

BOSITE:
A framework to guarantee
activities lead to real business
outcomes

Omar Khawaja

Q: Where are we going?

A: hyper focus on enabling the business!





Q: What does the business want?

A: maximize business value!

Some of the challenges we are trying to address...

- ❑ Prioritize security investments

 - ...so we're confident we're making the right decisions

- ❑ Articulate justification for security investments

 - ...so the business wants to invest in security but does not micro-manage

- ❑ Communicate employee expectations / performance objectives

 - ...so employees work on what maximizes business outcomes

- ❑ Increase employee engagement

 - ...so high performing employees want to stay forever

- ❑ Measure productivity of security program

 - ...so we can enumerate value to the business (at least monthly!)

 - ...so the business wants to keep investing in security

When should we address these challenges?

Measure / validate value of a control using a consistent approach across the control lifecycle:

- ❑ **Before** approving a new initiative / control
- ❑ **During**: when tracking progress on an initiative / control being rolled out
- ❑ **After**: once a control is operating in steady state

How is business value measured?

Revenues (\$)

- Expenses (\$)

= Net Income (\$)

How is security program value (typically) measured?

$$\begin{array}{r} \text{Revenues (\$)} \\ - \text{Expenses (\$)} \\ \hline = \text{Net Income (\$)} \end{array}$$


How do we increase security program value?

- 1 Reduce expenses

$$\begin{array}{r} \text{Revenues (\$)} \\ - \text{Expenses (\$)} \\ \hline = \text{Net Income (\$)} \end{array}$$

How could we increase security program value?

- 1 Reduce expenses
- 2 Increase revenues (business outcomes)

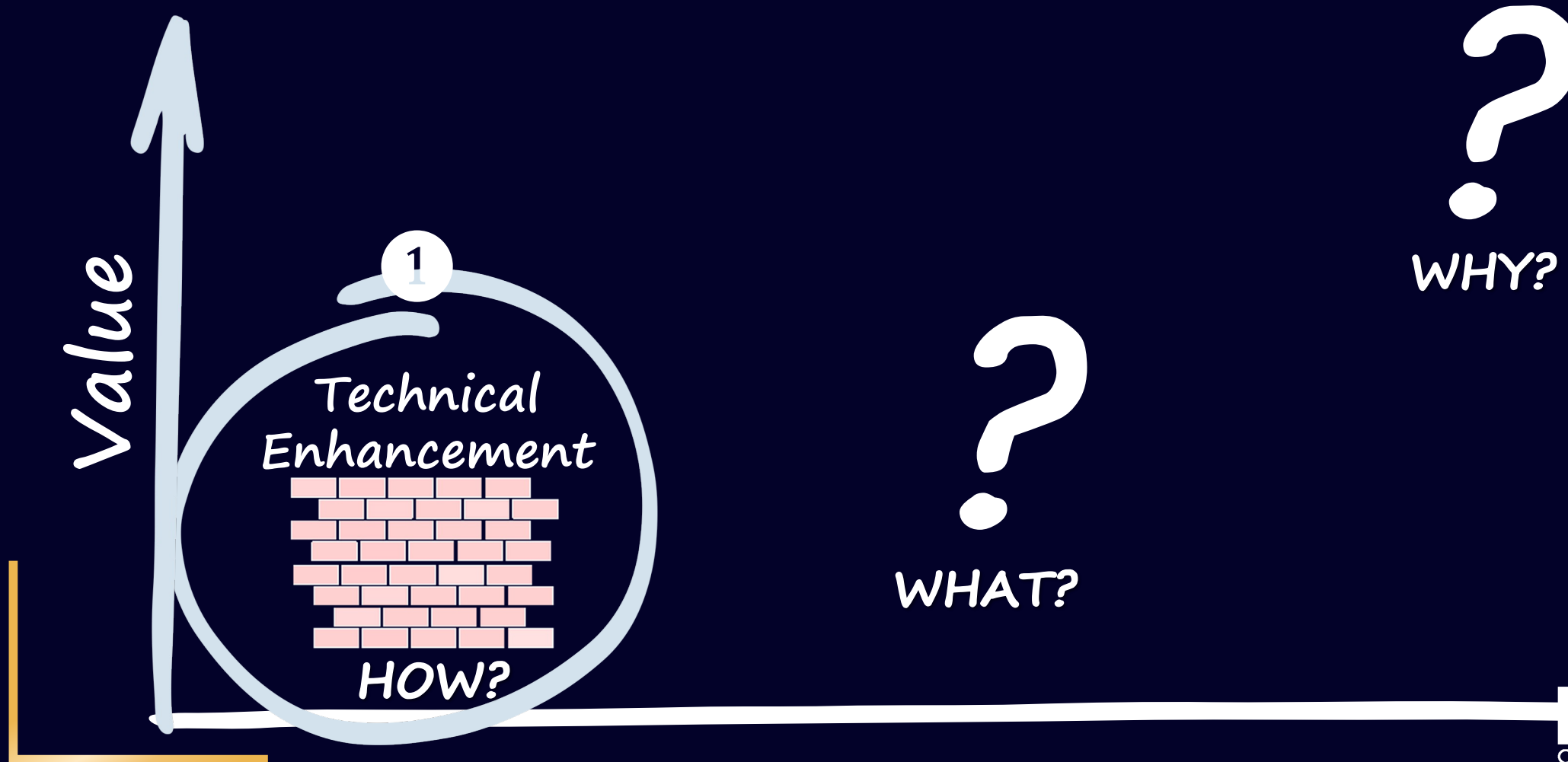

$$\begin{array}{r} \text{Revenues (\$)} \text{ 2} \\ - \text{Expenses (\$)} \text{ 1} \\ \hline = \text{Net Income (\$)} \end{array}$$

What are *business outcomes* of Highmark's security program?

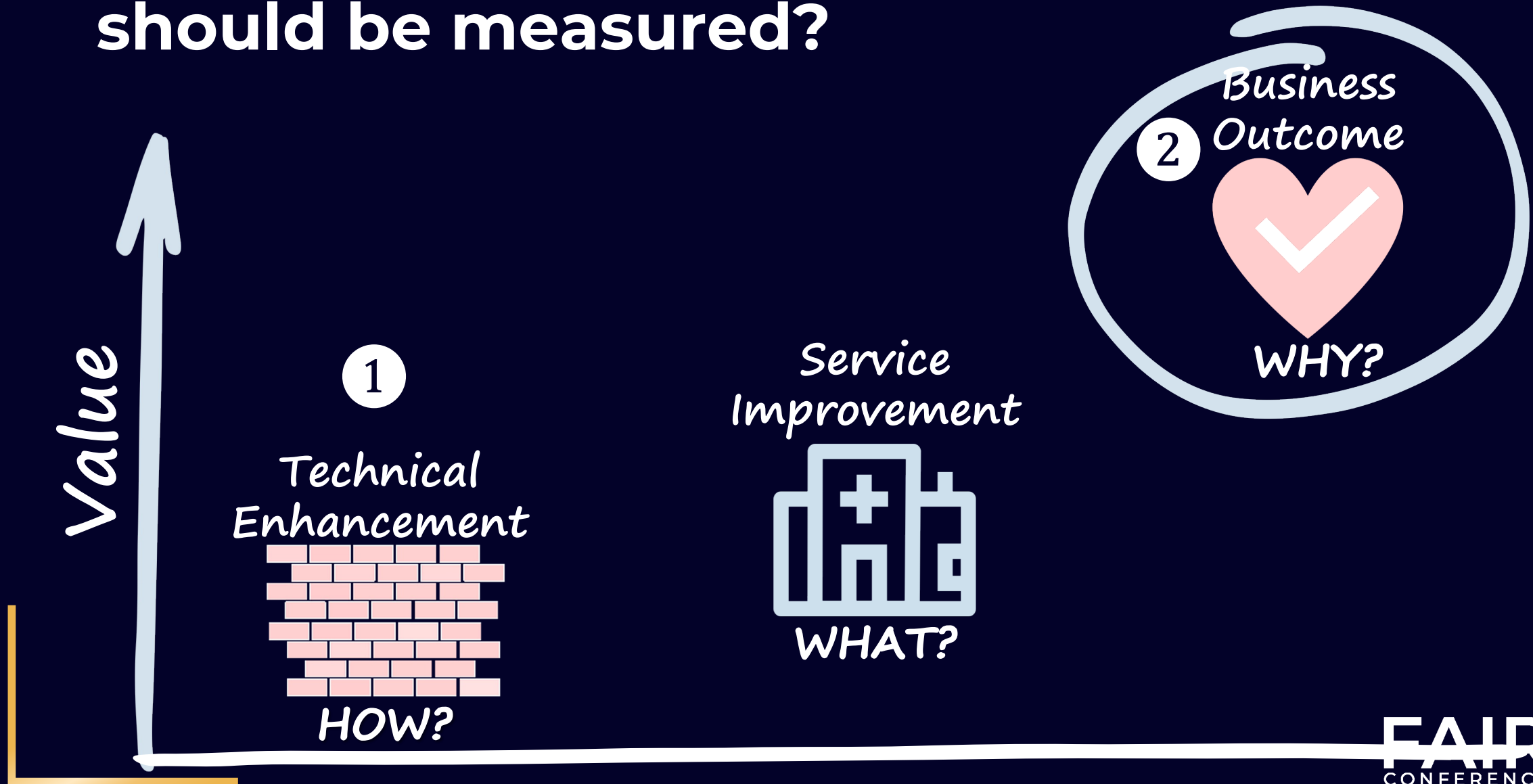


- Risk reduction
- Customer experience
- Operational excellence
- Compliance

What outcomes of a security program are typically measured?



What outcomes of a security program should be measured?



What is BO-SI-TE?

Business
Outcome



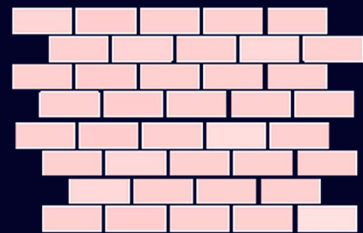
WHY should the business care? This is the ultimate destination.

Service
Improvement



WHAT are we going to make better? This the path to the destination

Technical
Enhancement



HOW are we going to achieve the results? These are the specific steps along the path to the destination.

Highmark Health ISRM "BOSITE" framework for: business case, project tracking and capability evaluation

1

HOW? (e.g.: laying bricks)

III. TECHNICAL ENHANCEMENTS (TE)

How are we going to achieve the results? What specific steps will we take on the path to our destination?
 Can include: vendor names, technology names, use cases, version numbers, technical terms, acronyms
 Cannot include: risk reduction, compliance, operational excellence, customer experience

2

WHAT? (e.g.: building a hospital)

II. SERVICE IMPROVEMENTS (SI)

What are we going to make better? What's the path to our destination?
 Can include: ISRM service / capability names, use cases, KPIs
 Cannot include: vendor names, technology names, version numbers

WHY? (e.g.: make / keep people healthy: create a remarkable health experience)

I. BUSINESS OUTCOMES (BO)

Why should someone outside of the service area care? What's the ultimate destination?
 Can include: risk reduction, compliance, operational excellence, customer experience
 Cannot include: ISRM service / capability names, vendor names, technology names, version numbers, technical terms, acronyms

What are the desired business outcomes?	How will the business outcomes be measured (BO metrics, e.g.: CyberScore, \$)?	What is the current value of each BO metric?	What is the target value of each BO metric?	By when will the target value of the BO metric be achieved?	What are the planned service improvements?	How will the service improvements be measured (SI metrics, e.g.: SECURE Index)?	What is the current value of each SI metric?	What is the target value of each SI metric?	By when will the target value of the SI metric be achieved?	What are the technical enhancements?	When will they be implemented?
Risk Reduction											
Customer Experience											
Operational Excellence											
Compliance											



Specific approaches to optimizing security program value ②

Future investments / controls

- Any proposed investments with acronyms, technology or vendor names in the title should not be considered ②
- All proposed security investments should be prioritized based on measurable *business outcomes* ②

Employees

- All security employees' performance objectives should align to either business outcomes or service improvements (especially leaders!) ②

Current controls

- Measure actual *business outcomes* from top 10 most expensive (HW, SW and labor) controls ②
- **Sunset** technologies with low / negative value (cost of *technical enhancement* is greater than *business outcome*) ②

Communication

- Keep executives and the business **out of the cockpit**: convey *business outcomes* (and sometimes, *service improvements*), but not *technical enhancements* ②

How should we measure security program value?

Revenues (\$)

- Expenses (\$)

= Net Income (\$)

Business Outcomes (\$)

- Technical Enhancements (\$)

= Value (\$)

A photograph of two men in a workshop setting. One man, wearing a plaid shirt and brown overalls, is leaning over a laptop screen. The other man, with a beard and wearing a light-colored shirt, is looking at the screen. The background shows wooden walls and hanging lamps. The image is overlaid with semi-transparent text boxes.


Q: What does the business want?

A: maximize business value!

... based on the business' needs

... in the business' language

FAIR
INSTITUTE



BOSITE:
A framework to guarantee
activities lead to real business
outcomes

Omar Khawaja