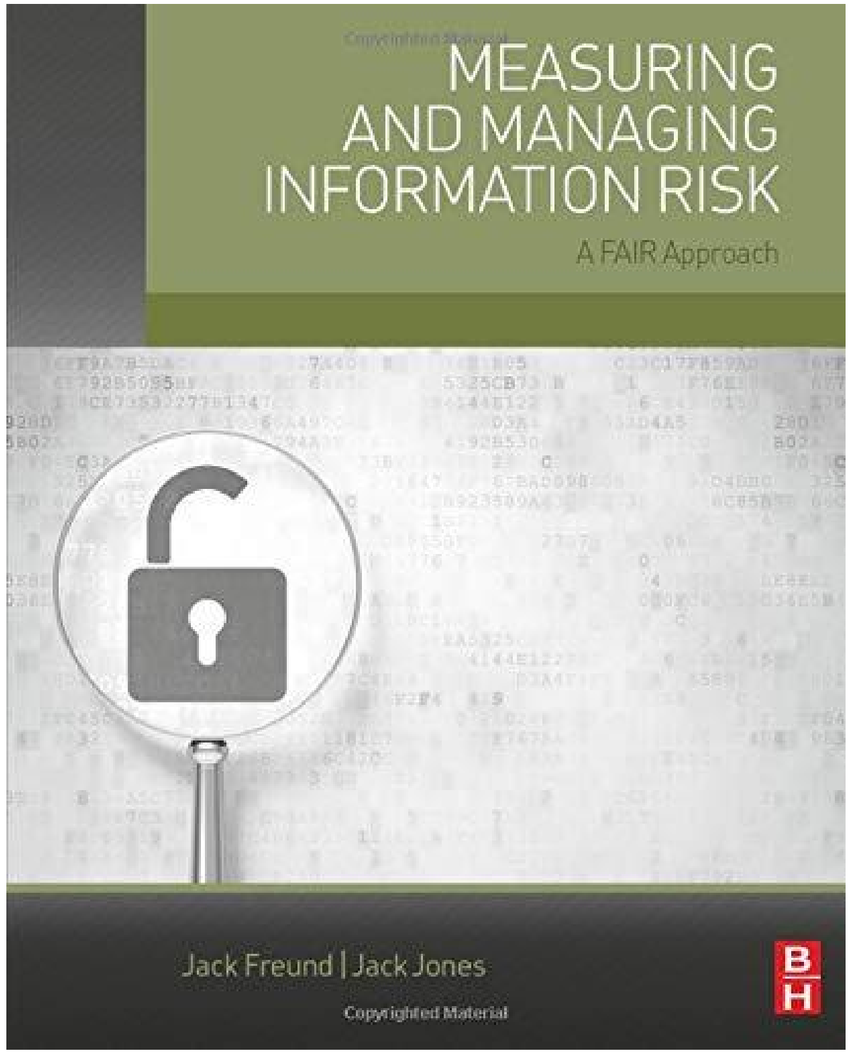
BOOK CLUB

Measuring and Managing Information Risk

Part 6: Chapters 12 - 14



What Will We Cover Today?

Use the following guide during your book club to drive discussion around the chapters outlined

Chapter 12

Risk Management

Chapter 13

Information Security Metrics

Chapter 14

Implementing Risk Management

Chapter 12: Risk Management

Take 10 - 15 mins to answer the questions below. Spend the next 10-15 mins talking through your answers and understanding where the group has similarities and differences.

1

What is your definition of effective risk management?

2

How does your organization meet the expectation of effective risk management?

3

How does your organization not meet these expectations?

4

Identify 3 - 5 areas where you could begin to implement the attributes of effective risk management. Where can you make improvements.

Chapter 13 - Information Security Metrics

Start with the End in Mind

Before beginning any analysis - think to yourself what question do you need to answer!? This is one of the most important things to think through prior to beginning an analysis!!

Strategic

If you need to aid in a strategic decision you may need to spend a bit more time on a detailed analysis so ensure you have defensible data to back up the decision.
Ex: Investments in new technology

Tactical

If you need to aid in a more tactical decision a quick n dirty analysis should work - here think triage or wider ranges.
Ex: Vulnerability Mgt, Policy Exception, Prioritization

Know What Metrics to Use When...

What are your key stakeholders used to seeing?

- Heatmaps
- High/Medium/Low Ratings
- Finger in the Air

Do not fear your old ways - you can (and should) still build these in to your new and advanced quantitative process to ease your stakeholders into this new reporting.

The real value you will bring is having the financial figures to back your 'High' rating - which you've never been able to defend before.

How do you see your reporting changing or staying the same after adopting FAIR?

Where will you start?

You've now gone through the entire book on FAIR - have you thought as an organization or as a small group where you can start to build FAIR into your process?

TIP! I have been practicing FAIR for +4 years and have helped many organizations implement risk management programs and my #1 piece of advice is to start small. Do not try to change everything at once - it is like steering a GIANT ship. Do not expect to quantify all of your top risks, understand all of your vulnerabilities in financial terms, report to the board, and measure against a risk appetite all in the first year.

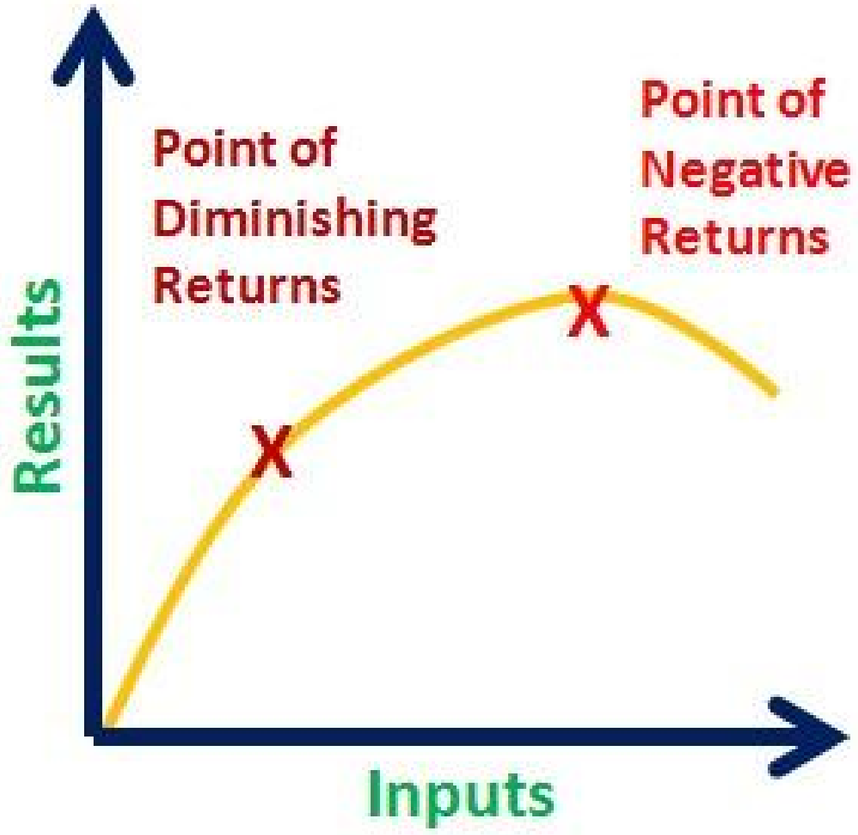
Start with what matters most!

Law of Diminishing Returns

When new analysts are starting out one of the biggest issues I see is analysis paralysis. We are analysts so we like to analyze and strive for perfection.

You need to make it your main focus to give answers when the questions are still being asked - know when an analysis is good enough to answer the question at hand!

How will you pull yourself out of the weeds and stay on track?



Chapter 14: Implementing Risk Management

This chapter goes deep into how you can begin to use FAIR to manage your risk portfolio. What are your general thoughts on how you can apply this new knowledge in your organization?

Do you expect you will get pushback or others will shut you down? How can you make a strong case for looking at risk in financial terms?

To the right are some key ways to begin the conversation - are there some you've done or would like to do?

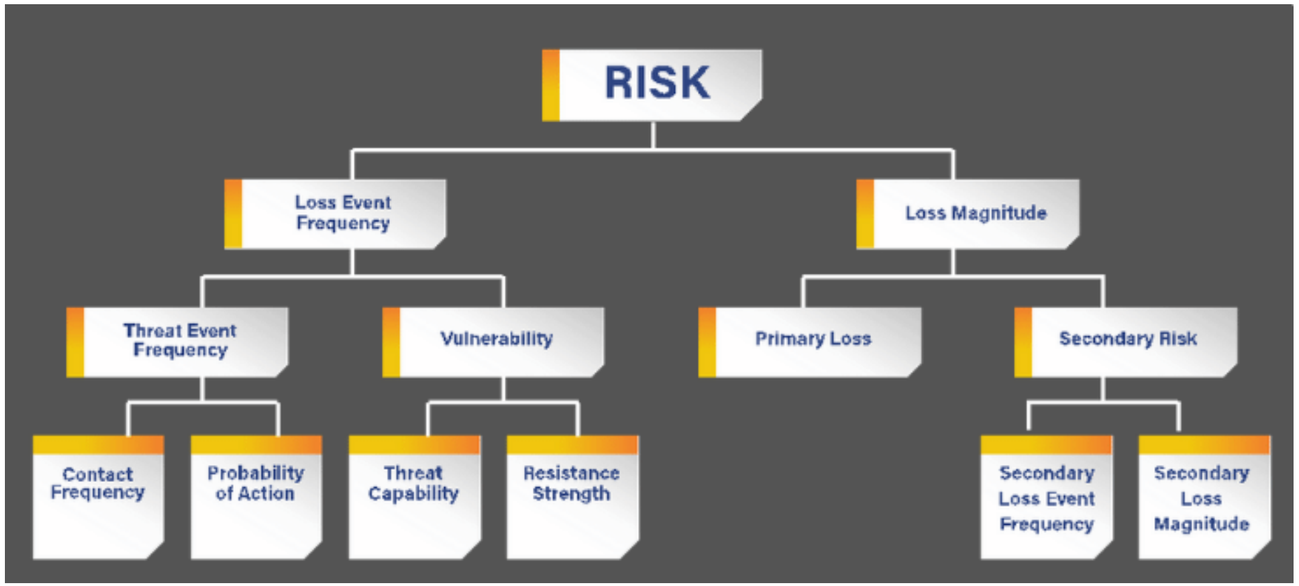
- Attend a FAIR Chapter Meeting
- Take FAIR Fundamentals Training
- Begin to measure top risks
- Measure vulnerabilities in $'s
- Train internally
- Meet other practitioners
- Understand policy changes that drive quantification

Final Book Club Guide

Congratulations - You've Made It!

You've made it to the end of book club. Please use this guide as a starting place for the many conversations to come today and in the future on risk management. This is not an easy subject - but we are the ambitious ones that believe there is something better than rating risk with a color or a finger in the air!

Keep looking and keep measuring - it can only go up from here!



Final Thoughts?

Open discussion...

Join the Book Club discussion online! Share your club's insights, your feedback to the Guide or pose a question at the FAIR Institute's LINK community site (FAIR Institute membership and LINK signup required).

Join the Book Club discussion online!