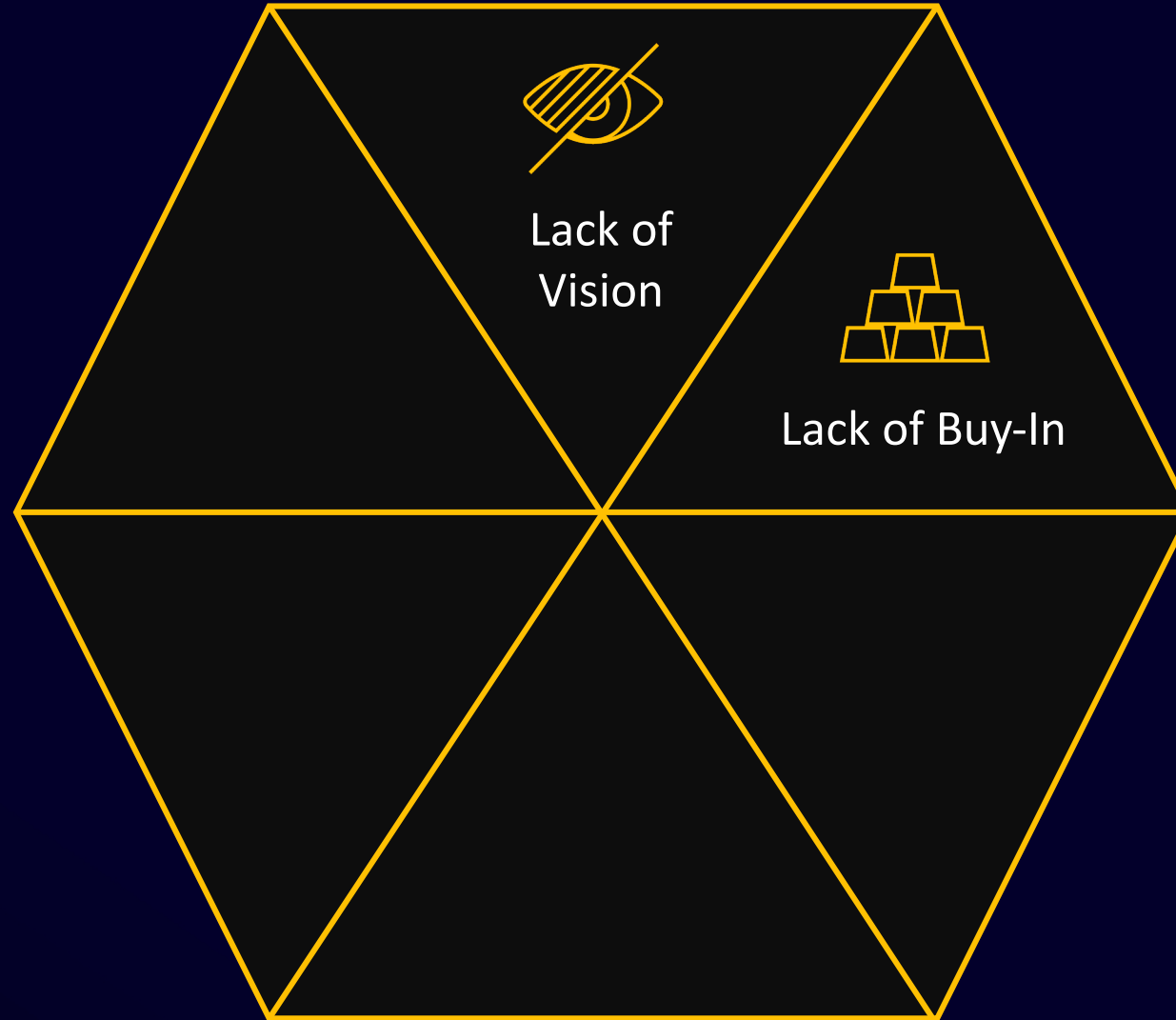
What is a CRQ (FAIR) Program?



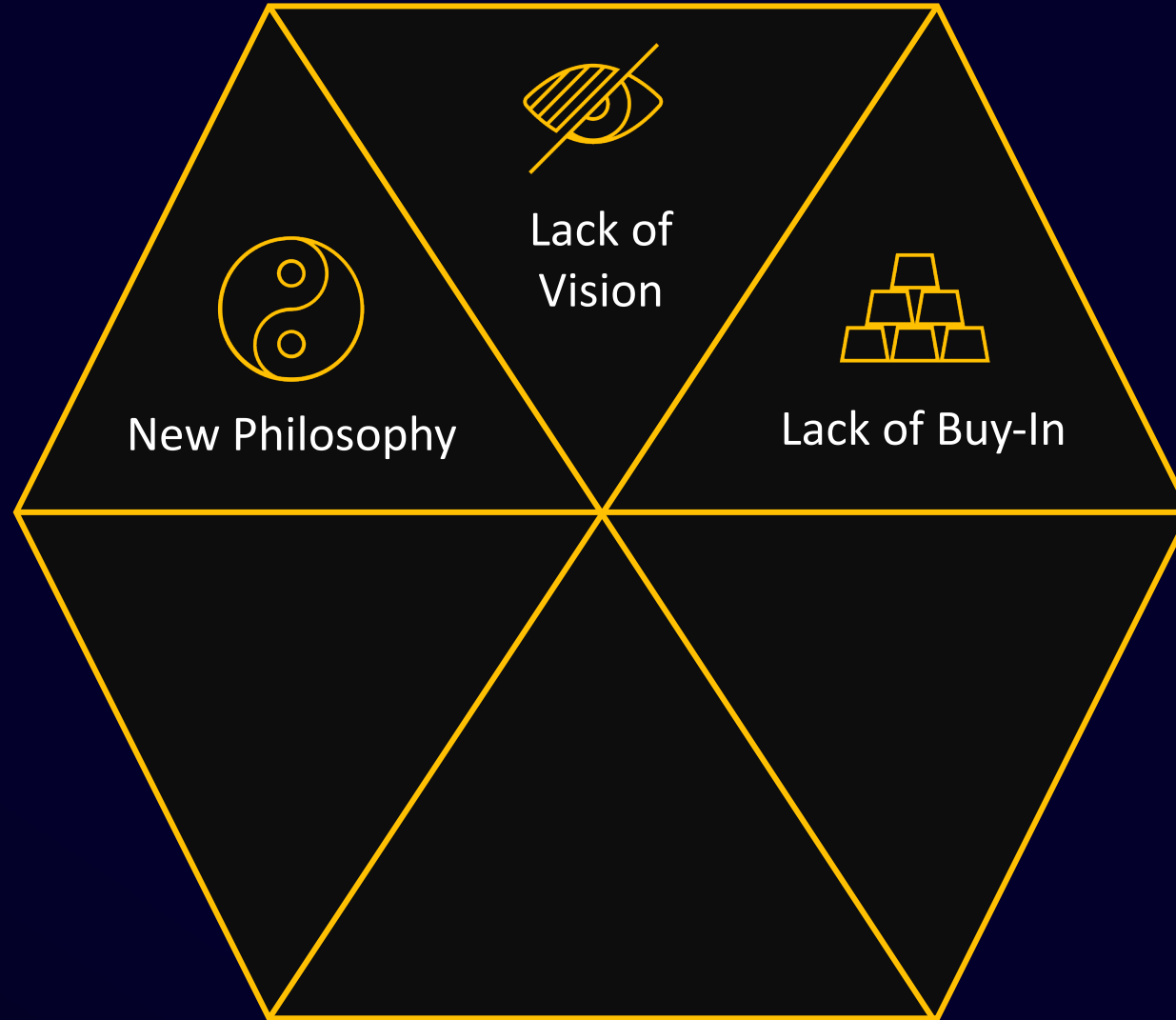
Challenges of Building



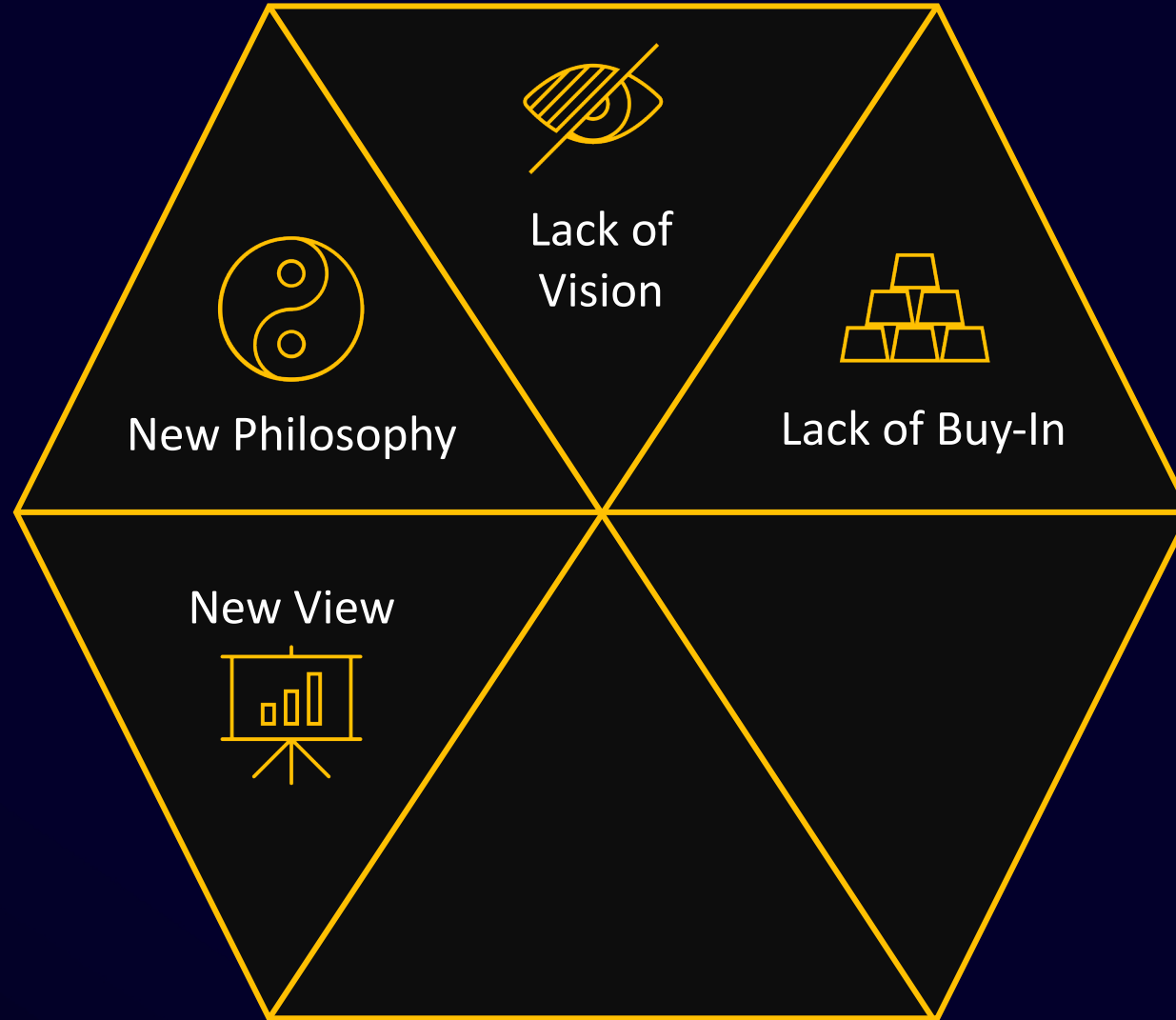
Challenges of Building



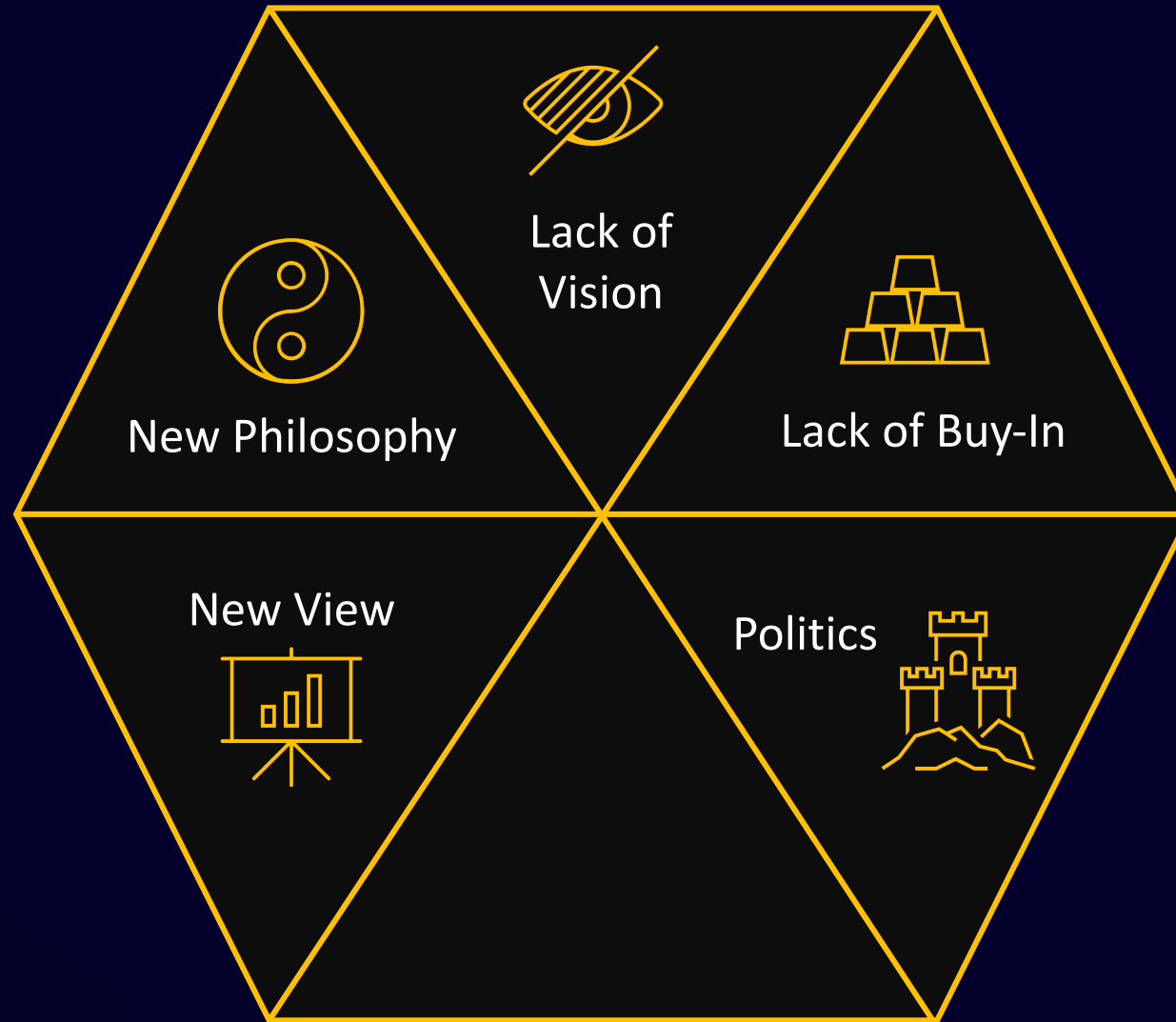
Challenges of Building



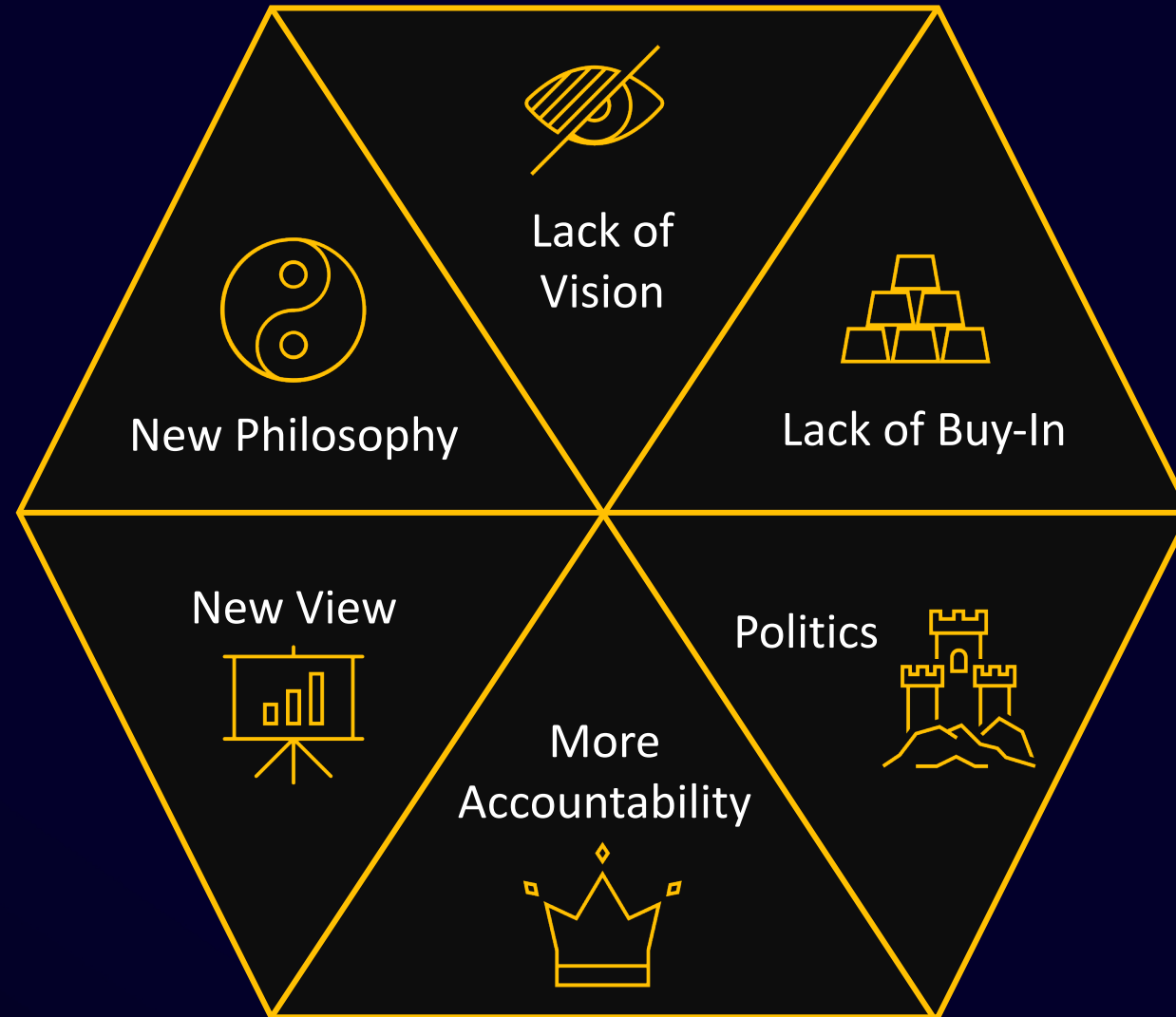
Challenges of Building



Challenges of Building



Challenges of Building

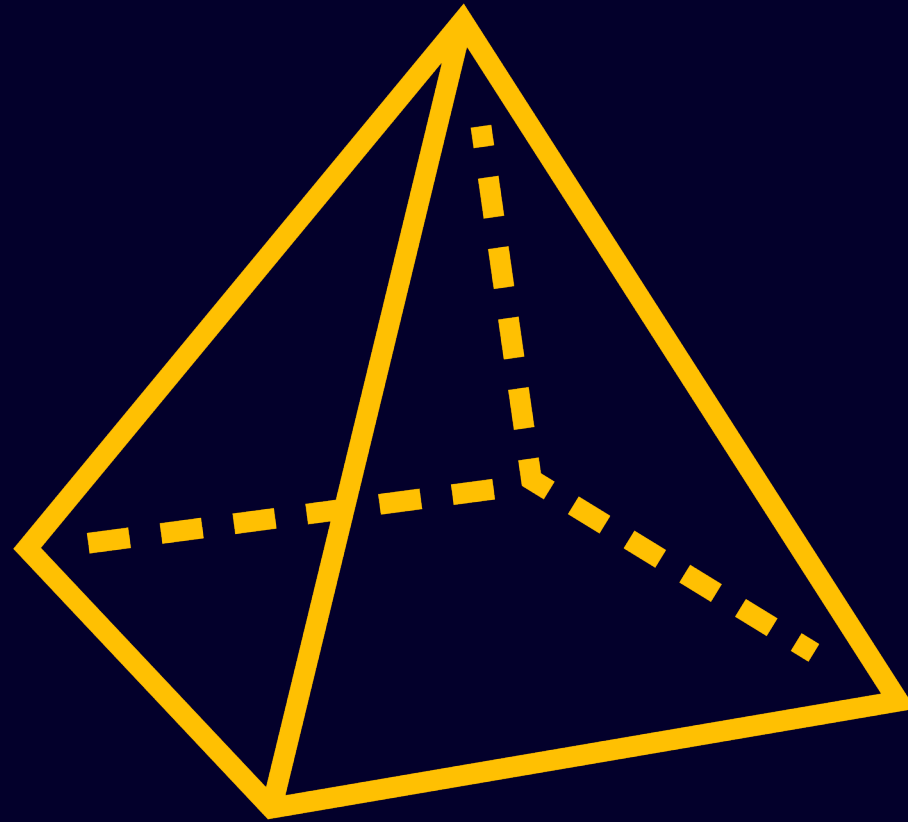


Challenges of Building



These challenges will exist whether you do things “right” or “wrong,” but having an effective and thoughtful approach to building a FAIR program makes these challenges speedbumps rather than insurmountable roadblocks.

The 3 Segment Approach to Building a FAIR Program



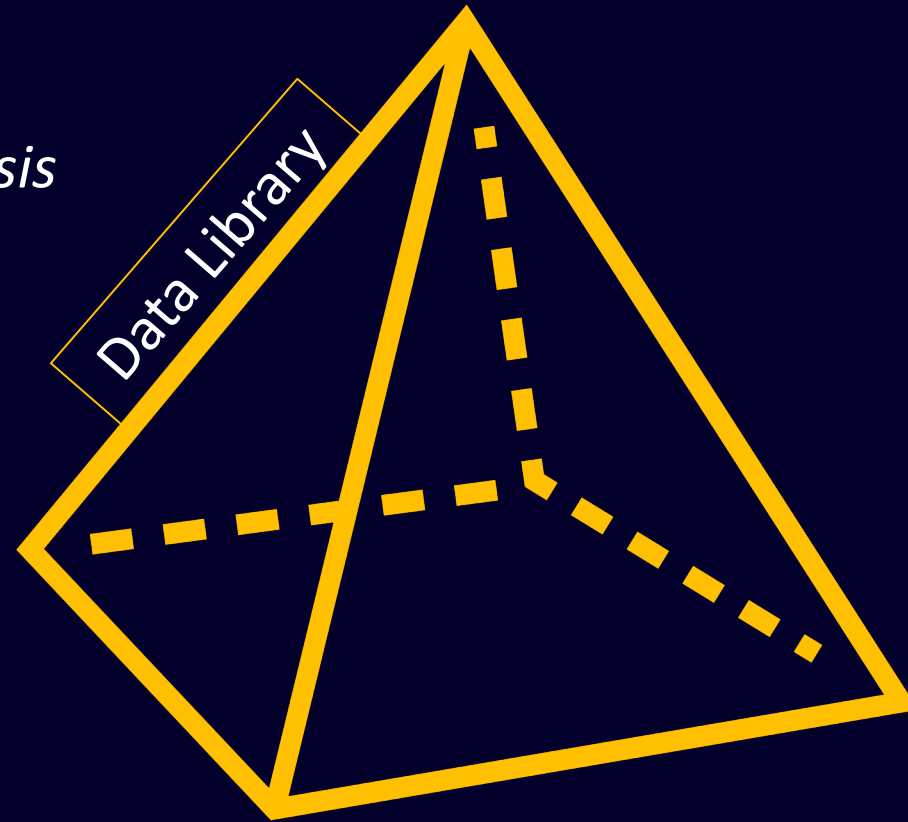
3 Se



Without all edges,
the program will
eventually fail.

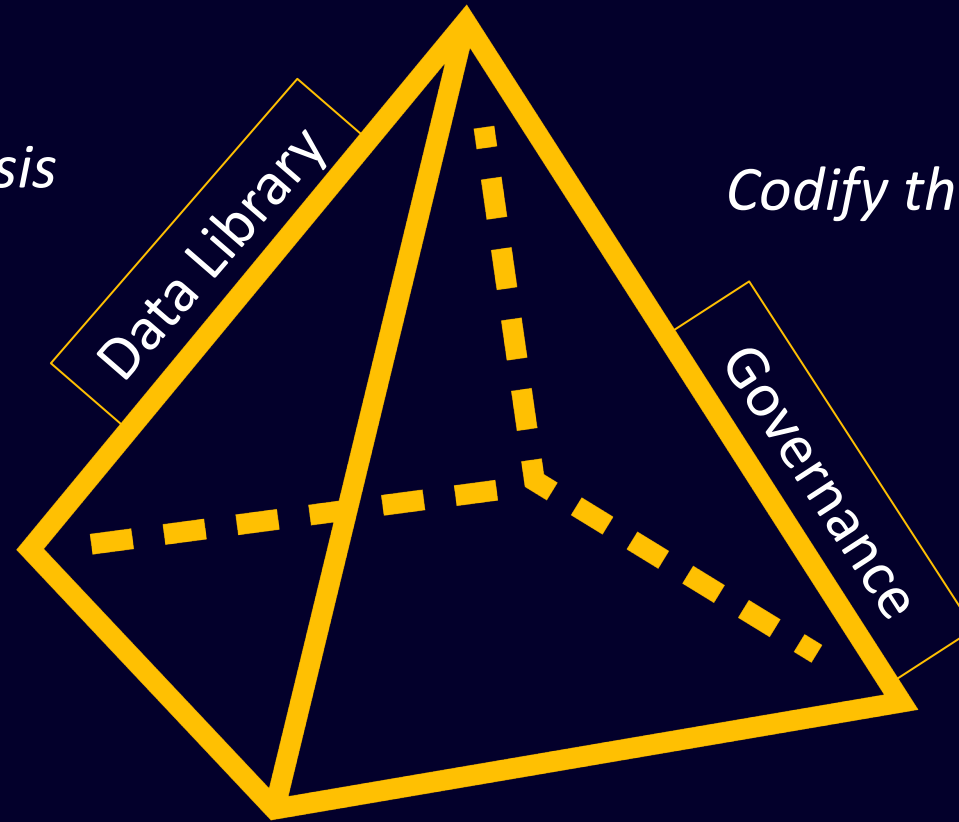
3 Segments of a CRQ Program

Information to drive analysis



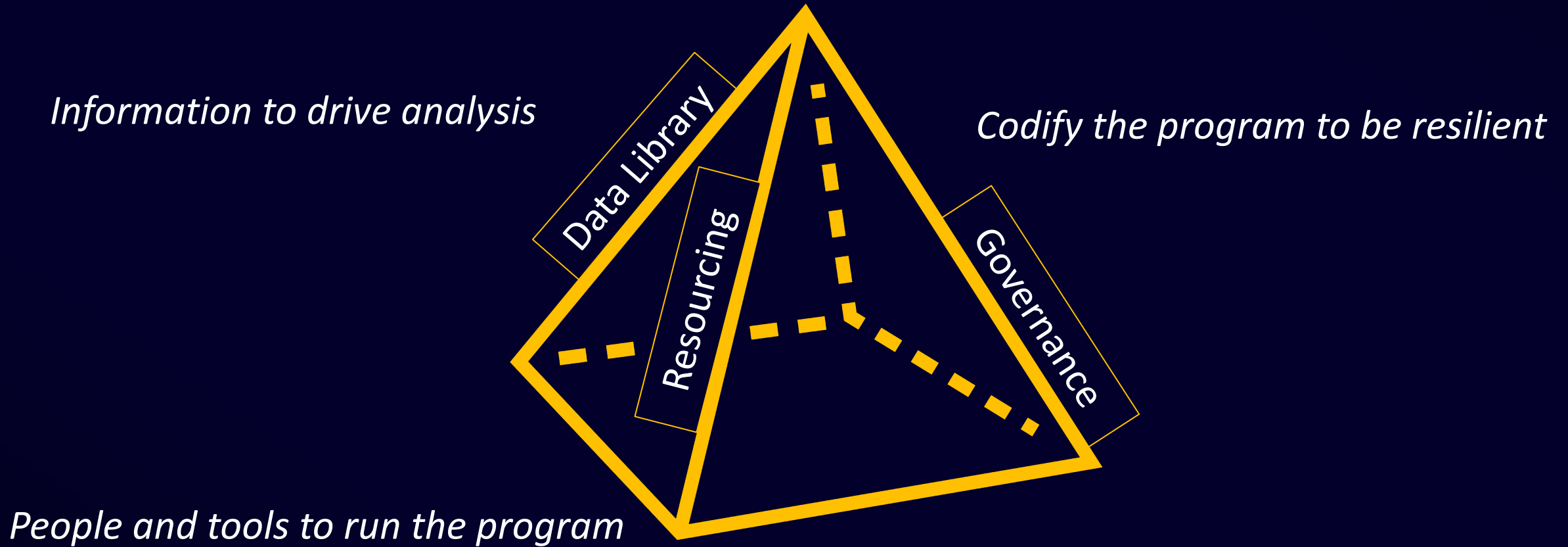
3 Segments of a CRQ Program

Information to drive analysis

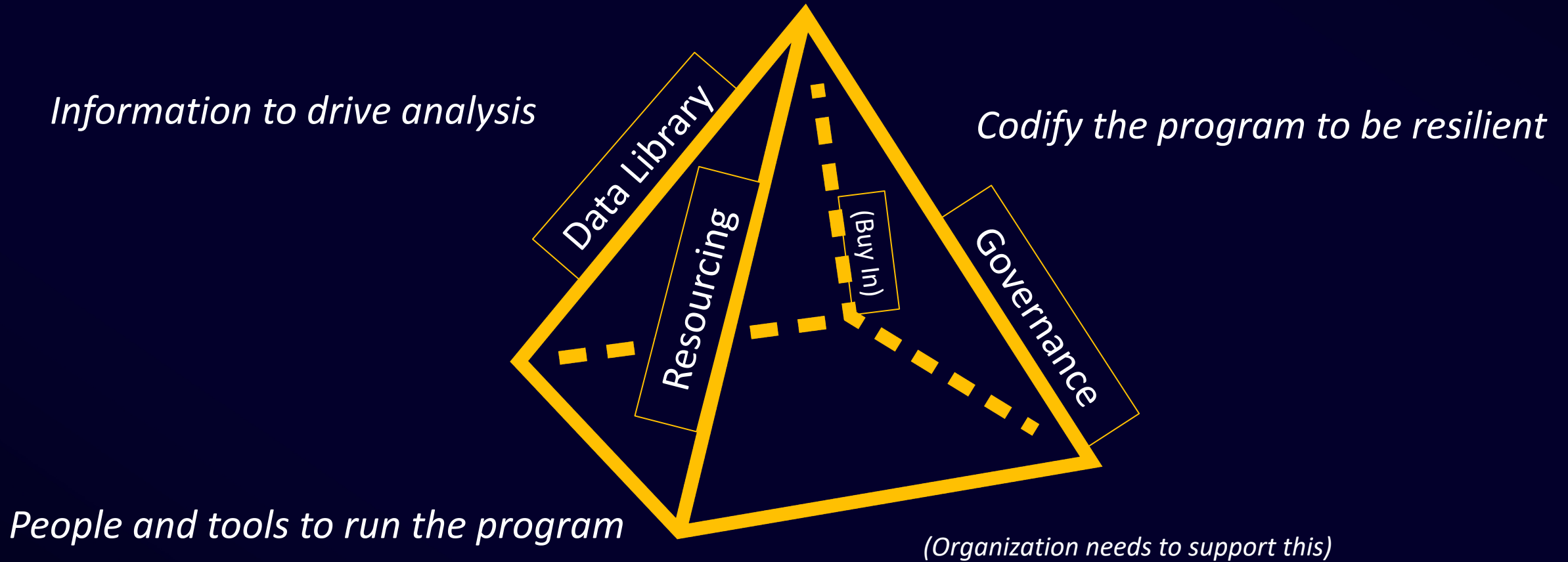


Codify the program to be resilient

3(1/2) Sides of a CRQ Program

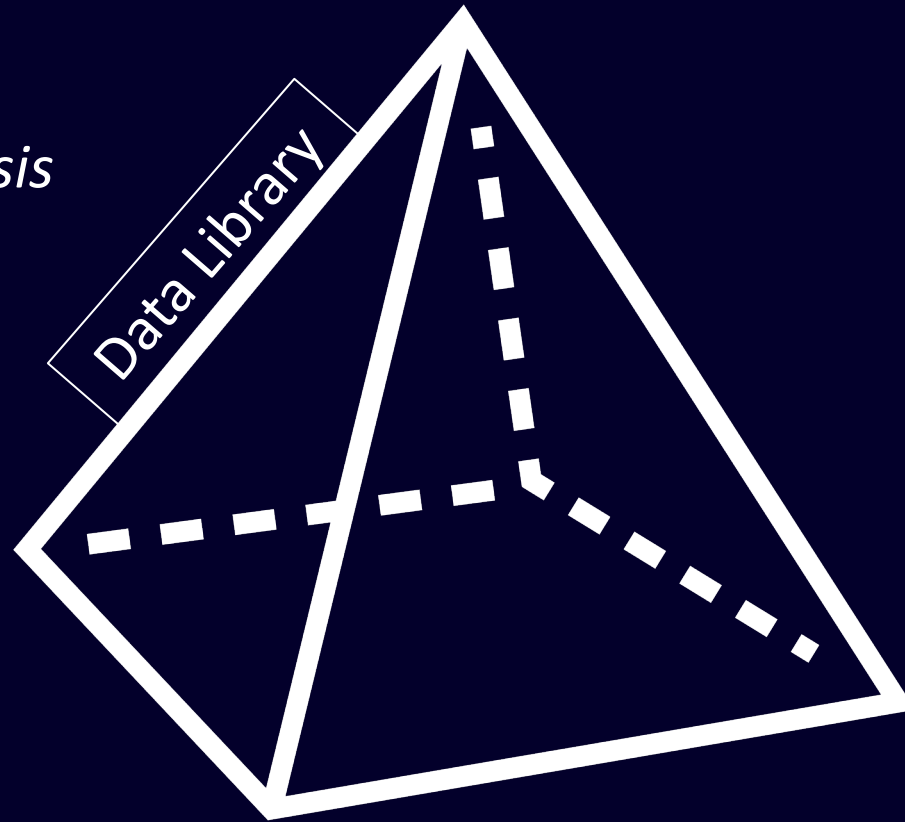


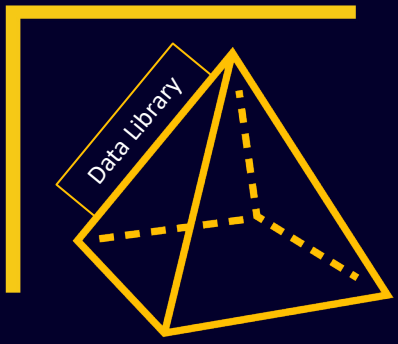
3 Segments of a CRQ Program



Data Libraries

Information to drive analysis

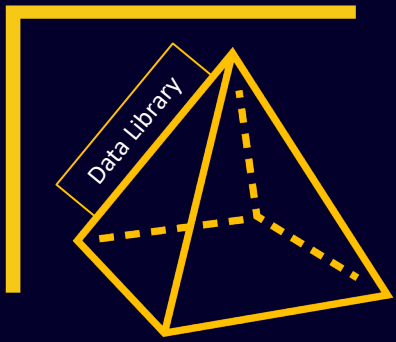




What are Data Libraries

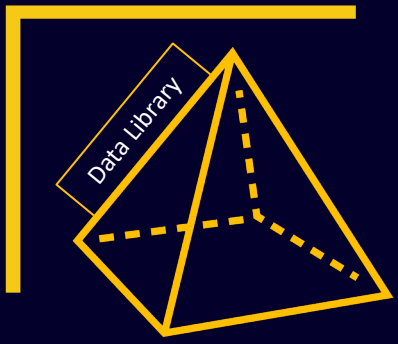
Repository of all information gathered from history, telemetry, SME estimates, SME rationale, and industry benchmark, that are organized in a meaningful and useful way manner





Goals of Data Libraries





Why Data Libraries

Collect once, and then monitor, rather than recollecting each analysis.

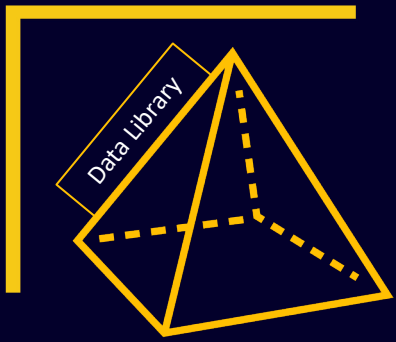
“More data selection, less collection”

Ensure that data is collected by the right SMEs.

“Always have Obi Wan’s force ghost in the room”

Be crystal clear on data you *have* vs what you *assume*.

“To know thyself is the beginning of wisdom”



How to Build Data Libraries

Question

Identify all of the contextual questions: *what do we need to know?*

- Incident metrics
- Control efficacy
- Fines per outage/breach
- Customer churn per breach/outage
- Breach response costs

...and so on

Context

Build data libraries based on attack model: *in what context should we collect data?*

- External actor footholds
- Ransomware
- Malicious insiders
- Churn at different loss severities
- Revenue loss per RTO

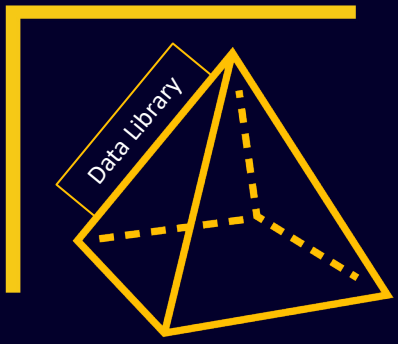
...and so on

Relevance

Identify critical assets and build data around those assets: *how can we collect meaningful data?*

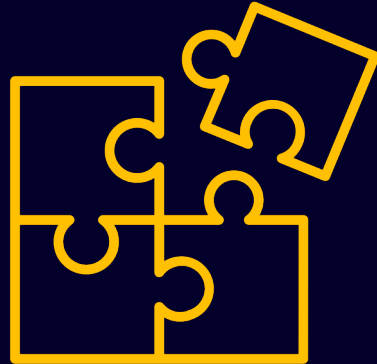
- Biggest repositories
- KTLO business processes
- Critical secrets
- Critical pipelines (ie CI/CD, manufacturing)
- Key customer apps

...and so on

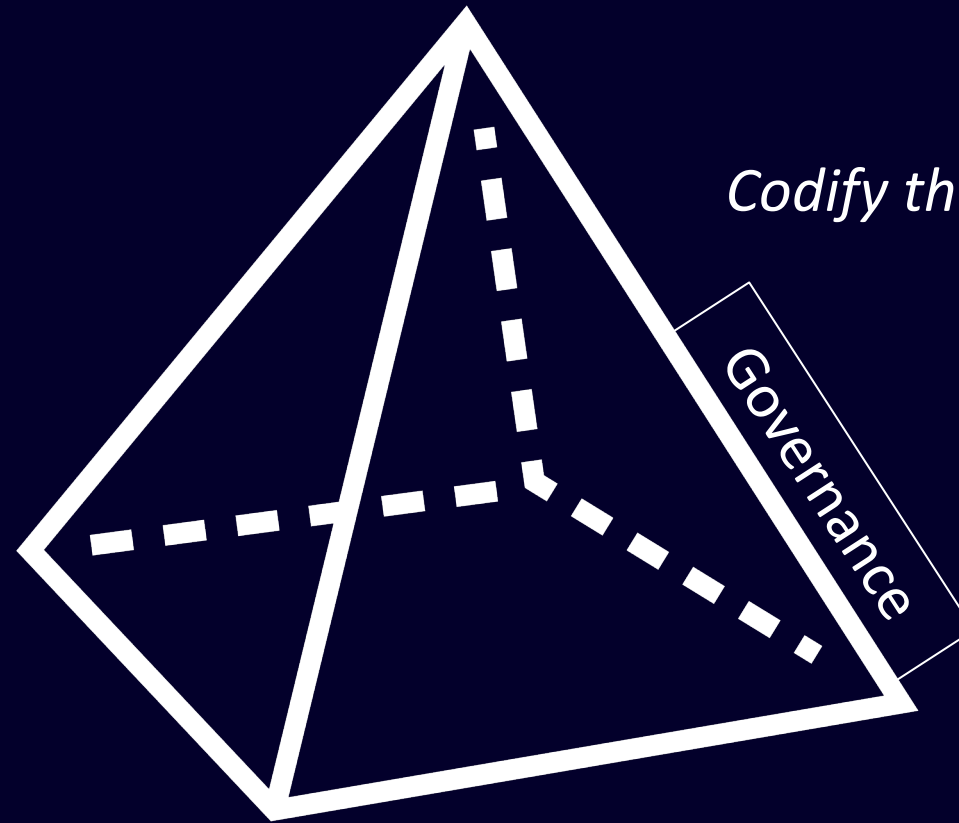


Data Library Outcome

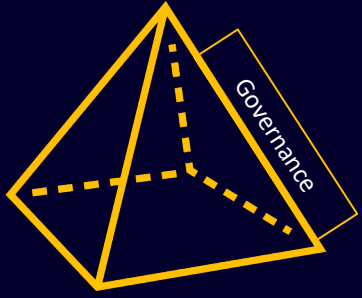
Stitch all available data together in meaningful ways



Governance



Codify the program to be resilient

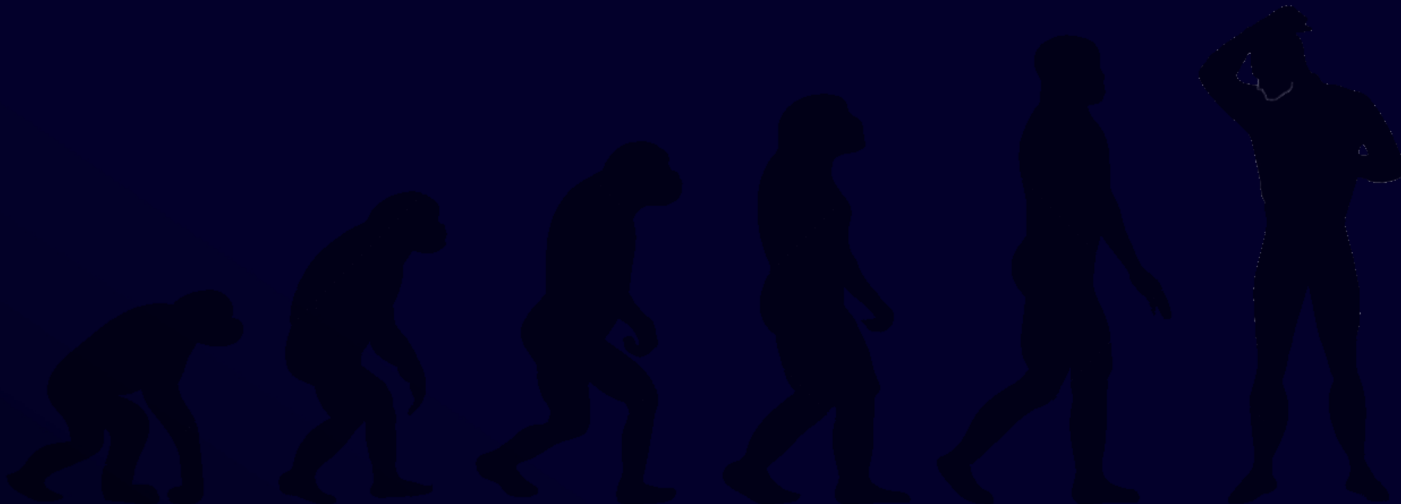


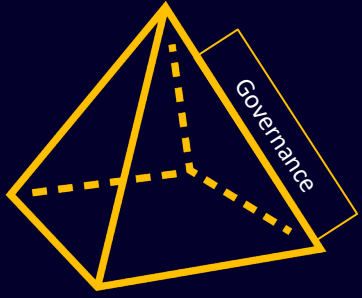
Goals of Governance

Program is depended
on a person



Program is depended
on the process





Must-Have Governance

Use-cases

Prescriptive guidelines on what circumstances we do analysis work

Ownership

Have an ownership model to be prescriptive on what happens with results – the 'so what' factor

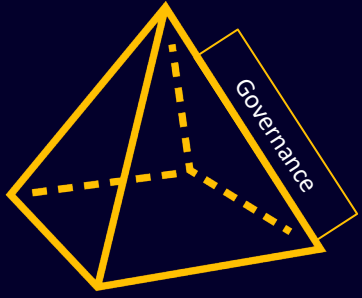


Processes

A comprehensive process for how FAIR analysis is conducted

Roles/Responsibilities

Have clear boundaries on who is responsible for what in the program

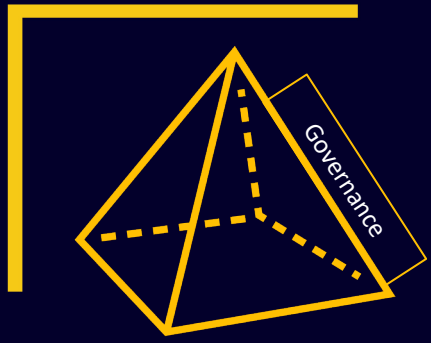


How to Create Governance

Build simple
process to
service use-
cases

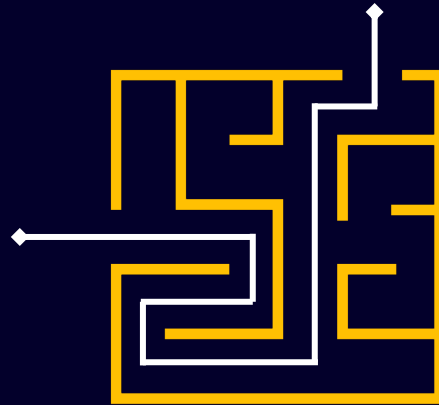
Clarify NEEDS,
build use-cases

Be
prescriptive
on
expectations

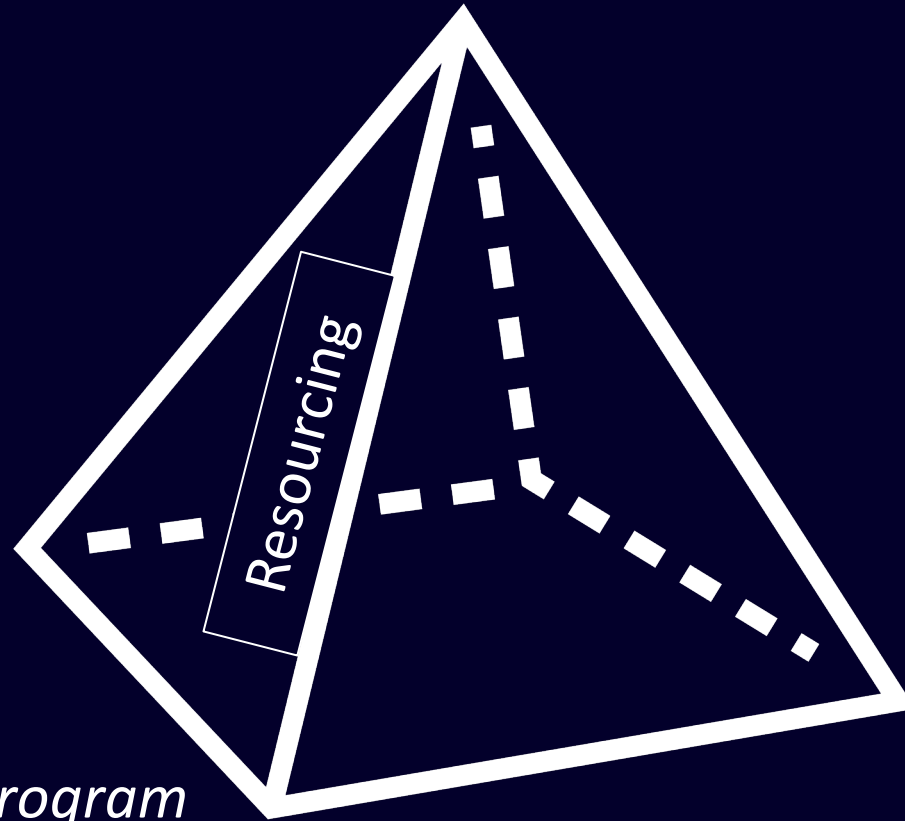


Governance Final Products

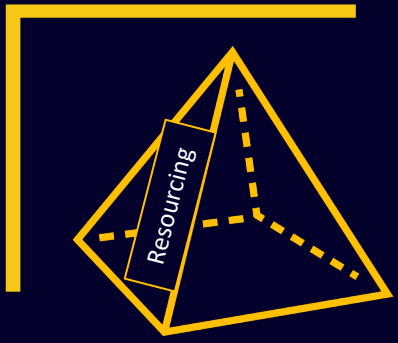
Organize the messy complexities of the real world



Resourcing



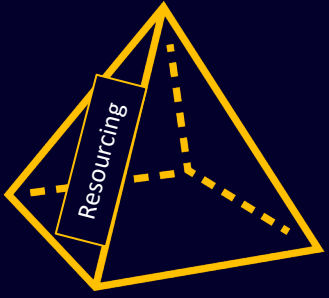
People and tools to run the program



Goals of Resourcing

Prevent the program from getting 'stuck'

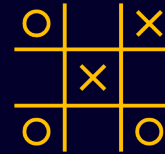




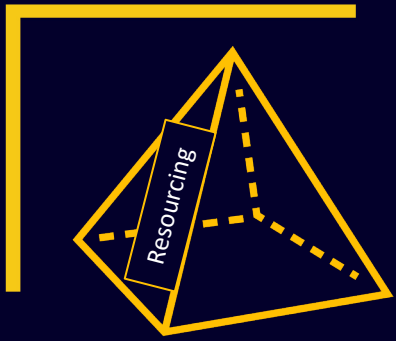
What is Resourcing



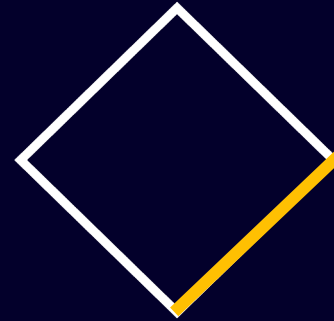
**Providing the people and tools
needed to run the program**



*You can have a field and a
playbook, but without players and
equipment there's no game*

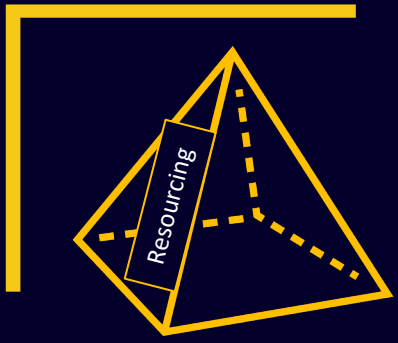


How to Resource



Provision People

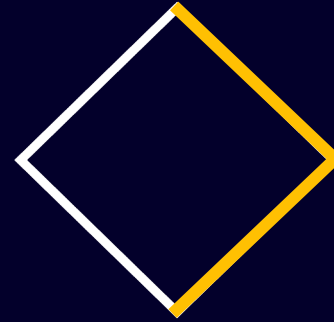
1-3 dedicated people to run the program, be it single use-case or all quant



How to Resource

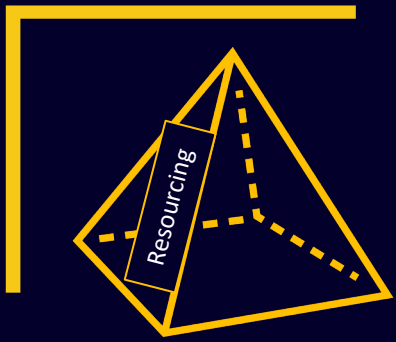
Provision Tooling

Software, registers, internal website
resources, simple intake mechanism



Provision People

1-3 dedicated people to run
the program, be it single
use-case or all quant



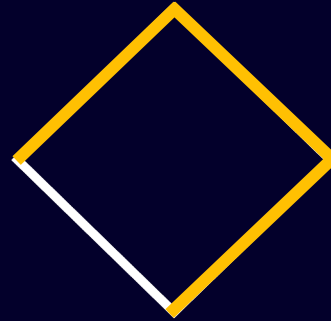
How to Resource

Provision Tooling

Software, registers, internal website resources, simple intake mechanism

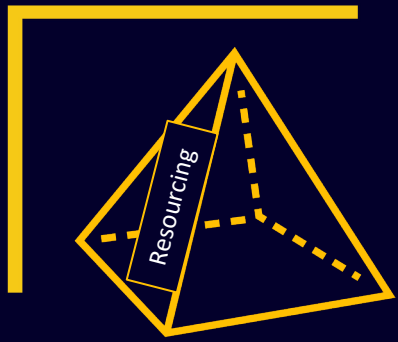
Provision Training

Short, topical videos for anyone to learn all they need to about FAIR in minimum time



Provision People

1-3 dedicated people to run the program, be it single use-case or all quant



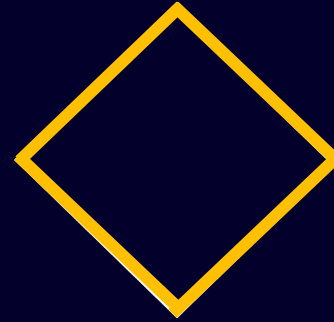
How to Resource

Provision Tooling

Software, registers, internal website resources, simple intake mechanism

Provision Training

Short, topical videos for anyone to learn all they need to about FAIR in minimum time

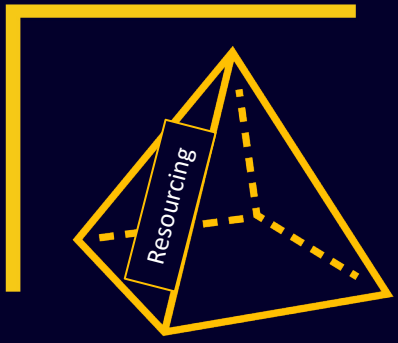


Provision People

1-3 dedicated people to run the program, be it single use-case or all quant

Provision End-Goal

Document very clear expectations about how the 'final product' should operate

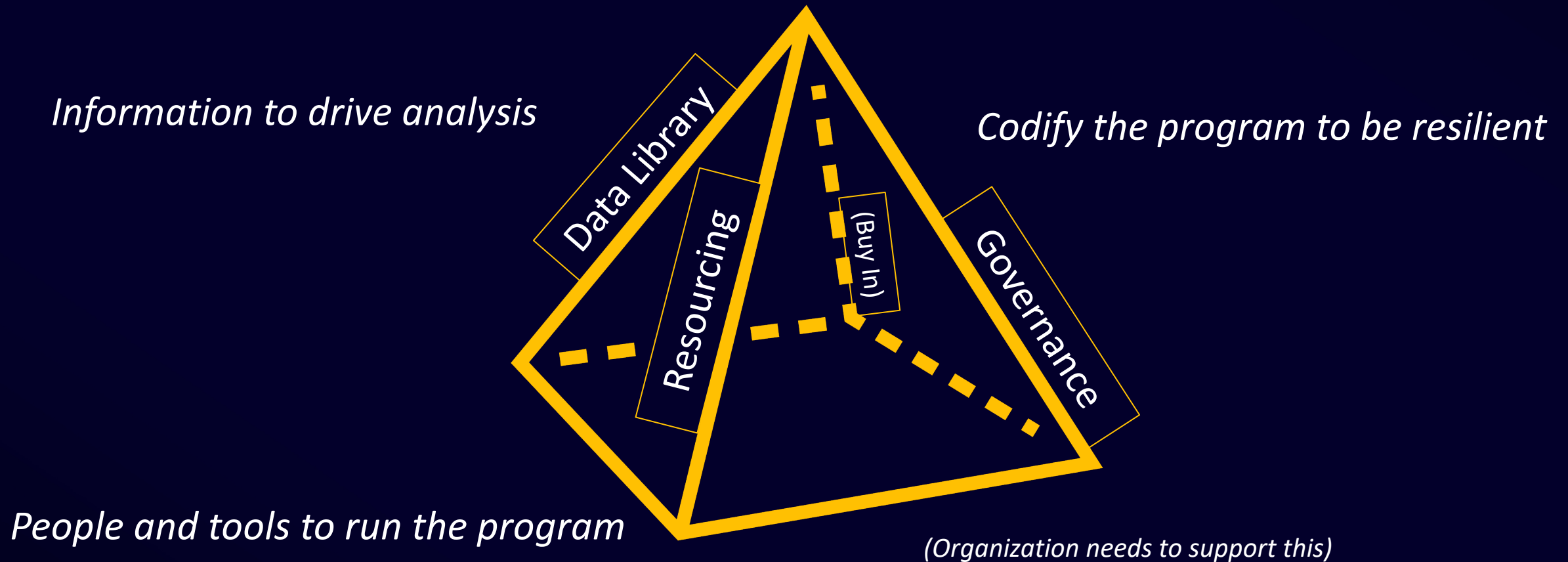


Resourcing Outcomes

An operational program



Bringing it All Together



Bringing it All Together

Data Library

Get the best available information from the right people to enable high quality, refined analysis in a short amount of time. Do this by collecting contextual information that is tied to key assets.

Governance

Codify your quant risk program in a document to ensure that your program is depended on the process and not a person. Key components that the governance document should outline are prescriptive use-cases, processes, ownership policy, and responsibility guidelines

Resourcing

Provide the people and tools needed to operationalize your program. These tools should enable people to perform analysis, track analysis, communicate results, train stakeholders, and manage the program towards a vision.



Thank you

Tyler Britton
tbritton@dropbox.com

