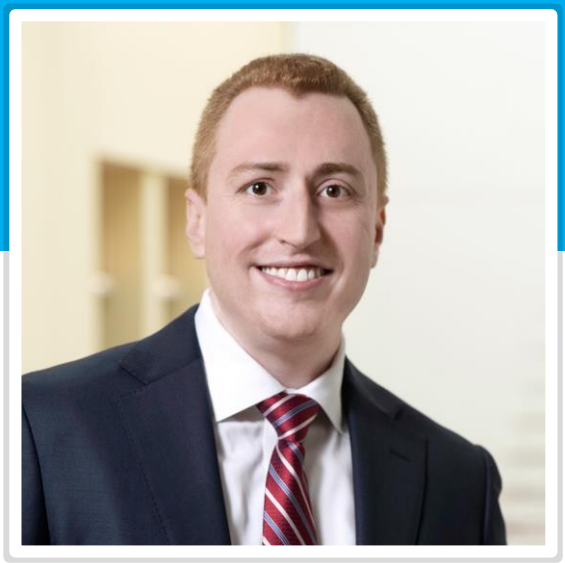
Quantified Cyber Risk Management:

Three steps to success

HIGHMARK HEALTH



Jason Martin

Manager

CRISC, GSEC, FAIR

HIGHMARK HEALTH

CYBER RISK & CONTROLS MANAGEMENT

Jason.Martin@hmhs.com

412-544-5652

Quantified Cyber Risk Program

Key Outcomes:

1. Measurable – Able to compare business units and track trending
2. Aligned – Maps to Information Security, Audit, Privacy, ERM, etc. programs
3. Rational – Results are built upon robust and defensible logic
4. Audience-Centric – Express risk in business terms
5. Decision Support – Results simplify taking appropriate actions

Steps to Achieve:

1. Identify – Know what risks you face
2. Quantify – Understand the logical factors driving the risk
3. Manage – Influence the factors that put your business at risk

The Case for Change…

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

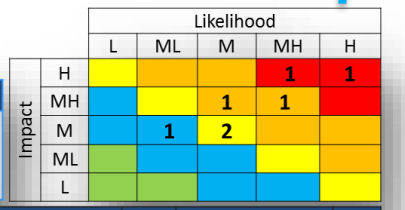
Not Audience Centric:
Vague broad statements. Terminology is a mix of technical jargon and Fear, Uncertainty, and Doubt

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.

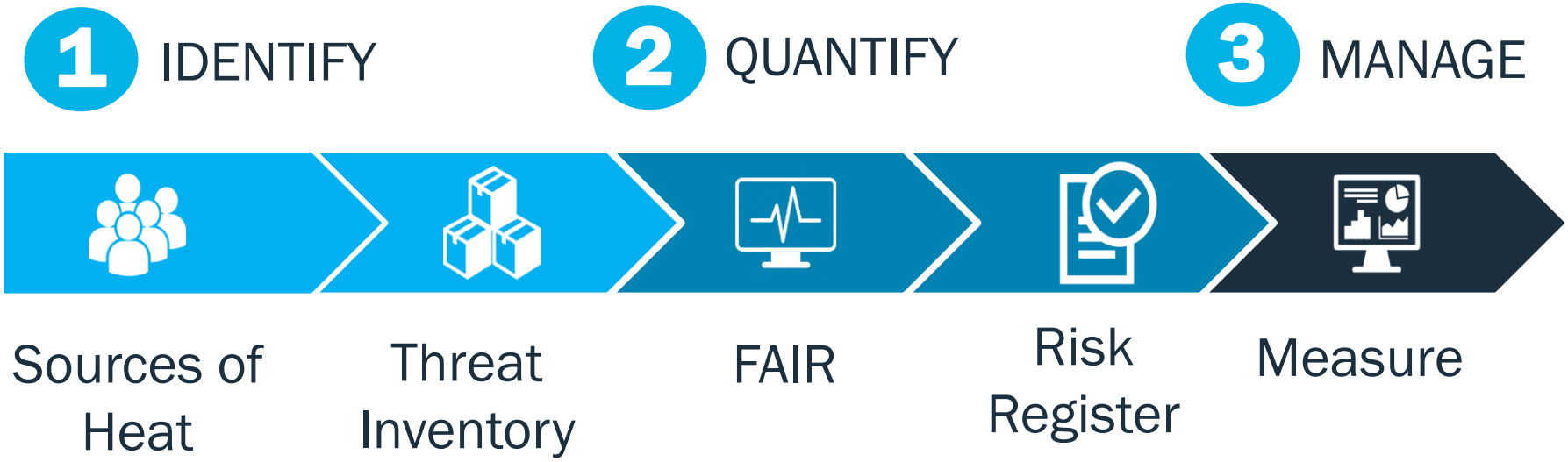


	Control Category	Findings	Risk	Suggested Mitigating Controls	2016	Treatment	2017
1	09.e Service Delivery	Non-US citizen and non-clearance cloud vender personnel could access subsidiary's member information when providing backend data, application or process support.	Poor legal standing in contracts, 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

* 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.

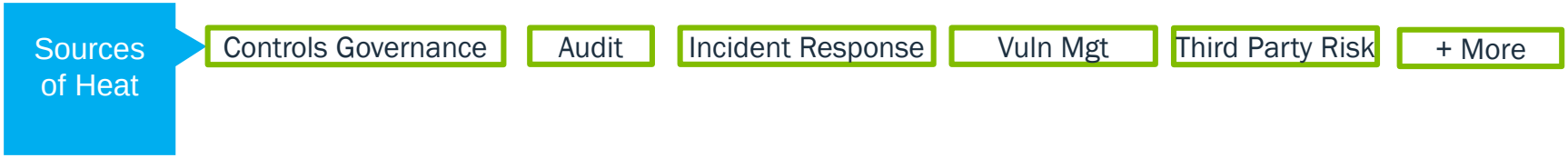
Three steps to success



1. Identify

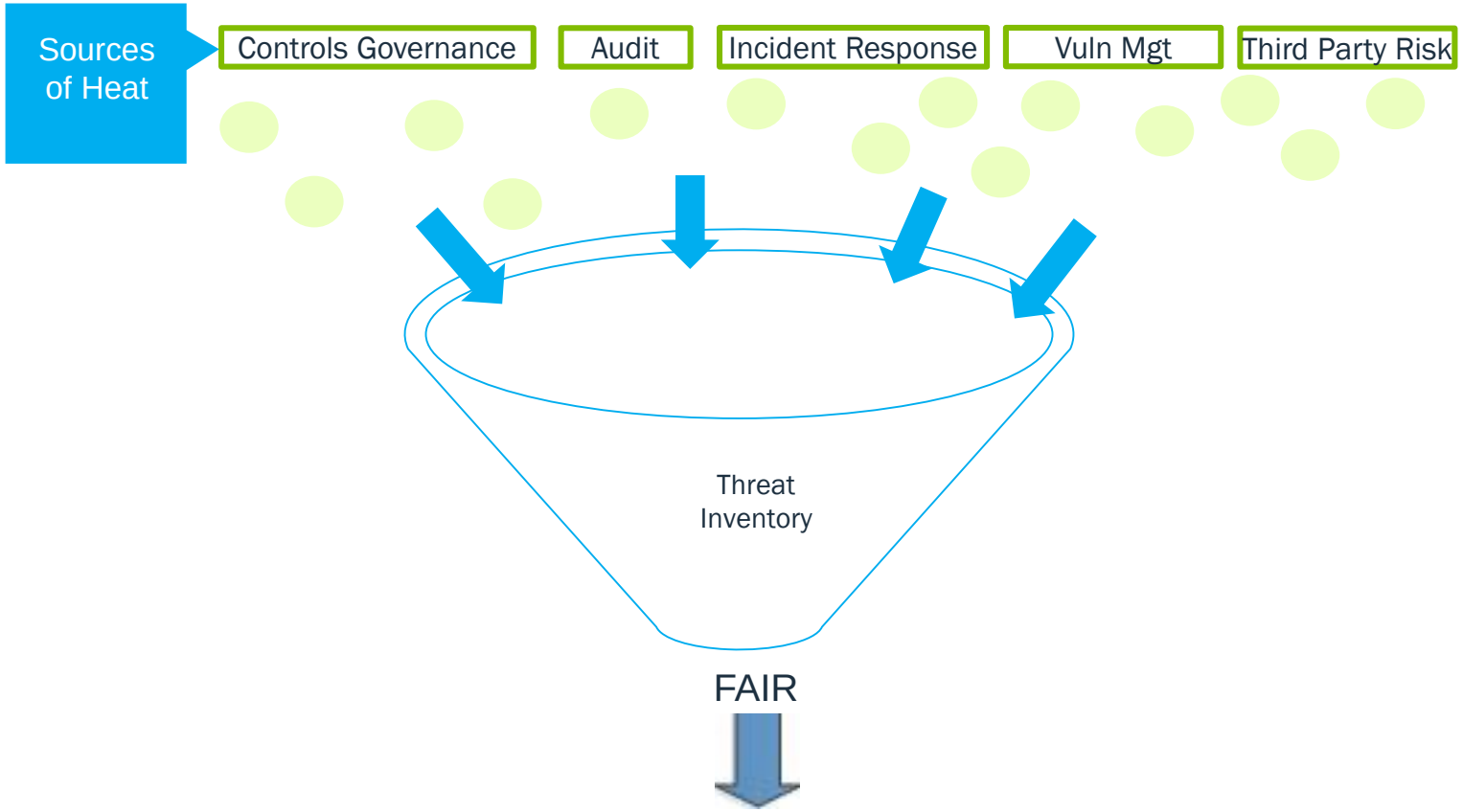
Aligned - Maps to ISRM, Audit, Privacy, ERM, etc. programs

Solution: Sources of Heat



Areas of the enterprise that feed us *potential risks*

1. Identify


Sources of Heat
Controls Governance
Audit
Incident Response
Vuln Mgt
Third Party Risk
Threat Inventory
FAIR

1. Identify

Risk Definition (FAIR):

The probable frequency and probable magnitude of future loss.

When identifying risks, a true risk must have all three:

1. **Asset:** a thing of value you wish to protect (data, reputation, etc.)
2. **Threat:** agent capable of acting in a manner that may result in harm
3. **Effect:** Confidentiality, Integrity, Availability

1. Identify

Example: Third Party Risk Management has identified a vendor who “needs to” place a managed server on our clinical network, connected by VPN tunnel.

Asset: Hospital Enterprise Health Record (EHR) services.

Threat: Cyber Criminal compromises vendor with ransomware that spreads to AHN connected systems.

Gap	Control	Threat
1	09.j Controls Against Malicious Code	LIN32: Ransomware

Effect: Loss of Availability

Result

Risk Scenario: LIN32 acts on 09.j control gaps causing a loss of Availability of Asset.

1. Identify

- **Aligned** - Sources of Heat allow us to gather input at a moments notice, mitigating the possibility of “unknown” risks

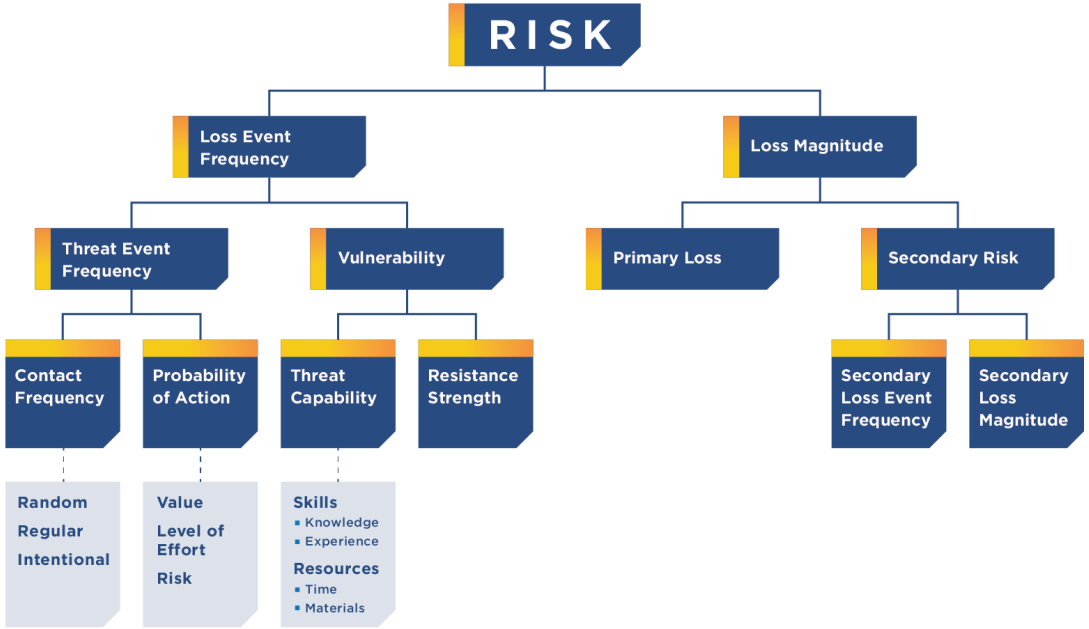
Lessons Learned:

1. Map control gaps to threats
2. Rigorous risk definition helps filter “noise” into actionable risk scenarios

2. Quantify

- **Rational** – Results must be built upon robust and defensible logic
- **Audience-Centric** – Express risk in business terms ($$)

FAIR Model: Decompose each risk into its quantifiable contributing factors

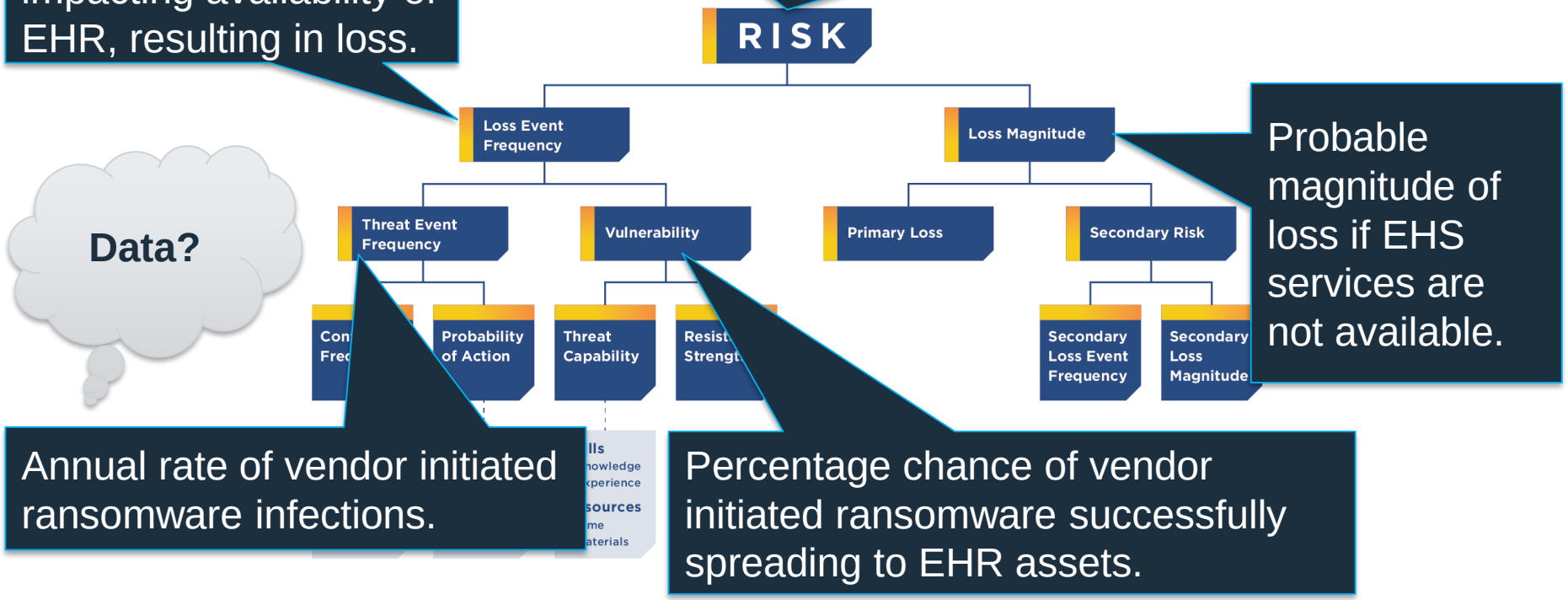


2. Quantify

Scoping: Define the risk scenario's logical factors using the FAIR ontology

Probable frequency and probable magnitude of future loss due to third-party ransomware attack impacting EHR availability.

Probable frequency of ransomware attack impacting availability of EHR, resulting in loss.



Probable magnitude of loss if EHS services are not available.

Annual rate of vendor initiated ransomware infections.

Percentage chance of vendor initiated ransomware successfully spreading to EHR assets.

2. Quantify

Hi Team,

Please reply to this message with the requested data or the name of the resource you have assigned to participate in this analysis.

The resource will be contacted shortly after with a meeting invite.

Facilitator:	[Team Member(s)]
Subject:	[Assessment Name] FAIR LEF Session Request
Purpose:	Cyber Risk Management is requesting a resource from the following groups to participate in gathering the data detailed below, as agreed upon in the Engagement Model between your team and Cyber Risk Management.
Loss Scenario:	[Insert Scenario from Scoping Document] [Attach Scoping Document]
Data of Interest*:	LEF: [Refer to Pg X of Scoping Document] - [Team/representative(s)] TEF: [Refer to Pg X of Scoping Document] - [Team/representative(s)] VULN: [Refer to Pg X of Scoping Document]- [Team/representative(s)] CF: [Refer to Pg X of Scoping Document] - [Team/representative(s)] PoA: [Refer to Pg X of Scoping Document]- [Team/representative(s)] TCap: [Refer to Pg X of Scoping Document]- [Team/representative(s)] RS: [Refer to Pg X of Scoping Document] - [Team/representative(s)]

*Sufficient data will not always be available for each model element listed above. In such cases, you may be asked to provide your best estimate of what the value could be. This will be an open-ended discussion led by a FAIR-certified assessor who can help you arrive at a reasonably accurate and precise estimate.

Thank you,
[Your Signature]

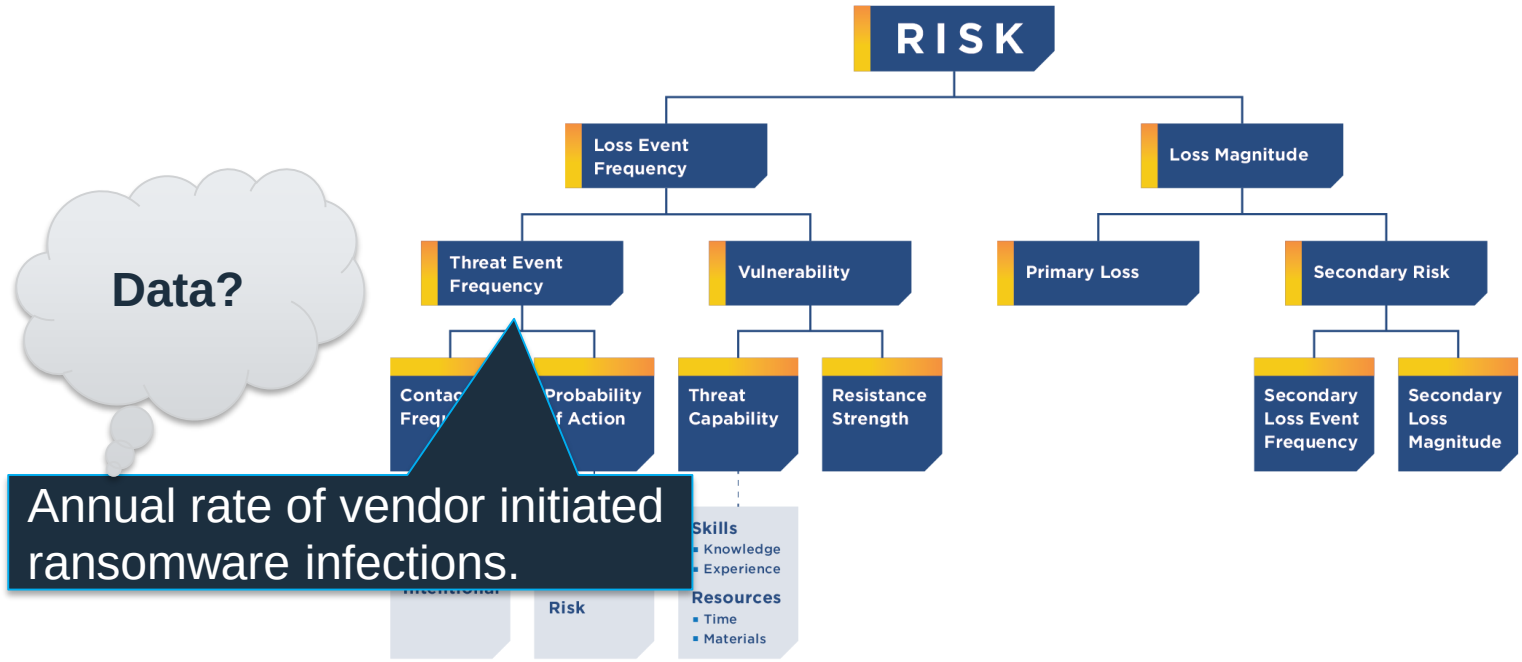
2. Quantify

Expert Estimation:

Min = **?**

Max = **?**

Most Likely = **?**

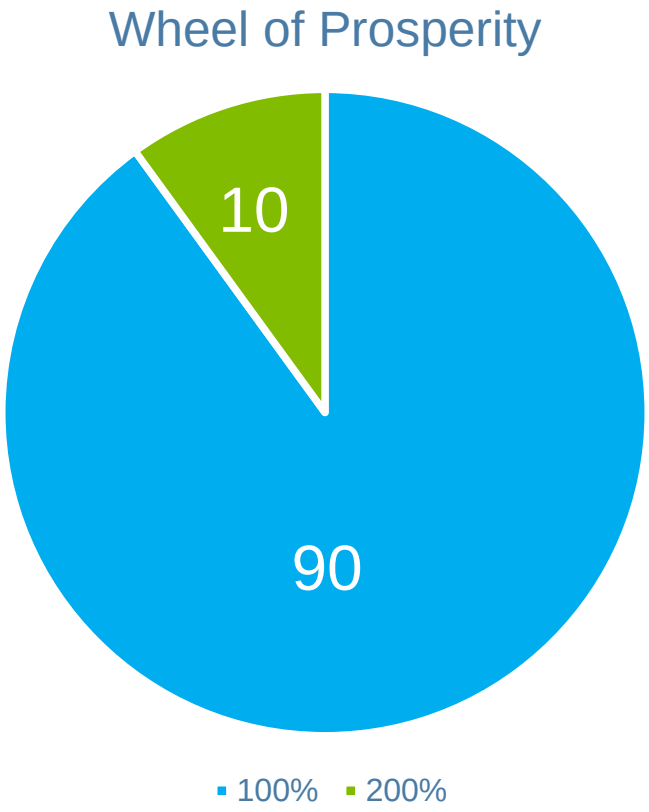


2. Quantify

Equivalent bet test:

Land on the **green** to win $1,000,000

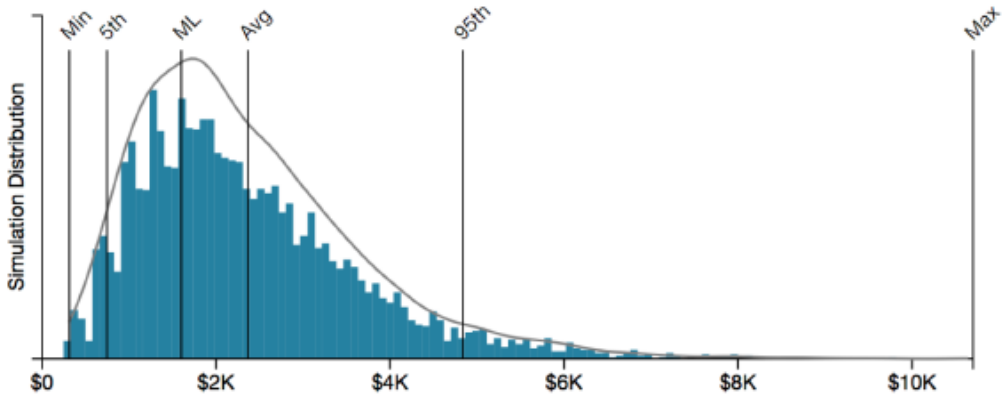
or win $1,000,000 if your range is correct?



2. Quantify

Quantification: Crunch the input numbers with whatever engine you have available

Maximum	$11K
95th %	$5K
Most Likely	$2K
Average	$2K
5th %	$751
Minimum	$310



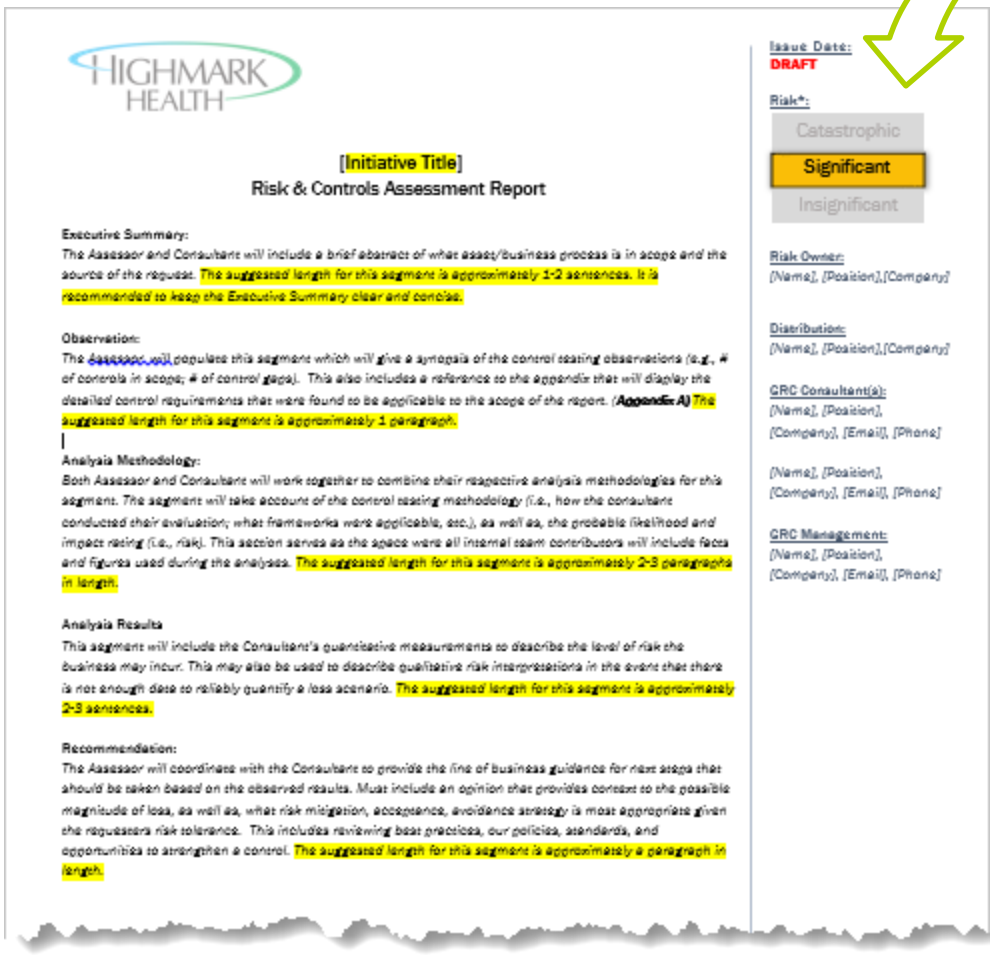
This risk is driven by:

- High Contact Frequency
- Low Resistive Strength of relevant controls

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

2. Quantify: The Report

Start with a template.



HIGHMARK HEALTH

[Initiative Title]
Risk & Controls Assessment Report

Executive Summary:
The Assessor and Consultant will include a brief abstract of what asset/business process is in scope and the source of the request. The suggested length for this segment is approximately 1-2 sentences. It is recommended to keep the Executive Summary clear and concise.

Observation:
*The Assessor will populate this segment which will give a synopsis of the control testing observations (e.g., # of controls in scope; # of control gaps). This also includes a reference to the appendix that will display the detailed control requirements that were found to be applicable to the scope of the report. (**Appendix A**) The suggested length for this segment is approximately 1 paragraph.*

Analysis Methodology:
Both Assessor and Consultant will work together to combine their respective analysis methodologies for this segment. The segment will take account of the control testing methodology (i.e., how the consultant conducted their evaluation; what frameworks were applicable, etc.), as well as, the probable likelihood and impact rating (i.e., risk). This section serves as the space where all internal team contributors will include facts and figures used during the analysis. The suggested length for this segment is approximately 2-3 paragraphs in length.

Analysis Results
This segment will include the Consultant's quantitative measurements to describe the level of risk the business may incur. This may also be used to describe qualitative risk interpretations in the event that there is not enough data to reliably quantify a loss scenario. The suggested length for this segment is approximately 2-3 sentences.

Recommendation:
The Assessor will coordinate with the Consultant to provide the line of business guidance for next steps that should be taken based on the observed results. Must include an opinion that provides context to the possible magnitude of loss, as well as, what risk mitigation, acceptance, avoidance strategy is most appropriate given the requestors risk tolerance. This includes reviewing best practices, our policies, standards, and opportunities to strengthen a control. The suggested length for this segment is approximately a paragraph in length.

Issue Date:
DRAFT

Risk*:
Catastrophic
Significant
Insignificant

Risk Owner:
[Name], [Position],[Company]

Distribution:
[Name], [Position],[Company]

GRC Consultant(s):
[Name], [Position], [Company], [Email], [Phone]

[Name], [Position], [Company], [Email], [Phone]

GRC Management:
[Name], [Position], [Company], [Email], [Phone]

Issue Date:
DRAFT

Risk*:
Catastrophic
Significant
Insignificant

Risk Owner:
[Name], [Position],[Company]

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

2. Quantify: The Report

Rational – Results are built upon robust and defensible logic

Analysis Methodology:

The data points below were considered to quantify the **probable frequency** of third-party compromise spreading to [COMPANY] to a reasonable degree of accuracy and precision:

- [COMPANY] responded to [XX} security incidents that originated from a third-party in 2018.
- [COMPANY] is not able to centrally monitor the vendors VPN network traffic to detect and respond to threats
- The server placed on the [COMPANY] clinical network will have vendor owned user accounts with root access
- [VENDOR] does not possess a SOC2 or SOC2 + HITRUST report

The data points below were considered to quantify the **probable magnitude** of a third-party compromise spreading to [COMPANY] to a reasonable degree of accuracy and precision:

- [COMPANY] is exposed to the following forms of loss: Response Costs, Productivity Costs, and Reputational Damage
- Due to the requested placement of this server, infection of the endpoint could move laterally to [X-X%] of all [COMPANY] networks, including EHR services.

2. Quantify: The Report

★ Rational – Results are built upon robust and defensible logic

Analysis Results:

Our analysis indicates a 16% likelihood that [COMPANY] experiences a third-party compromise originating from [VENDOR] in the next year. Should [COMPANY] lose access to EHR services due to a third party ransomware compromise, the expected loss experienced by [COMPANY] falls within the range of $1,500,000-33,300,000 with a most likely loss of $2,800,000 experienced.

Opinion:

Placing the *[VENDOR]* server inside the [COMPANY] network introduces the risk of third party malware compromise impacting the availability of EHR services. It is recommended that [VENDOR] adhere to [COMPANY] standard remote support connectivity methods agreed to within the Business Associate Agreement (BAA) to mitigate the risk of third-party compromise. Without a root cause analysis identifying why the system is experiencing performance issues, an exception to relevant policy and control requirements to move the server inside the AHN test network is not acceptable.

2. Quantify: Quality Review

2. Quantify

- **Rational** – FAIR model provides defensible data gathering and risk analysis methodologies.
- **Audience-Centric** – Express risk in business terms

Lessons Learned:

1. Automate as much as possible with templates, common contact lists, data repositories, etc.
2. You have more data than you think
3. You need less data than you think

"If a man tells you he knows a thing exactly, then you can be safe in inferring that you are speaking to an inexact man."

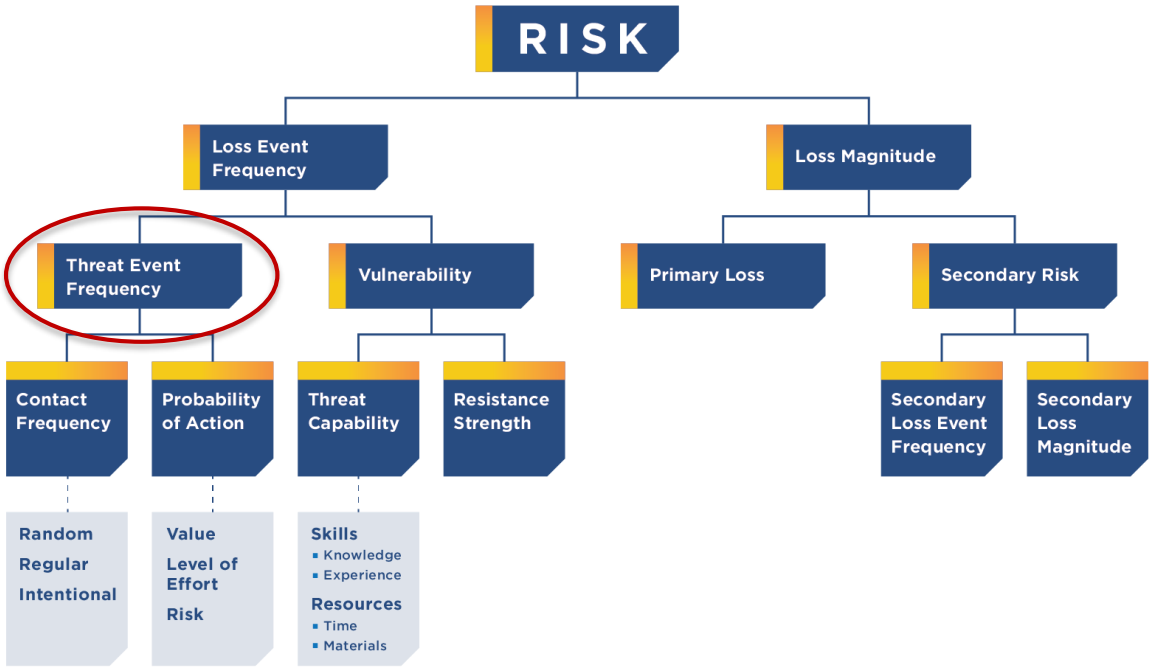
– Bertrand Russell, Mathematician and Philosopher

(Hubbard, How To Measure Anything in Cybersecurity Risk)

3. Manage

- **Decision Support** – results should simplify taking appropriate actions
- **Measurable** – able to compare business units and track trending

Target the factors most responsible for driving the risk, solve for lowest Total Cost of Risk (TCOR)

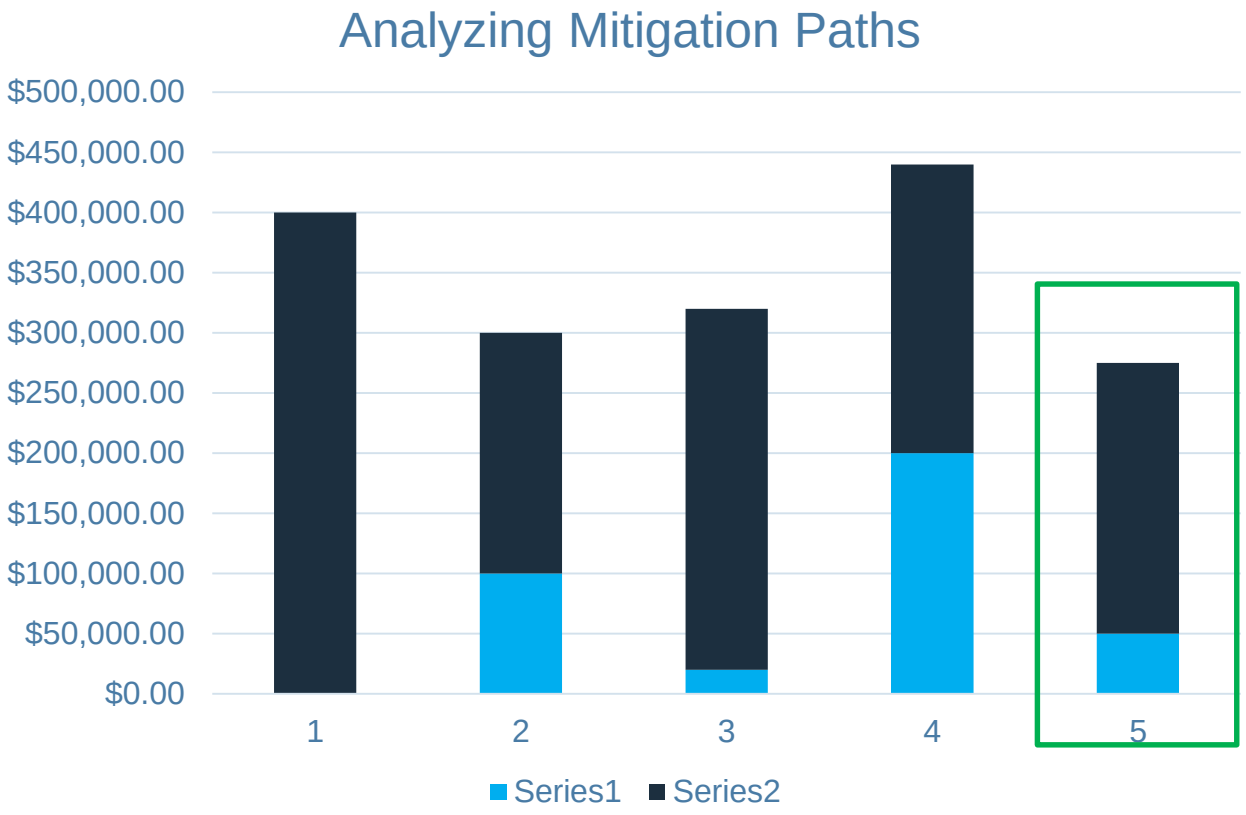


3. Manage

Mitigation Option	Cost of mitigation	Risk Reduction	Residual Risk	TCoR (Cost of mitigation + Residual Risk)
A: Network Segmentation	$100,000	$-200,000	$200,000	$300,000
B: User Awareness Training	$20,000	$-100,000	$300,000	$320,000
C: Threat Intelligence Product Purchase	$200,000	$-160,000	$240,000	$440,000
D: Improve OS Patch Rate	$50,000	$-175,000	$225,000	$275,000

3. Manage

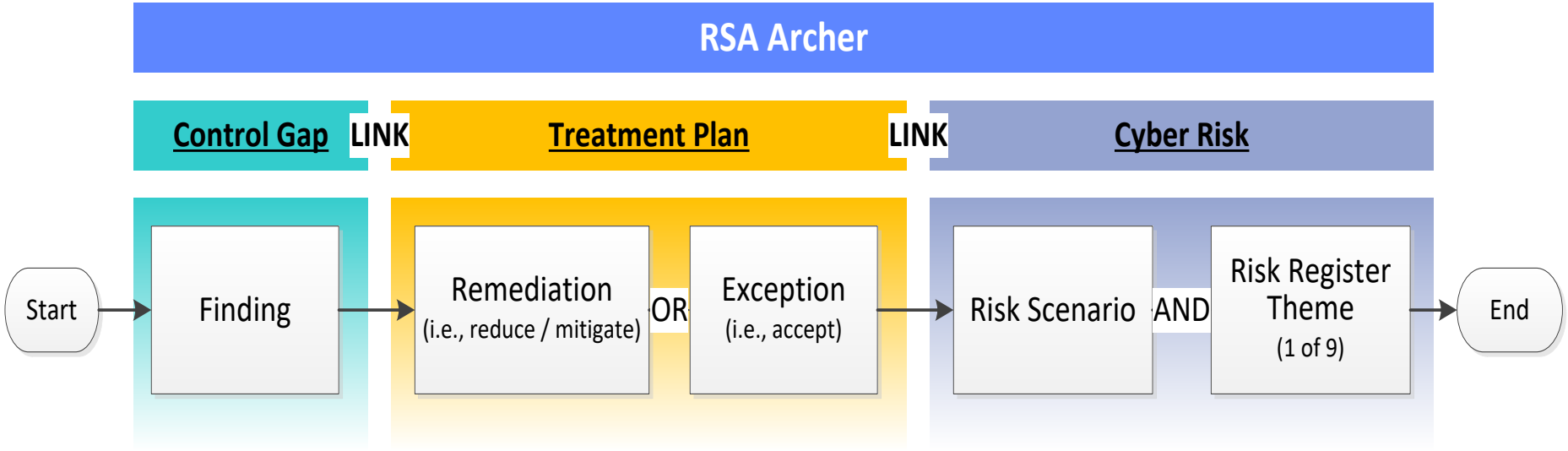
Decision Support – results should simplify taking appropriate actions



Maximized Control Value = Lowest Total Cost of Risk (TCOR)

3. Manage

Measurable – Manage control remediation



Quantified Cyber Risk Program

Key Outcomes:

1. Measurable – able to compare business units and track trending
2. Aligned – maps to other parts of the Cyber program (controls, audit, etc.)
3. Rational – results are built upon robust and defensible logic
4. Audience-Centric – Express risk in business terms
5. Decision Support – results simplify taking appropriate actions

Steps to Achieve:

1. Identify – Know what risks you face
2. Quantify – Understand the logical factors driving the risk
3. Manage – Influence the factors that put your business at risk

Resources

- FAIR Institute
  - https://www.fairinstitute.org/
- Measuring and Managing Information Risk: A FAIR approach
  - Jack Jones and Jack Freund
- Control Framework (HITRUST, NIST, etc.)
- Threat Catalog (HITRUST, MITRE, etc.)
- Risk Taxonomy
  - https://www.opengroup.org/certifications/openfair
- How To Measure Anything in Cyber Security Risk
  - Douglas W. Hubbard & Richard Seiersen