WHAT GOOD LOOKS LIKE - USING KPI'S, KCI'S AND KRI'S EFFECTIVELY

ROB CAMPBELL – ENTERPRISE SECURITY ARCHITECT

EMAIL – COSAC@ASSUREDCONTROL.COM

BENEFITS OF GOOD SECURITY METRICS

- Improve and prove your organisations security posture
- Identify and fix issues before they cause a problem
- Fix the cause rather than just treat the symptom
- Help make sure your controls work by proving it
- Secure by design is great but only if you can prove it is secure throughout the controls lifetime
- Enables strategy – after all how do you develop strategy if you don't know what needs doing?

WHAT ARE KRI'S, KCI'S AND KPI'S

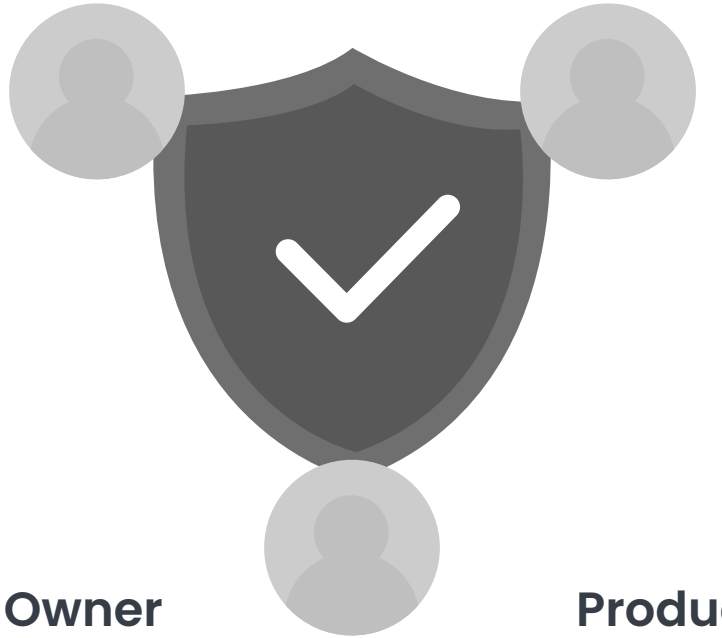
- KEY CONTROL INDICATORS – ARE WE IN CONTROL?
- KEY RISK INDICATORS – HOW IS OUR RISK PROFILE CHANGING AND IS IT WITHIN DESIRED TOLERANCES?
- KEY PERFORMANCE INDICATORS – ARE WE ACHIEVING OUR DESIRED PERFORMANCE LEVELS?

Who is your Audience

Metrics need to developed for the audience. This is where Business Attribute mapping and domain modelling comes in handy because these tell you what is important to the stakeholders you are targeting with the metrics.

Senior Stakeholders

- Are we protected against?
- You need to reduce cost. Find me x$.
- New regulation requires us to…?



CISO

- Are we managing the risk effectively?
- Where can we find savings without increasing risk?
- Am I getting value for money from x?

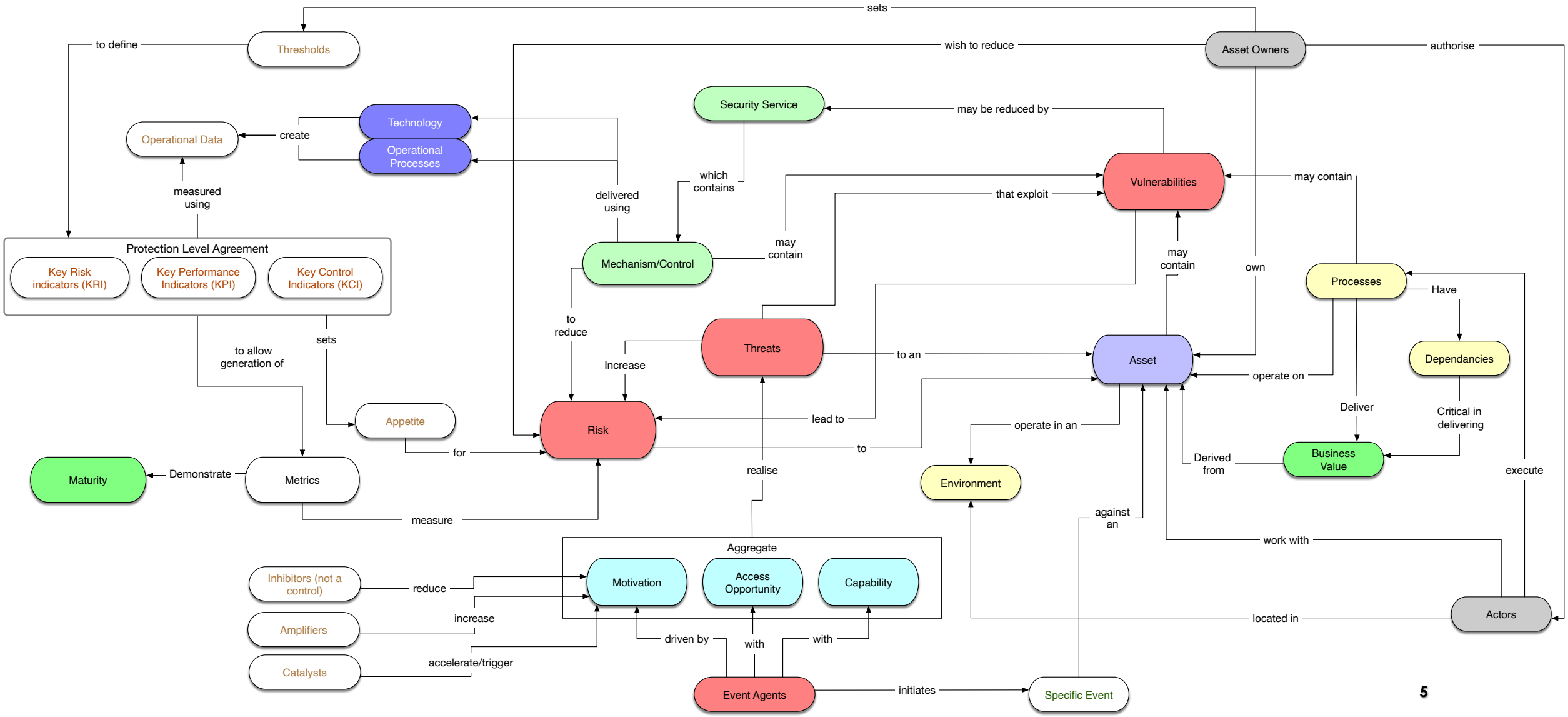
Capability or Service Owner

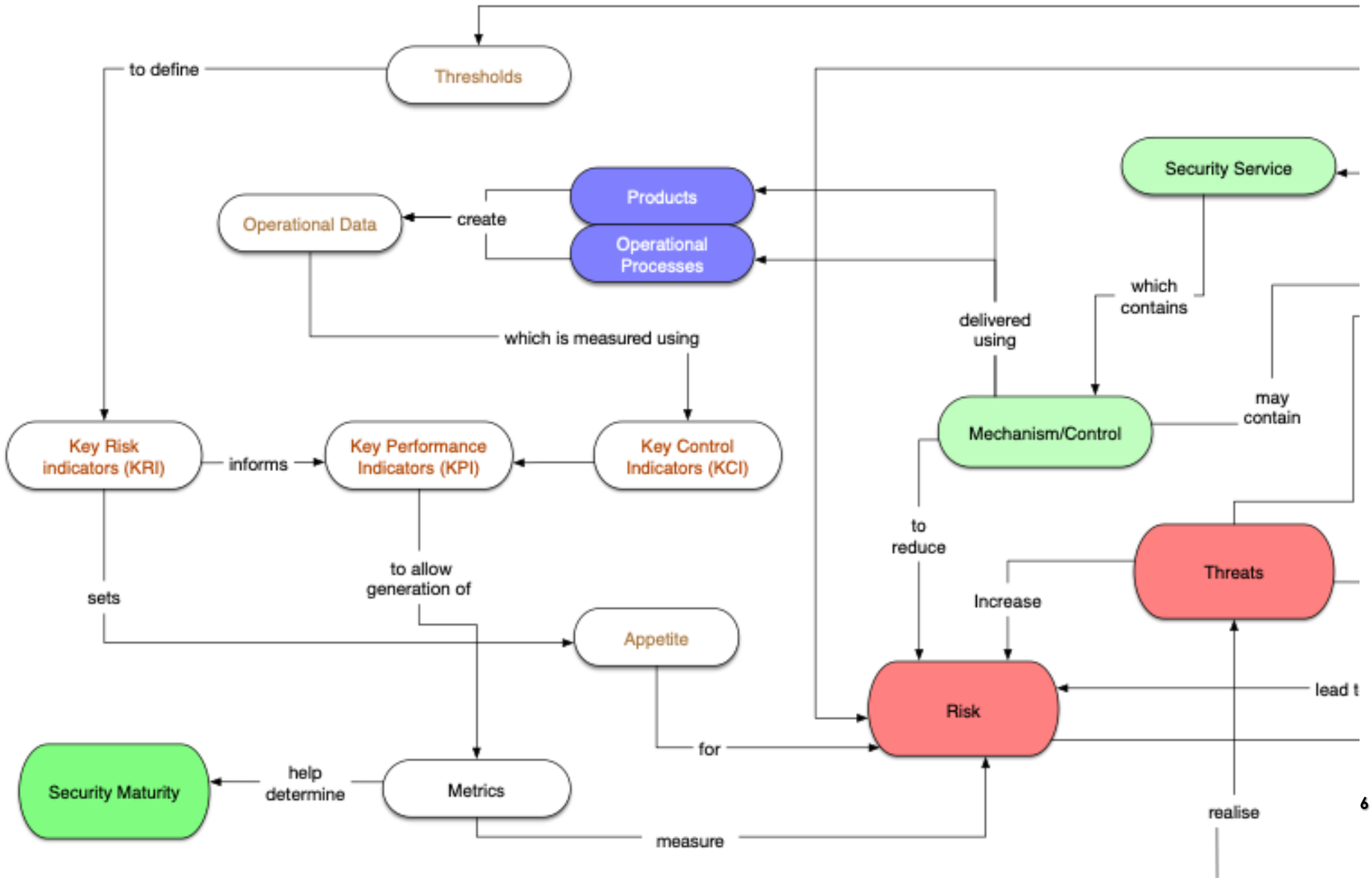
- Are all products performing as expected?
- Have we covered everything we need to?
- Do we have the right resource profile?

Product Owner

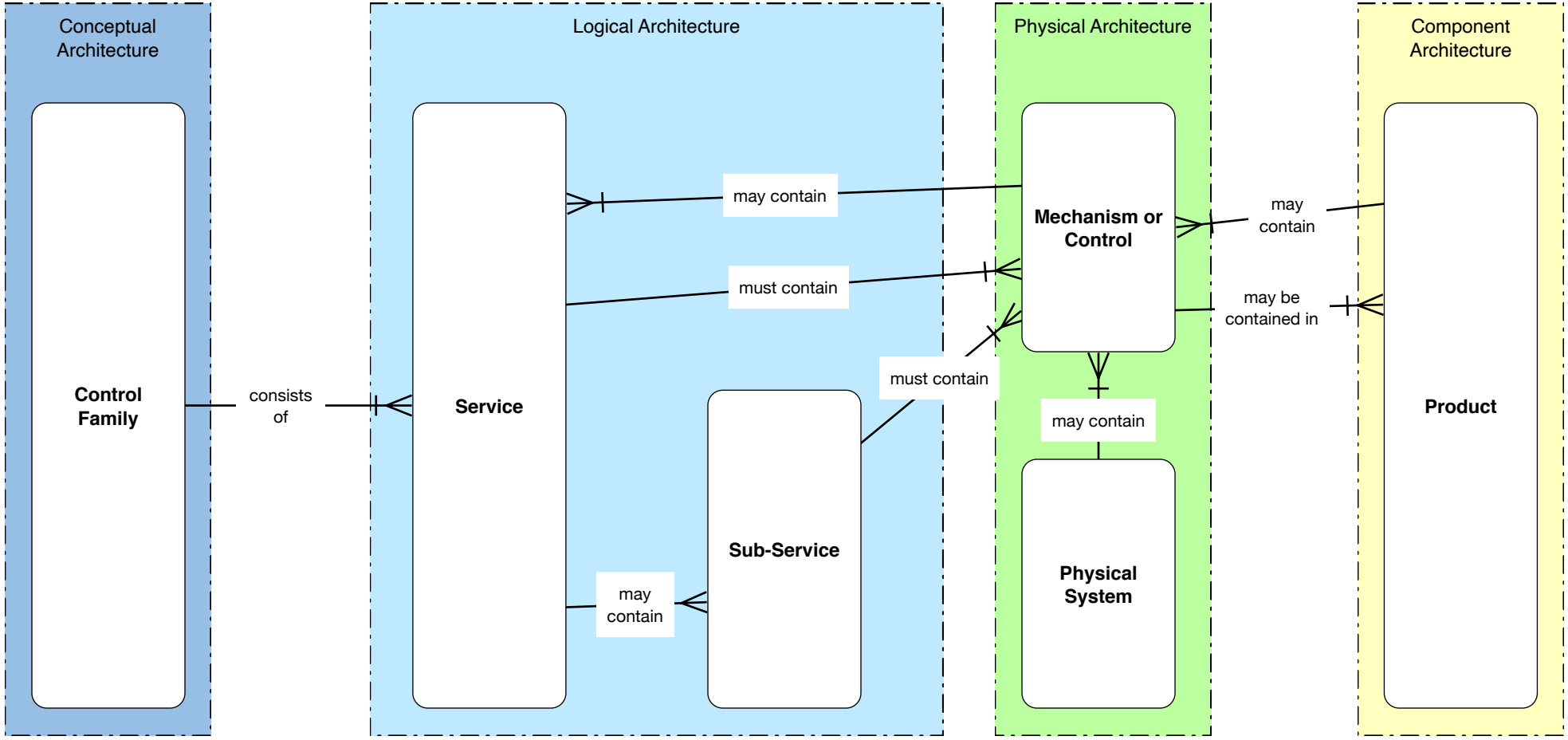
- Is it working?
- Do we have complete coverage?
- Are we up to date?
- Are we keeping up with faults and service requests?

Where do metrics fit within Risk Management?

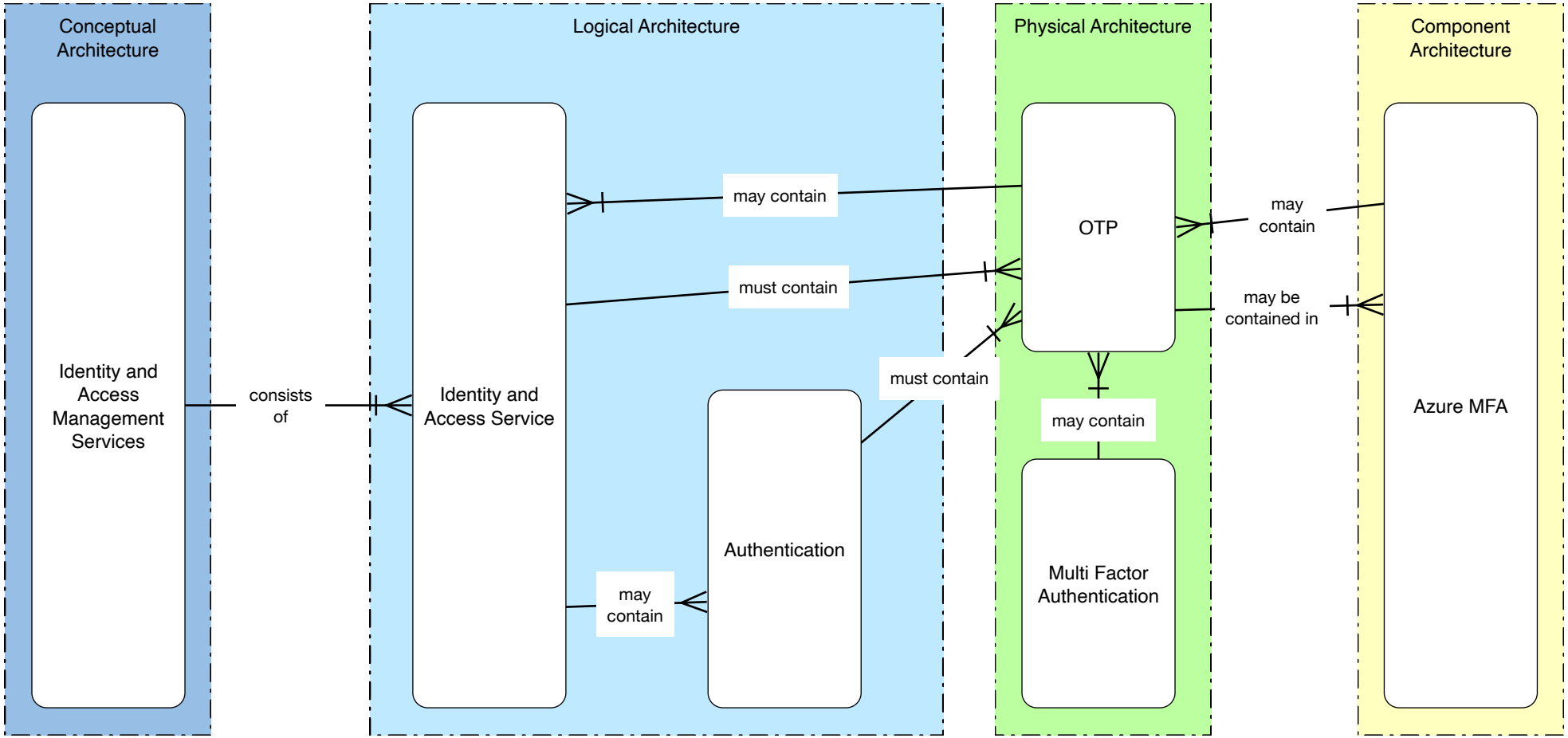



to define
Thresholds
Security Service
Products
Operational Data
create
Operational Processes
which contains
delivered using
which is measured using
may contain
Mechanism/Control
Key Risk indicators (KRI)
informs
Key Performance Indicators (KPI)
Key Control Indicators (KCI)
to reduce
Threats
Increase
sets
to allow generation of
Appetite
lead t
Risk
for
Security Maturity
help determine
Metrics
realise
measure

Different Stakeholders want to know different things from different layers in the architecture



Different Stakeholders want to know different things from different layers in the architecture



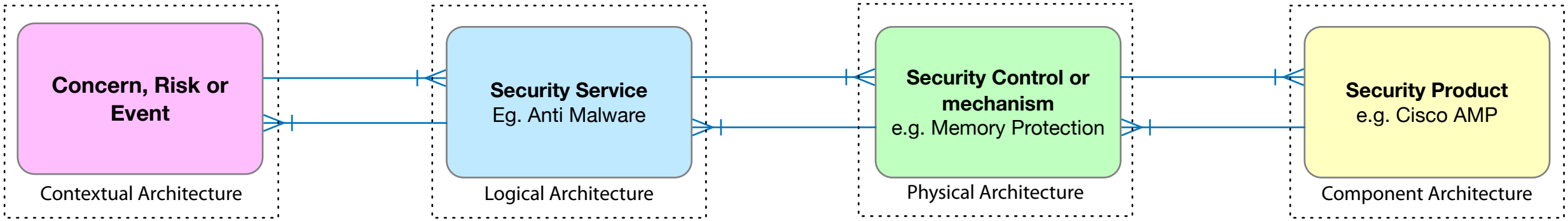
Where most organisations fail

Our senior stakeholders want to understand if we are prepared

The CISO usually only has part of the picture so can't honestly answer

We don't recognise or measure this

We try to answer the question using this



We don't understand the status of this

We fixate on this

So where do we go wrong?

Often the people responsible for operating the control don't really understand the risk the control is supposed to mitigate.

Often businesses can't determine whether a risk is controlled just that a contributing factor related to an often undisclosed risk has some form of control.

Businesses report on A narrow set of KCIs and confuse them with KRIs which doesn't reflect whether a risk is actually controlled.

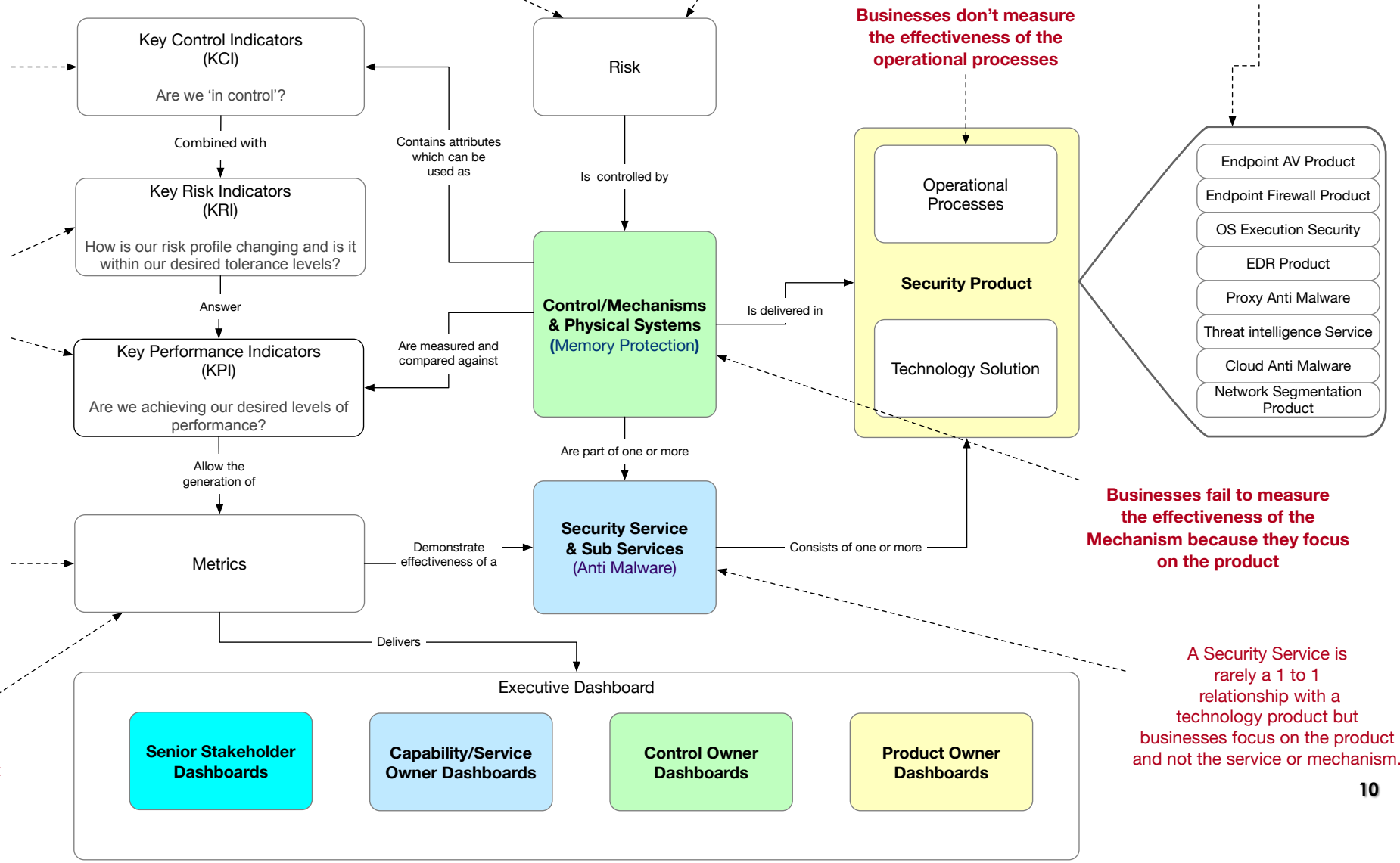
Most Indicators I have seen seem to focus on deployment status and often based on unreliable data

Businesses don't measure the effectiveness of the operational processes

Often criteria is not aligned to business requirements, priorities Or risk profile

Often businesses just measure deployment however this metric Is unlikely to change

Often metrics seem to be focused on project deliverables not control effectiveness



Businesses fail to measure the effectiveness of the Mechanism because they focus on the product

A Security Service is rarely a 1 to 1 relationship with a technology product but businesses focus on the product and not the service or mechanism.

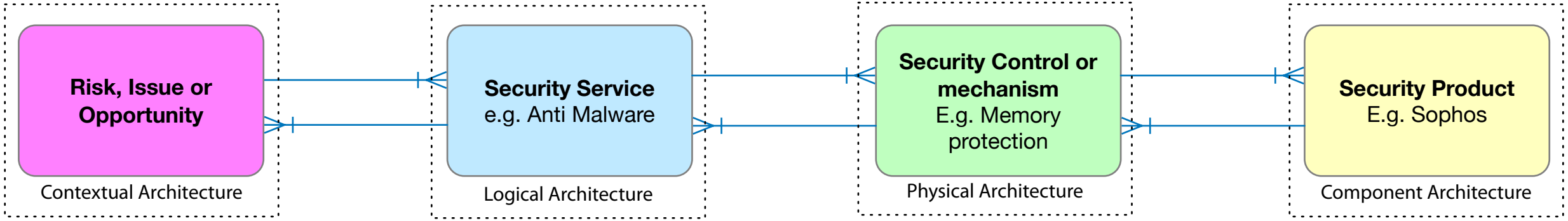
So what's the answer

We need clarity here to support decisions and placate investors

The CISO needs clarity here to support decisions and inform leadership

So measuring this gives a more complete picture

We use the data from here which allows us to build a status picture of each product



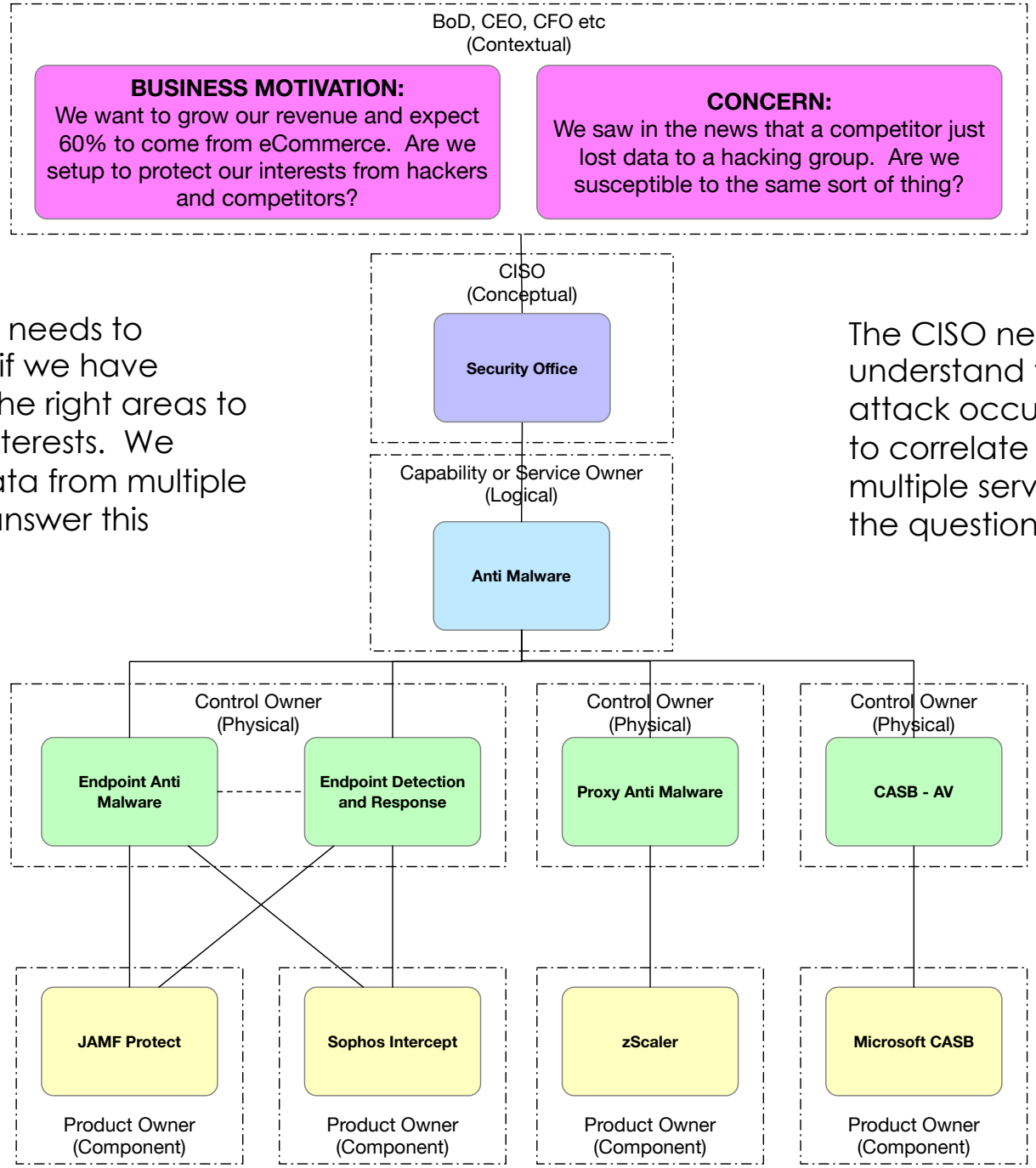
To present risk status here

We need to understand risk status here

So we measure this

Which will show weakness here

Lets work through an example to show how we need to look across the security landscape to obtain the answers.

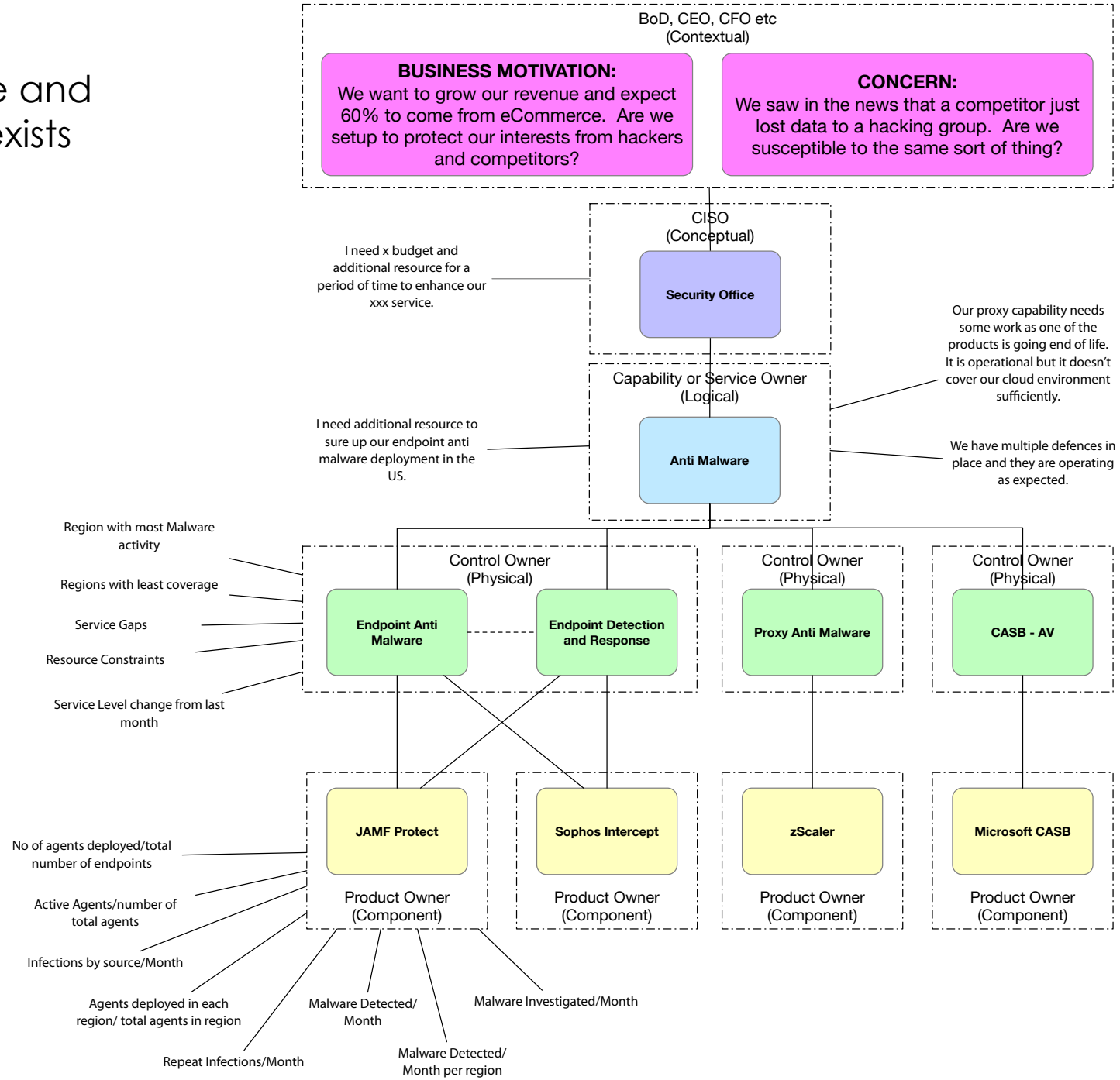


The business needs to understand if we have invested in the right areas to protect its interests. We correlate data from multiple services to answer this question.

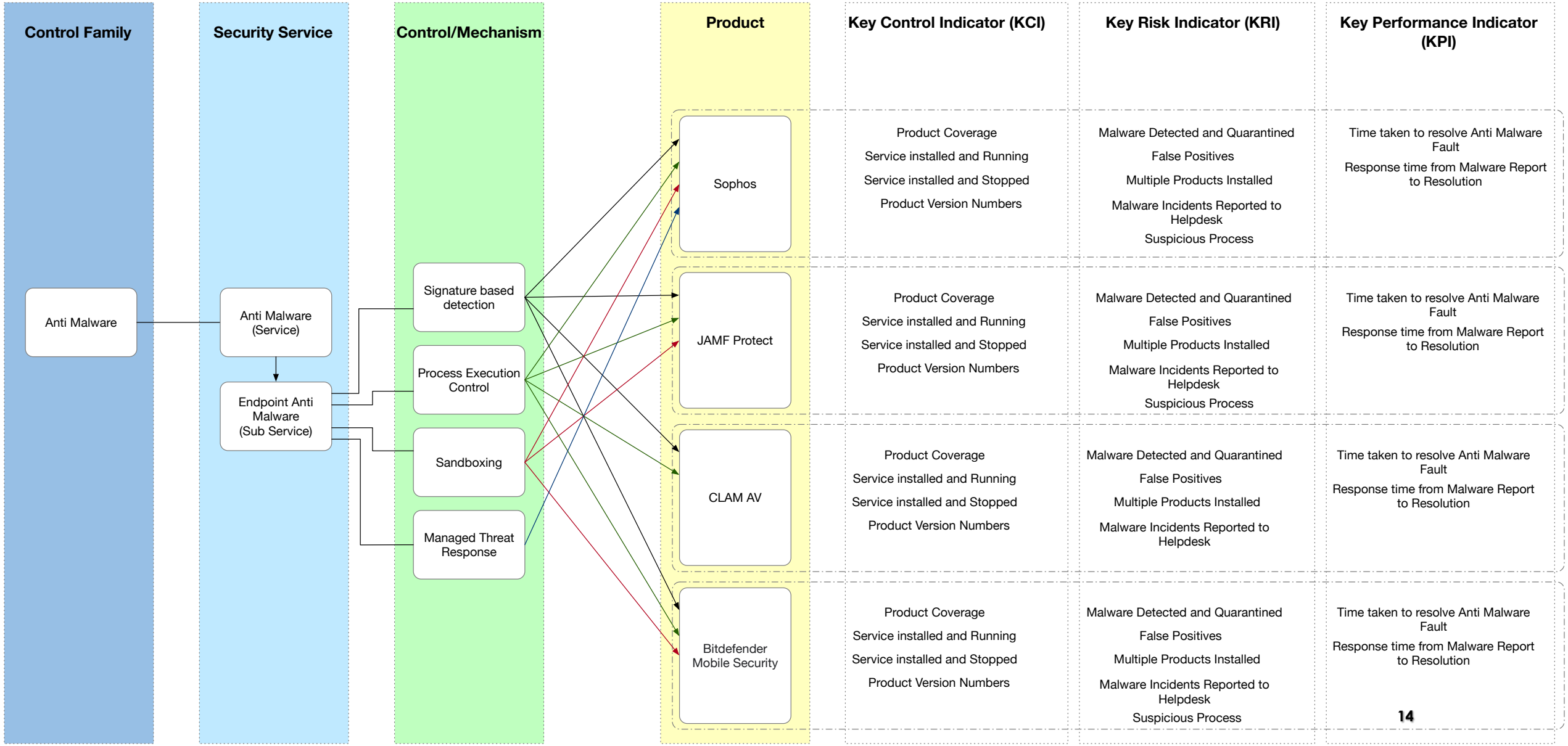
The CISO needs to understand the how the attack occurred and needs to correlate data from multiple services to answer the question accurately.

Incomplete limited sample to aid understanding

The Metrics allow us to answer with confidence and authority. Traceability exists through the layers.



I still don't get it – Where do KRI, KCI and KPI's come into play?



Incomplete limited sample to aid understanding

Example Key Control Indicator for Anti Malware

Endpoints with Multiple Anti Malware software package installed.	All endpoints with more than one Anti Malware product installed. This will inform of the of the following scenarios; 1.The machine has had a virus incident in the past and specialised removal software has been employed to remove it. 2.When the corporate AV software was installed the legacy package was not removed or failed to remove properly. 3.A secondary package is present as it will co-exist and provides additional protection over and above the primary tool. In general endpoints do not require more than one anti virus product installed and more often than not multiple anti virus products will create problems as they will conflict with each other.	•**Total Managed Endpoints with more than 1 AV** - Number of endpoints / Total number of managed devices - => 10% RED •**Total Managed Windows Servers with more than 1 AV** - Number of Windows Servers / Total number of managed Windows servers - => 10% RED •**Total Managed Linux Servers with more than 1 AV** - Number of Servers / Total number of managed servers - => 10% RED •**Total Managed Laptops with more than 1 AV** - Number of Laptops/ Total number of managed servers - => 10% RED •**Total Managed Macs with more than 1 AV** - Number of Macs / Total number of managed Macs- => 10% RED	•**Total Managed Endpoints with more than 1 AV** - Number of endpoints / Total number of managed devices - <10% AMBER •**Total Managed Windows Servers with more than 1 AV** - Number of Windows Servers / Total number of managed Windows servers - <10% AMBER •**Total Managed Linux Servers with more than 1 AV**- Number of Linux Servers / Total number of managed servers - <10% AMBER •**Total Managed Laptops with more than 1 AV** - Number of Laptops / Total number of managed servers - <10% AMBER •**Total Managed Macs with more than 1 AV** - Number of Macs/ Total number of managed Macs - <10% AMBER	**< 5% GREEN**

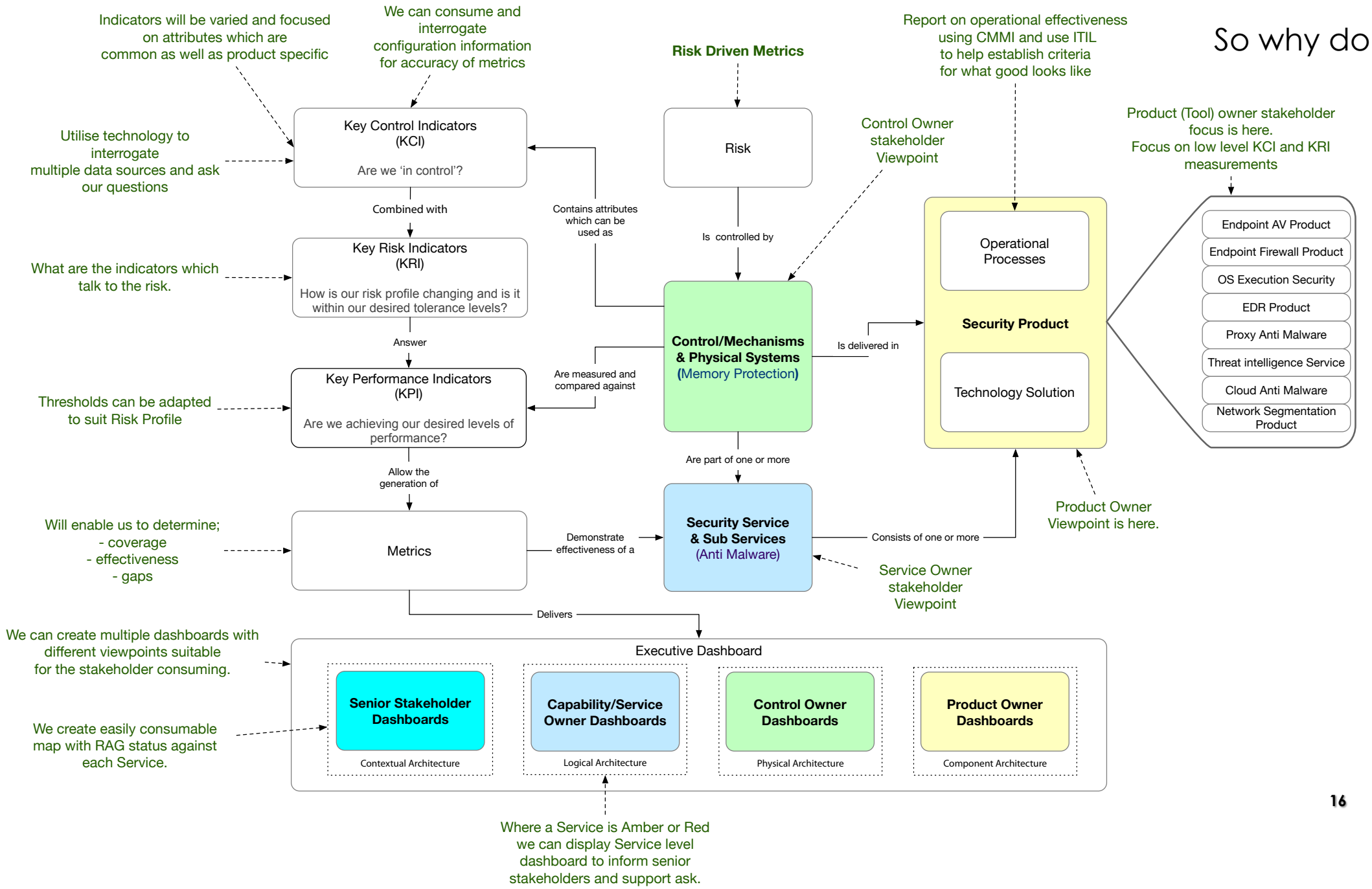
Example Key Risk Indicator for Anti Malware

Malware Detected	Demonstrates control effectiveness and if the numbers fluctuate broadly could indicate the following; •The product has improved and we are catching more •Malware attacks have increased •Perimeter defences are performing better/worse	10% fluctuation of average

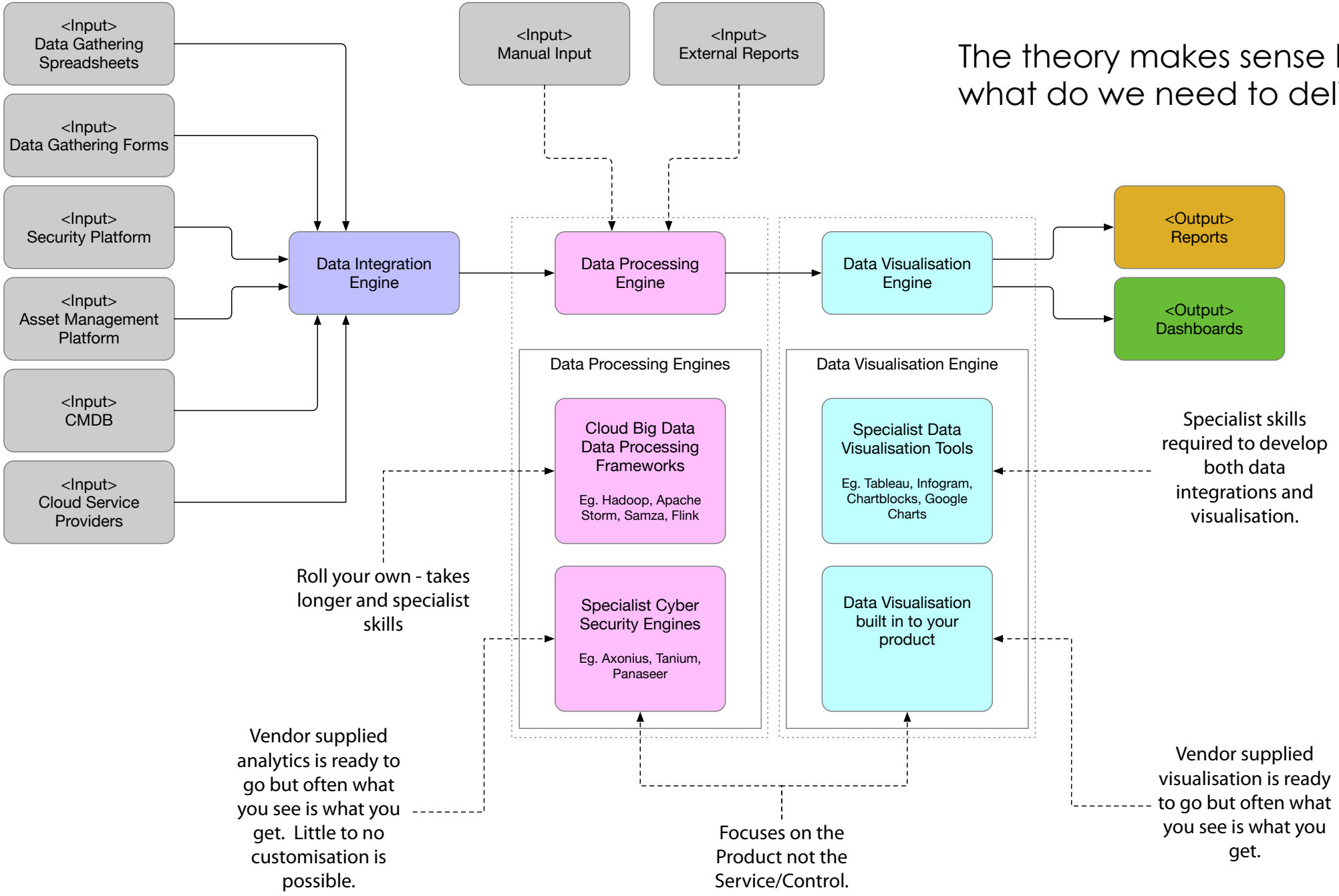
If we correlate with other data points we can tell different stories.

Incomplete limited sample to aid understanding

So why do this?



The theory makes sense but what do we need to deliver it?



In Summary

I have tried to provide a framework for evidence-based management to enable organisations to build a comprehensive metrics program in a structured way based on SABSA foundations. Its now up to you to roll your sleeves up and begin.

The reality is that a metrics program which provides the value described across your security landscape would take considerable time to build in its entirety, but early benefits could be easily be achieved with limited budget and simple tooling. To succeed:

- Plan the program;
- Focus on one service at a time;
- Define your indicators first; and
- Build out the tools you need to obtain and process the data.

Prove the value with one service first then expand.

Don't forget you can also report on opportunities in the same way by using Key Opportunity Indicators (KOI)

Quote : "What's measured improves"
— **Peter Drucker**

Questions?

Contact: Rob Campbell
Email : cosac@assuredcontrol.com
Linkedin : robert-campbell-security

These slides and other goodies – https://www.assuredcontrol.com

I am willing to provide the layered source diagrams for you to modify and use. They are in Omnigraffle format but I can convert to Visio. Just email and ask.