Jason Martin and Greg Rothauser

09/23/21

Operationalizing FAIR at a Healthcare Insurer and Provider

Jason Martin

IT/IS Manager
Vulnerability & IT Asset Mgmt

Contacts

jason.martin@highmarkhealth.org

412-544-5652

Greg Rothauser

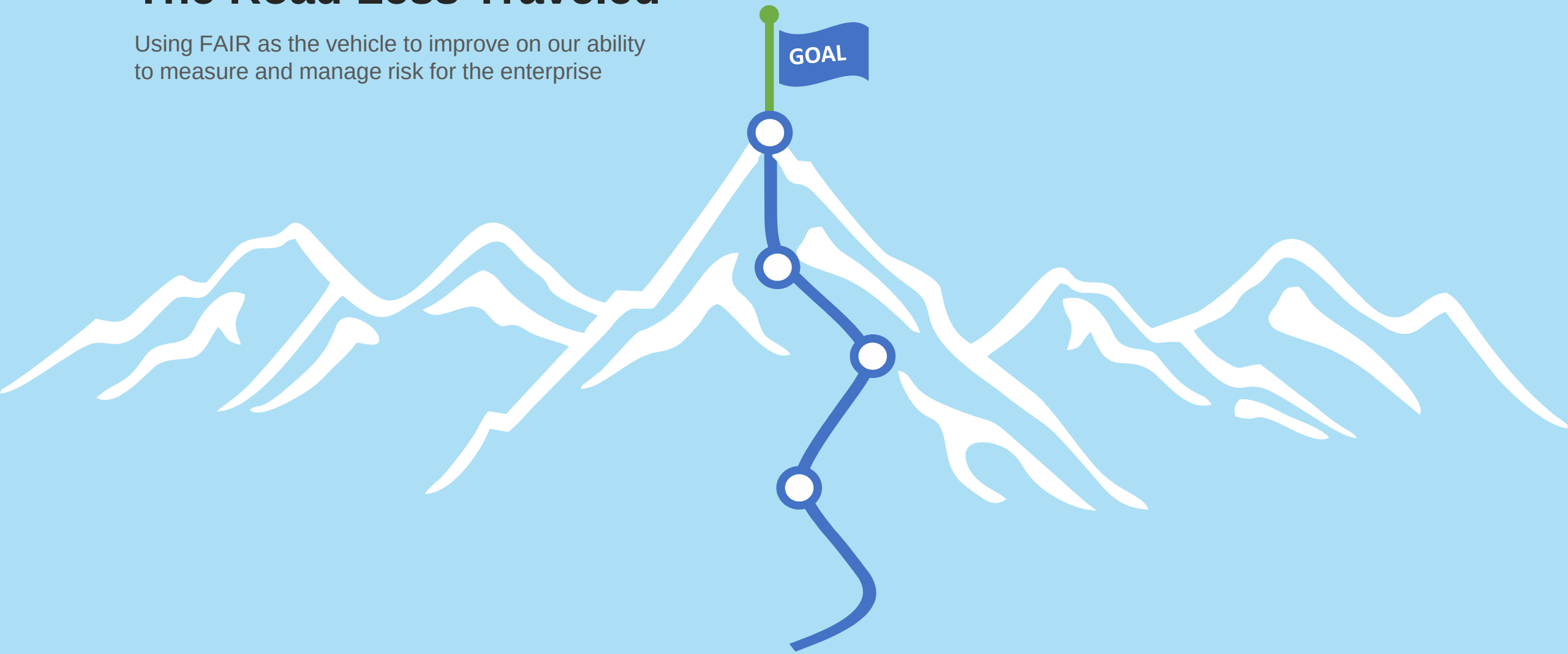
Senior Information Risk Consultant
Governance, Risk, & Compliance

Contacts

gregory.rothauser@highmarkhealth.org

The Road Less Traveled

Using FAIR as the vehicle to improve on our ability to measure and manage risk for the enterprise



The Case for Change…

Not Audience Centric:
Vague broad statements. Terminology is a mix of technical jargon and Fear, Uncertainty, and Doubt

Not Rational, or Measurable:
Your Medium = My Medium?
We all bring biases to heat maps

HM Health Solutions

nt Assessment Overview:
Mobile Messaging Solution*

Scope:	Subsidiary	Reported	11/2016
ISRM Assessor:	Jason Martin	Security Architect:	John Doe
Requestor:	Business Owner	Privacy Reviewer:	Jill Smith

Description:
Vendor is designing a portable mobile/tablet application for subsidiary that includes messaging solution to improve member and patient engagement. Providers can access the solution via web application to send messages via phone app to groups of members. Will require cloud computing environment to facilitate backend services.

Impact \ Likelihood	L	ML	M	MH	H
H				1	1
MH			1	1	
M		1	2		
ML					
L					

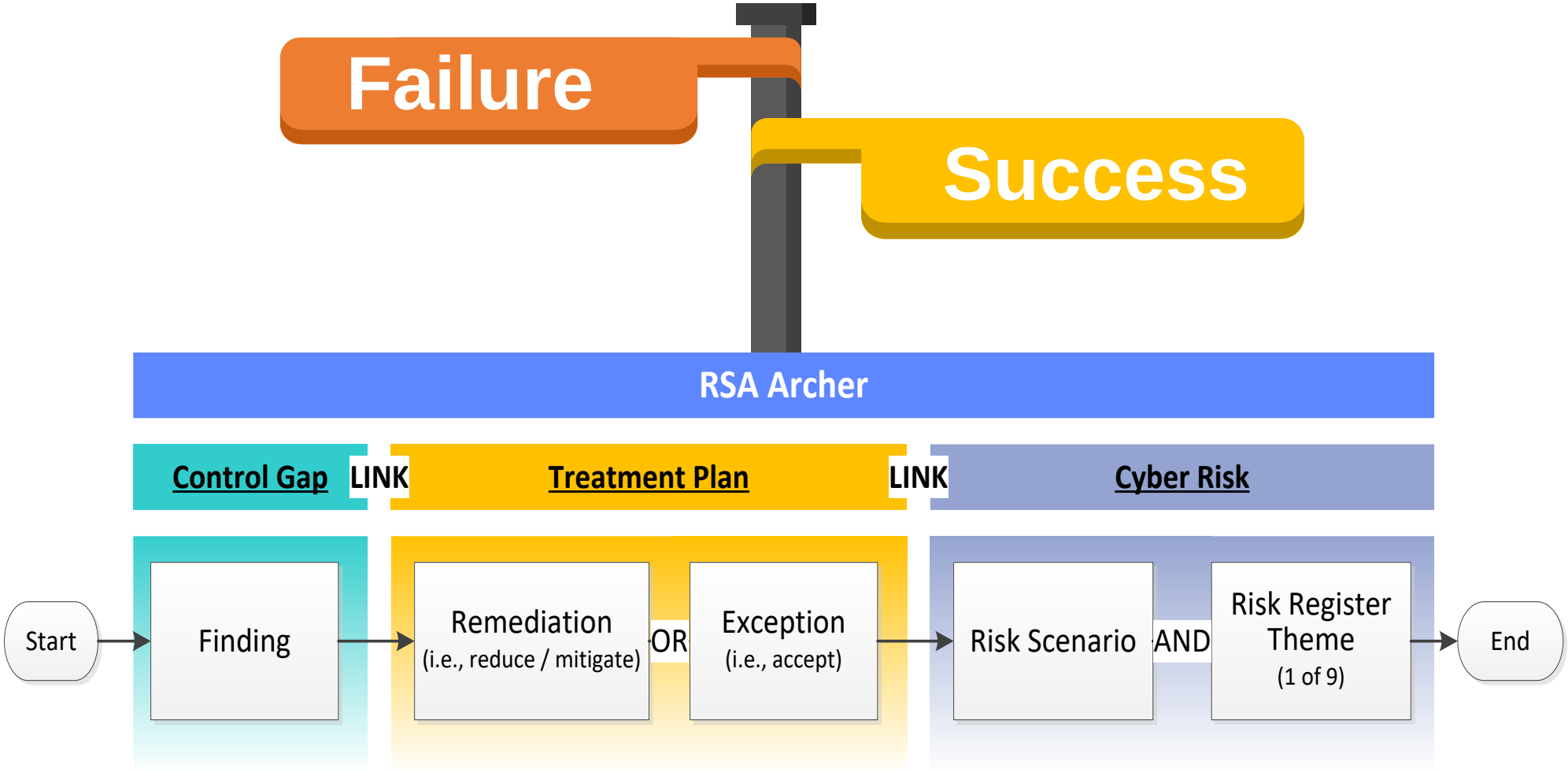
	Control Category	Findings	Risk	Suggested Mitigating Controls	2016	Treatment	2017
1	09.e Service Delivery	Non-US citizen and non-clearance cloud vender personnel could access subsidiary's member information when providing backend data, application or process support.	Poor legal standing in contracts, potential litigation or civil actions. (RSK-1787)	All employees working on the program must be US citizens with clearance.	High	Will not store and/or process government contract PHI or PII.	Closed
2	01.v Information Access Restriction	Data captured on devices and files uploaded to mobile app will stay in the cloud for 48 hours unencrypted before either transmitted or cleared off from storage.	Power users have direct access data in cloud and allow unauthorized ability to read / view PHI/PII information. (RSK-1784)	Data-at-rest and files uploaded containing PII/PHI attributes should be encrypted using AES-256 strength encryption.	High	Remediated	Closed
3	10.m Vulnerabilities	Vendor is using an unsupported version of relational database system for customer data storage and encryption.	Known security vulnerabilities (e.g. CVE-2013-1899) and lack of backward compatibility allow for less effective data protection. (RSK-1782)	Evidence that vendor is running on the newest supported version of Postgres.	Med-High	Remediated	Closed
4	05.j Risks Related to External Parties	Cloud vendor has a global data center infrastructure; unclear if data will be stored on cloud servers located offshore.	Improper data handling can lead to unintentional data disclosures. (RSK-1786)	Request location be hosted at the US data center(s) only.	Med-High	Remediated	Closed
5	01.w Sensitive System Isolation	System / file-level encryption performed at vendor lacks suitable key rotation policy.	Risks to the confidentiality, availability and integrity of corporate information and potential data related regulatory issues. (RSK-1783)	Request vendor's technical specifications and controls to ensure that data is properly wiped when requested.	Medium	Data encrypted and no one from vendor has access to the encryption keys	Closed
6	06.d Data Protection and Privacy	Data, application or process could be legally owned by the cloud service provider.	Non-compliance that can result in fines, censures, civil and legal liabilities. (RSK-1786)	Sub-contracts must reflect the same standard that is expected from Highmark to prevent unauthorized data disclosures.	Medium	Remediated:	Closed
7	01.c Privilege Management	Vendor employees uses cloud based file hosting service for external and internal file sharing.	Over-authorization of users' roles or acc data, transactions or business systems. (RSK-1784)				Closed

Not Decision Support, or Aligned:
Illusion of communication; cannot compare cyber risk to other business risks

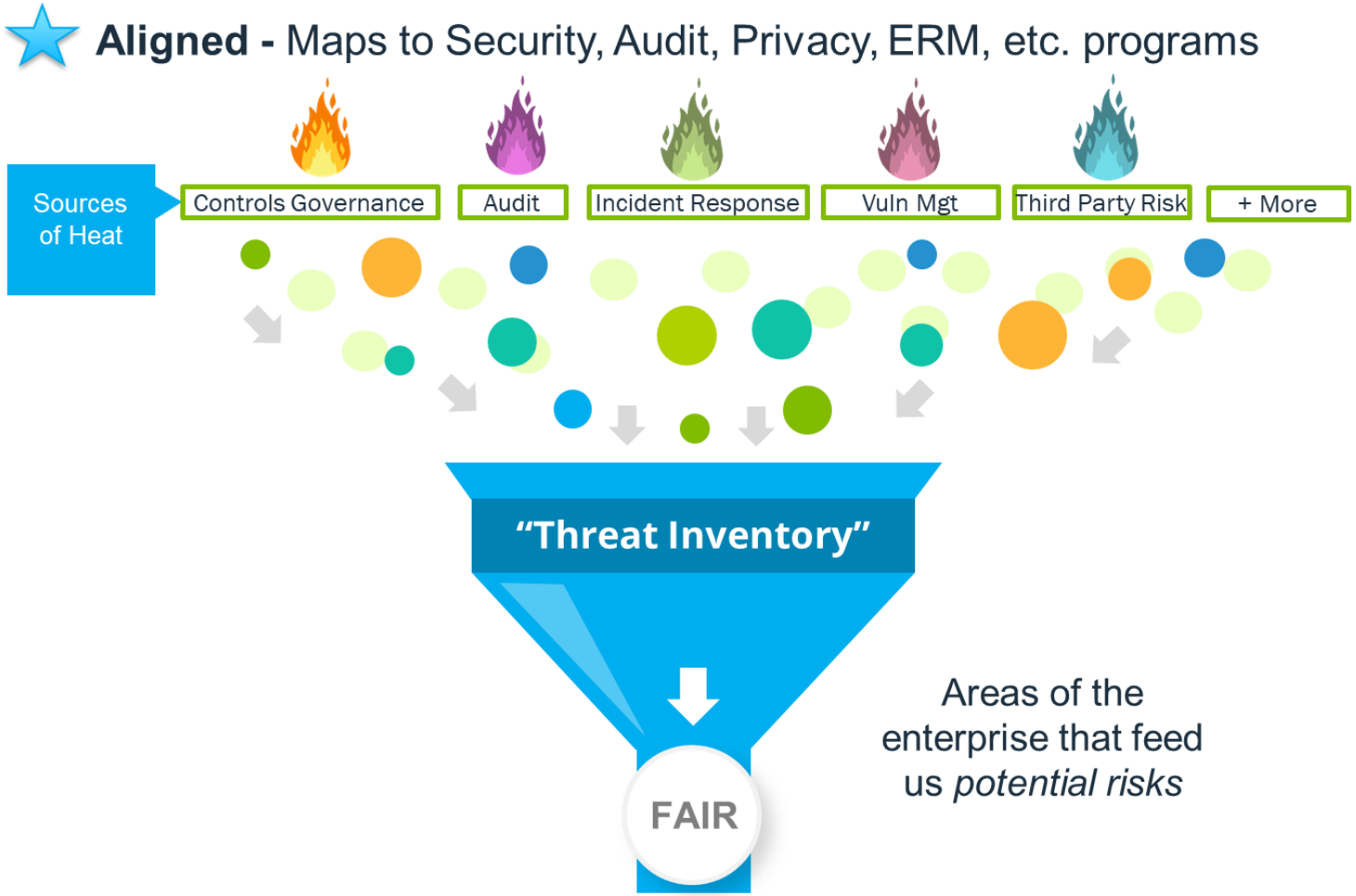
ETO

* The information described in the preceding example has been compiled solely for illustrative purposes. The results depicted are NOT those from a risk assessment of a real organization.

Exception Management



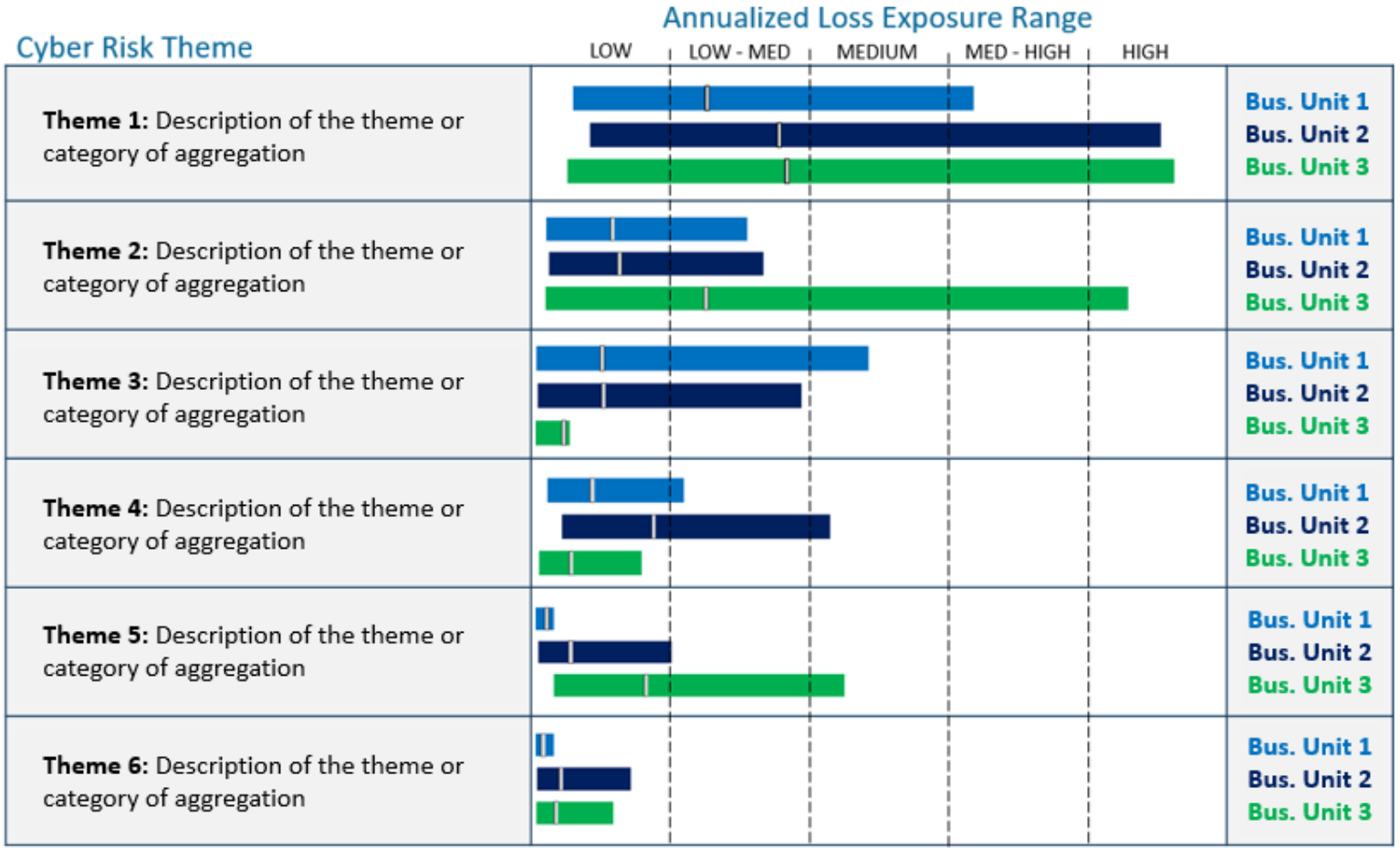
Challenges & Lessons Learned



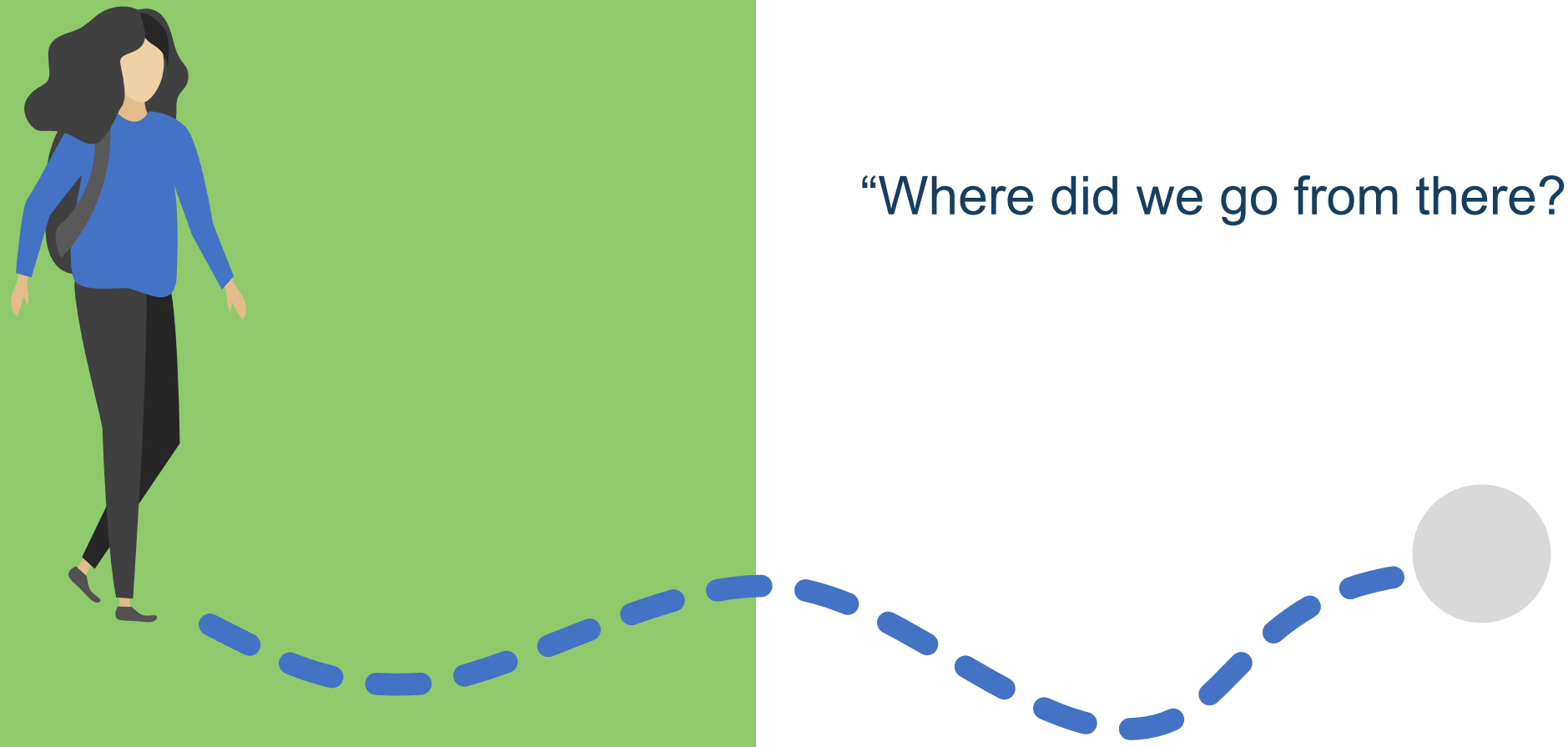
A Better Foundation

Has its uses…

But is only a start

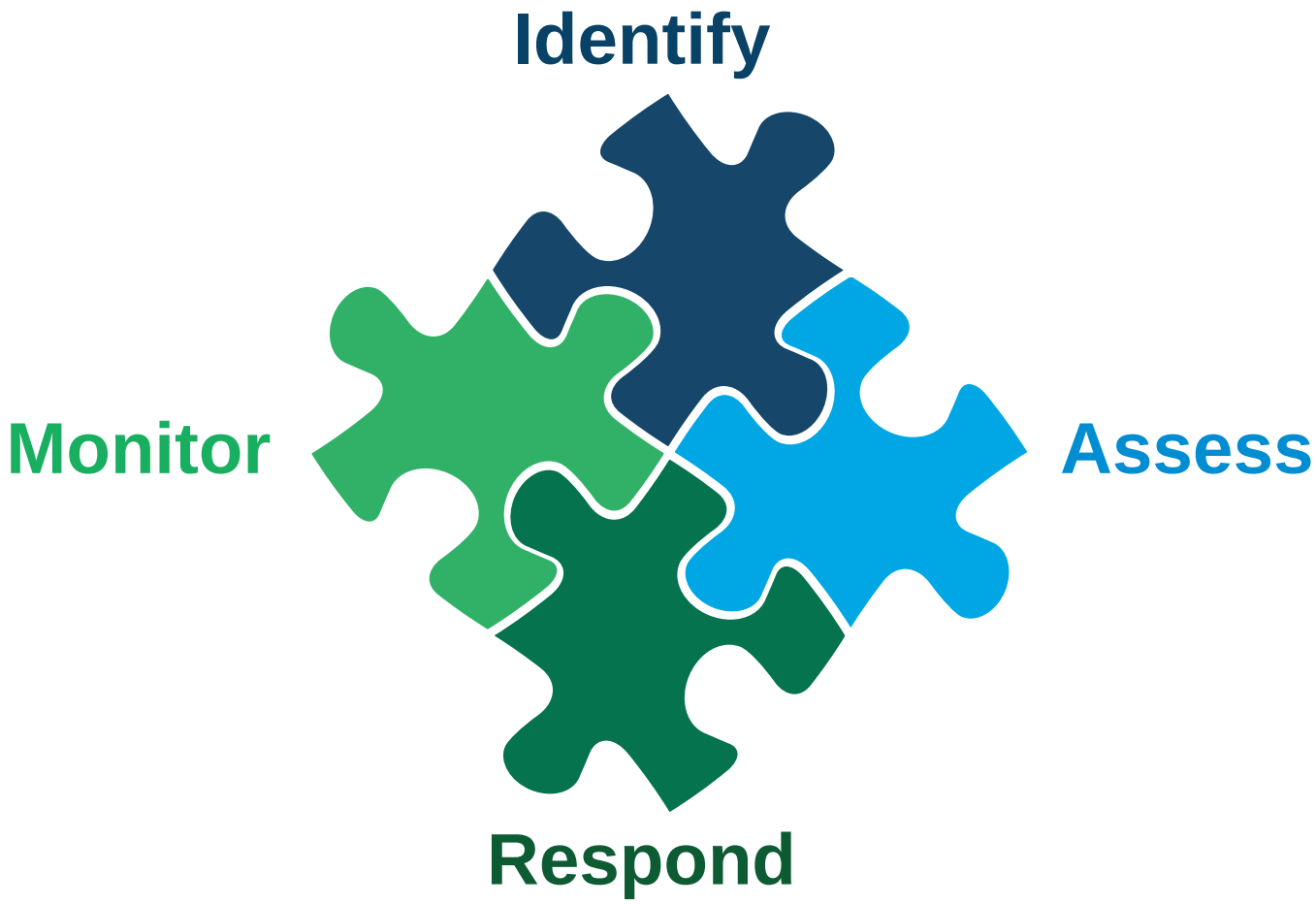


Current Use Cases



"Where did we go from there?"

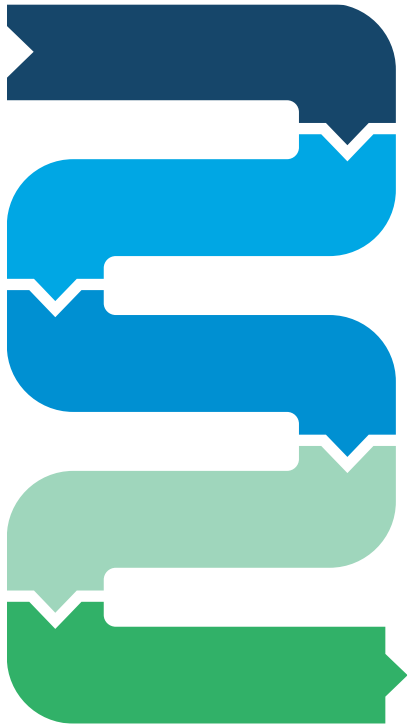
What are we trying to do?



The Process

Needs to be efficient and flexible

Identify Top Risks



Create Baseline

Adjust FAIR Inputs

Run Comparison

Report Results

Using the Results

Name	Description	Measurable Outcome	2021 Budget Request	Average ALE Reduction	ROI (per $ Spent)
Project 1	Bastion Server for PHI DBases	95% of all privileged access using MFA	$400,000	$3,600,000	$9.00
Project 2	ISP Provided DDoS protection	All DDoS traffic Blackholed within 5 mins	$300,000	$1,800,000	$6.00
Project 3	...	...	$400,000	$1,900,000	$4.75
Project 4	...	...	$300,000	$1,700,000	$5.67
Project 5	...	...	$600,000	$1,800,000	$3.00
Project 6	...	...	$300,000	$1,200,000	$4.00

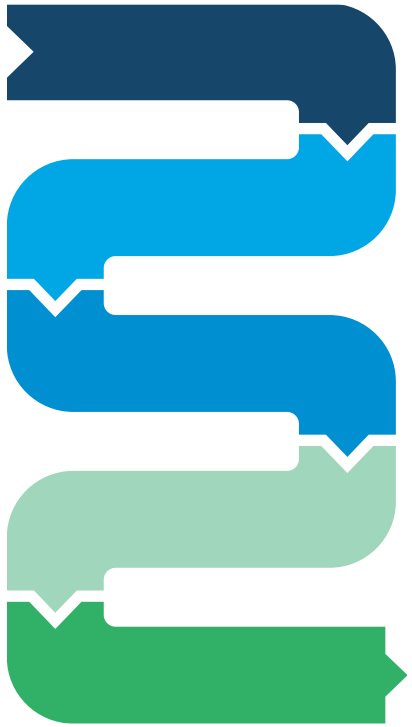
Effective Comparisons

Quick and Efficient

The Process

Needs to be efficient and flexible

Identify Top Risks



Create Baseline

Adjust FAIR Inputs

Run Comparison

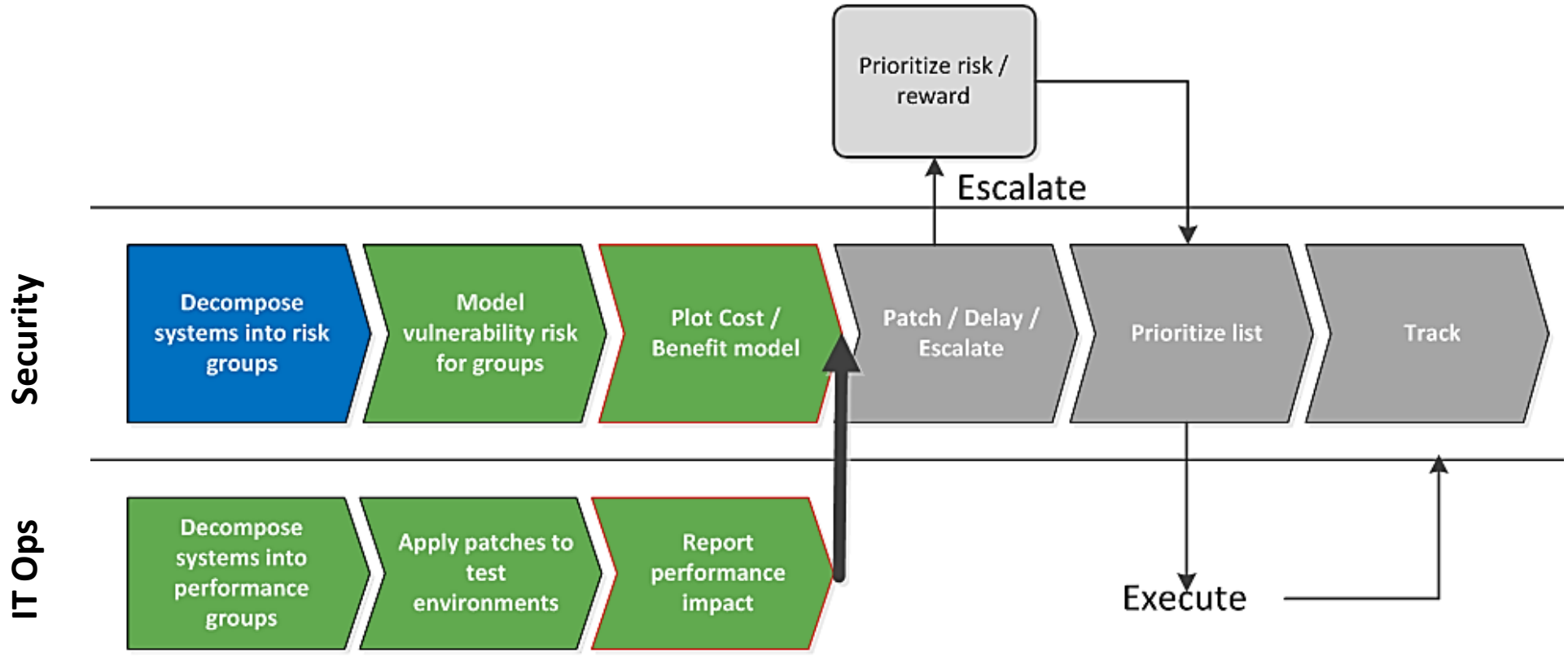
Report Results

Future Vision

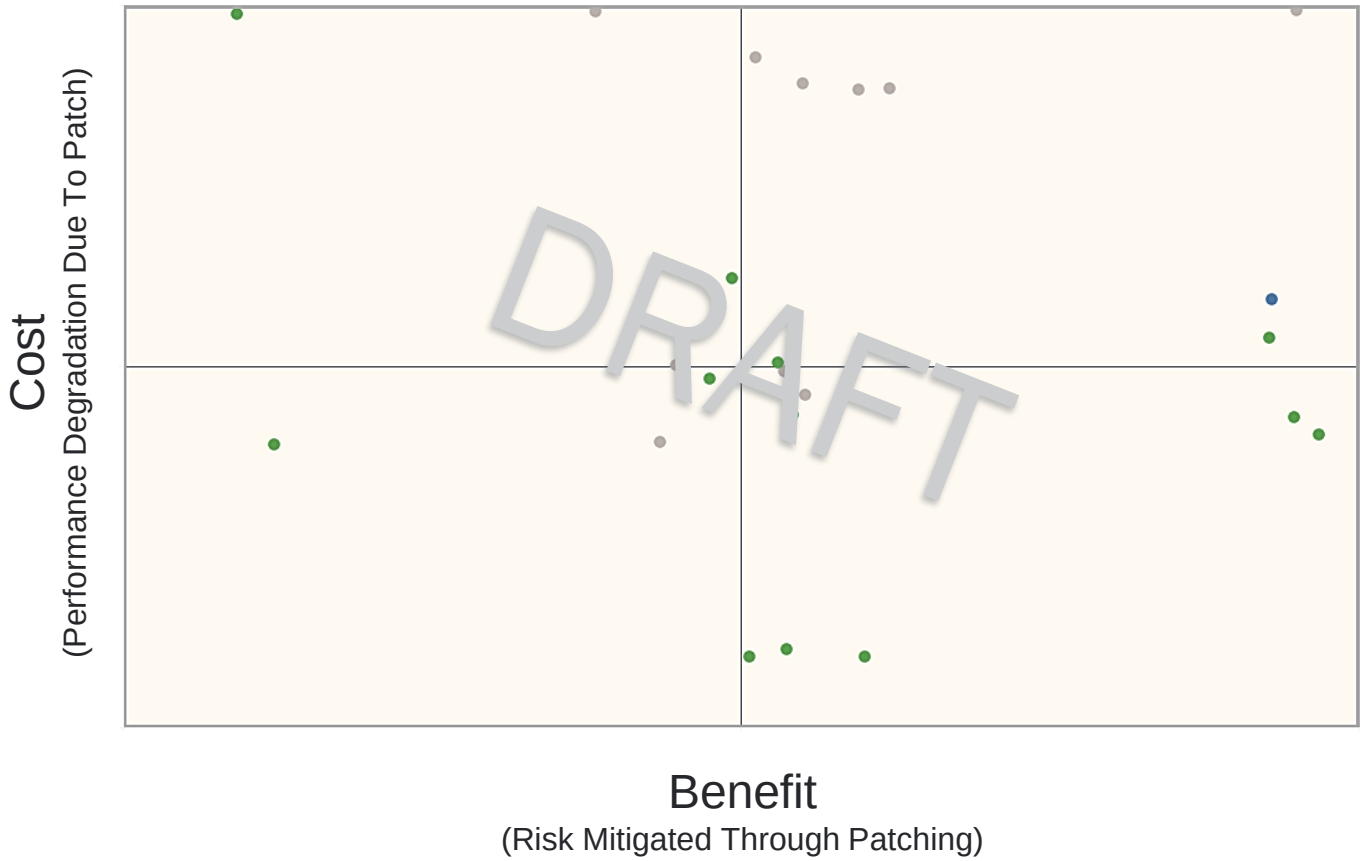
The Next Steps…

Vulnerability Governance

Continuously performing infrastructure assessments to identify, define, quantify, categorize, communicate, and mitigate risks



Vulnerability Governance



Prioritized list of assets for patching

1. Workstations
2. DMZ Servers
3. Vendor Servers
4. Extranet
5. Medical Devices
6. Middleware
7. IT Lab Environments

Status
- Completed
- In Progress
- Not Started

Graph is not real data but for demonstrative purposes only until real data is collected.

Combining Frameworks and Approaches

HITRUST®

- Threat Catalog
- Controls Framework

FAIR INSTITUTE

- Scenario Scoping
- Loss Magnitude

An accurate and efficient understanding of cyber risk

ETO

Improving Budgeting

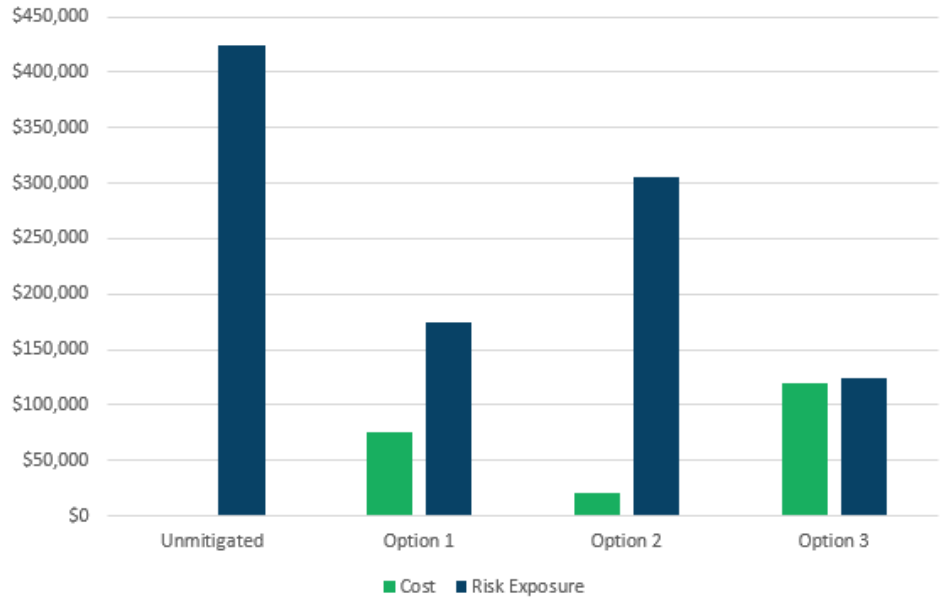
Where we are:

Name	Description	Measurable Outcome	2021 Budget Request	Average ALE Reduction	ROI (per $ Spent)
Project 1	Bastion Server for PHI DBases	95% of all privileged access using MFA	$400,000	$3,600,000	$9.00
Project 2	ISP Provided DDoS protection	All DDoS traffic Blackholed within 5 mins	$300,000	$1,800,000	$6.00
Project 3	...	...	$400,000	$1,900,000	$4.75
Project 4	...	...	$300,000	$1,700,000	$5.67
Project 5	...	...	$600,000	$1,800,000	$3.00
Project 6	...	...	$300,000	$1,200,000	$4.00

Improving Budgeting

Where we are going:

Focus Areas Identified → Projects Proposed → ROI Quantified → Response Selection



Name	Description	Measurable Outcome	2021 Budget Request	Average ALE Reduction	ROI (per $ Spent)
Project 1	Bastion Server for PHI DBases	95% of all privileged access using MFA	$400,000	$3,600,000	$9.00
Project 2	ISP Provided DDoS protection	All DDoS traffic Blackholed within 5 mins	$300,000	$1,800,000	$6.00
Project 3	...	...	$400,000	$1,900,000	$4.75
Project 4	...	...	$300,000	$1,700,000	$5.67
Project 5	...	...	$600,000	$1,800,000	$3.00
Project 6	...	...	$300,000	$1,200,000	$4.00

Where we started (Successes and challenges)

Current use cases

Improvements and additions to the program

Final Questions?