FAIR CONFERENCE 2019

Operationalizing Risk Quantification in Business Processes

JACK WHITSITT

SVP & FAIR Team Lead,
Bank of America

Why this talk?

FAIR CONFERENCE 2019

FAIR is useful “out of box”

FAIR can be easier

FAIR can be better

“Successful Program” goes far beyond “FAIR”

Who am I?

FAIR CONFERENCE 2019

- Co-Founded (Sheronas!) FAIR Team at the bank 3 years ago as first analyst, now leading a team of 8
- Board Vice President of Society of Information Security Risk Analysts (SIRA)
- 4 years at a non-profit
  - Building risk frameworks, teaching risk and how to build risk frameworks
  - Aiding information sharing in the Energy Sector
  - Occasional contributor to international cyber security policy discussions
- Several years in government coordinating Transportation Cybersecurity Public/Private Partnerships
  - Including launching a pipeline sector collaborative risk assessment
- National Critical Infrastructure Incident Response & Coordination (INL/DHS/NCCIC)
- Security Architect, Data Analysis & Visualization Artist, Builder of SOCs, Open Source Honeypot
- Backpacker, Cybersecurity Psychologist, Conceptual Lens Maker, Frequent Vagabond, Online 1987

About This Talk

FAIR CONFERENCE 2019

- **Slicing and Dicing the topic in three ways:**

  1. Program Success Attributes: What's a good program?
  2. Problem Spaces: How to think through your program
  3. Solution Spaces: Modularized ideas for Successful program

- We'll go through high level, use open questions to target detail

- **How to process this information:**

  - You are different; cherry pick ideas
  - The links between "Success Criteria", "Problems", "Solutions" is intentionally NOT made explicit (complex relationships)

Risk Quantification & Forecasting Program Success Qualities

FAIR CONFERENCE 2019

Meaning (Context)	Defensibility	Scalable	Sustainable	Impact
Technology	Problem / Scope Consensus	Modularity	Analysis Timelines	Decision Targets
Culture	Data Consensus	Coherence	Resource Burn	Information Arrangement
Language	Method Consensus	Availability	Focus	
Decision Frameworks	Resource Consensus		Quality	

Success Barrier Framework

FAIR CONFERENCE 2019

Program Management & Business Integration

Modeling Development & Enhancement

Team Structure & Dynamics

Program Management & Business Integration Barriers

FAIR CONFERENCE 2019

What problem?	Target Coordination	Process Shifting	Consensus & Defense	Human Brain Mgt
InfoSec History: Tech	Topics of Interest	Risk as a Namespace	Beliefs & Memes	Uncertainty
Implicit vs Explicit Risk	Shared Pain	Frontal Assaults	Engagement & Inclusion	Calibration
“It is known, Khaleesi!”	Scope Coherence	Augment or Supplant	Complex Unintegrated Views	Decomposition

Modeling Development & Enhancement

FAIR CONFERENCE 2019

Explicit Risk Management Framework	Decision Frameworks	Loss & Appetite	Metrics	Aggregation & LEGOs
Risk “Architecture”	Binary	Businesses Don’t Feel Risk	Measures vs Metrics	What ARE controls?
Measurement & Forecasting	Budget	A Dollar Isn’t a Dollar	Tail Wagging the Tail	Kill….Chains?
Risk Management Execution	Agility	Outcome vs Certainty	Inappropriate context	Scope Potatoe Scope Pototo
	Attrition			

Try Not Using the Word Risk

Team Structure & Dynamics

FAIR CONFERENCE 2019

Decomposition		
Converging Skills	T Shaped	Pairing

"Obvious" Skills	
FAIR	InfoSec
Cognitive Science	"MBA" / Business Ops
Facilitation	Decomposition

Less Obvious Skills	
Teaching	Modeling
Conflict Mgt	Anthropology
Comms	Hacker Mindset
Library Sci	

Yes. These, too.	
Storytelling	Kindness
Empathy	Humor
Curiosity	

Working Model of a FAIR Program

FAIR CONFERENCE 2019

Explicit Risk Management Question Framework

- Risk Architecture
- Measuring & Forecasting
- Risk Management Execution

Engagement Vehicles

- Governance
- Scenario & Targeting
- Data & Modeling

Analysis Team

- Front End
- Mid
- Back

Building Blocks

- Scenario Templates
- Loss Models (RCSA + Red Team?)
- Control Impact Models
- Aggregation & Scope Heuristics
- Articles of Risk Faith

Products & Services

- Tools
- Reference Quantities
- Analysis

Training & Socialization

- FAIR
- Decision Theory
- Branding /Marketing

Recap and Important Points

FAIR CONFERENCE 2019

- Problem Spaces
  - You're solving a largely unrecognized problem
  - A Dollar isn't the same dollar for everyone
  - InfoSec is entirely about implicit risk management; controls and metrics need translation
  - Consensus Management is Hard & Key, but Modularized Pre-Consensus Processes can help
    - Timeline management
    - Resource management
    - Acceptance and defensibility

- Solution Spaces
  - Your program as an iterative operational excellence tool making risk management explicit
  - Have an explicit risk management Goal/Question/Indicator/Measure framework
  - Have a Governance Process (Certification/Consensus, Priorities, Resourcing)
  - Have Targeting Process (Topics most likely to be analyzed pre-identified, pre-gathered)
  - Operate in context: Articles of Risk Faith and Decision Modeling
  - Operate at sustained scale: Data Tokenization/Modularization
  - Manage Long Term Data/Estimation Provisioning Assignments: It takes a village (Everyone is relevant)
  - Hire for culture shifting

- Think through your program and organization without using the word "Risk"

You can do it, don't be overwhelmed. Decompose, address gaps

Legal Disclaimer

FAIR CONFERENCE 2019

- Neither Bank of America nor its affiliates provide information security or information technology (IT) consulting services.
- This material is provided "as is," with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this material, and without warranty of any kind, expressed or implied, including, but not limited to warranties of performance, quality and fitness for a particular purpose.
- This material should be regarded as general information on information security and IT considerations and is not intended to provide specific information security or IT advice nor is it any substitute for your own independent investigations.
- If you have questions regarding your particular IT system or information security concerns, please contact your IT or information security advisor.

FAIR CONFERENCE 2019

Questions?

Thanks for listening!

Jack Whitsitt | john.Whitsitt@bofa.com | September 2019

Now with more Detail

Risk Quantification & Forecasting Program Success Qualities

FAIR CONFERENCE 2019

Meaning (Context)	Defensibility	Scalable	Sustainable	Impact
Technology	Problem / Scope Consensus	Modularity	Analysis Timelines	Decision Targets
Culture	Data Consensus	Coherence	Resource Burn	Information Arrangement
Language	Method Consensus	Availability	Focus	
Decision Frameworks	Resource Consensus		Quality	

Risk Quantification & Forecasting Program Success Qualities

FAIR CONFERENCE 2019

Meaning (Context)	Defensibility	Scalable	Sustainable	Impact
Technology	Problem / Scope Consensus	Modularity	Analysis Timelines	Decision Targets
Culture	Data Consensus	Coherence	Resource Burn	Information Arrangement
Language	Method Consensus	Availability	Focus	
Decision Frameworks	Resource Consensus		Quality	

Risk Quantification & Forecasting Program Success Qualities

FAIR CONFERENCE 2019

Meaning (Context)	Defensibility	Scalable	Sustainable	Impact
Technology	Problem / Scope Consensus	Modularity	Analysis Timelines	Decision Targets
Culture	Data Consensus	Coherence	Resource Burn	Information Arrangement
Language	Method Consensus	Availability	Focus	
Decision Frameworks	Resource Consensus		Quality	

Program Management & Business Integration Barriers

FAIR CONFERENCE 2019

What problem?	Target Coordination	Process Shifting	Consensus & Defense	Human Brain Mgt
InfoSec History: Tech	Topics of Interest	Risk as a Namespace	Beliefs & Memes	Uncertainty
Implicit vs Explicit Risk	Shared Pain	Frontal Assaults	Engagement & Inclusion	Calibration
“It is known, Khaleesi!”	Scope Coherence	Augment or Supplant	Complex Unintegrated Views	Decomposition

Program Management & Business Integration Barriers

FAIR CONFERENCE 2019

What problem?	Target Coordination	Process Shifting	Consensus & Defense	Human Brain Mgt
InfoSec History: Tech	Topics of Interest	Risk as a Namespace	Beliefs & Memes	Uncertainty
Implicit vs Explicit Risk	Shared Pain	Frontal Assaults	Engagement & Inclusion	Calibration
“It is known, Khaleesi!”	Scope Coherence	Augment or Supplant	Complex Unintegrated Views	Decomposition

Program Management & Business Integration Barriers

FAIR CONFERENCE 2019

What problem?	Target Coordination	Process Shifting	Consensus & Defense	Human Brain Mgt
InfoSec History: Tech	Topics of Interest	Risk as a Namespace	Beliefs & Memes	Uncertainty
Implicit vs Explicit Risk	Shared Pain	Frontal Assaults	Engagement & Inclusion	Calibration
“It is known, Khaleesi!”	Scope Coherence	Augment or Supplant	Complex Unintegrated Views	Decomposition

Program Management & Business Integration Barriers

FAIR CONFERENCE 2019

What problem?	Target Coordination	Process Shifting	Consensus & Defense	Human Brain Mgt
InfoSec History: Tech	Topics of Interest	Risk as a Namespace	Beliefs & Memes	Uncertainty
Implicit vs Explicit Risk	Shared Pain	Frontal Assaults	Engagement & Inclusion	Calibration
“It is known, Khaleesi!”	Scope Coherence	Augment or Supplant	Complex Unintegrated Views	Decomposition

Modeling Development & Enhancement

FAIR CONFERENCE 2019

Explicit "Risk" Questions	Decision Frameworks	Loss & Appetite	Metrics	Aggregation & LEGOs
Risk "Architecture"	Binary	Businesses Don't Feel Risk	Measures vs Metrics	What ARE controls?
Measurement & Forecasting	Budget	A Dollar Isn't a Dollar	Tail Wagging the Tail	Kill....Chains?
Risk Management Execution	Agility	Outcome vs Certainty	Inappropriate context	Scope Potatoe Scope Pototo
	Attrition			

Try Not Using the Word Risk

Team Structure & Dynamics

FAIR CONFERENCE 2019

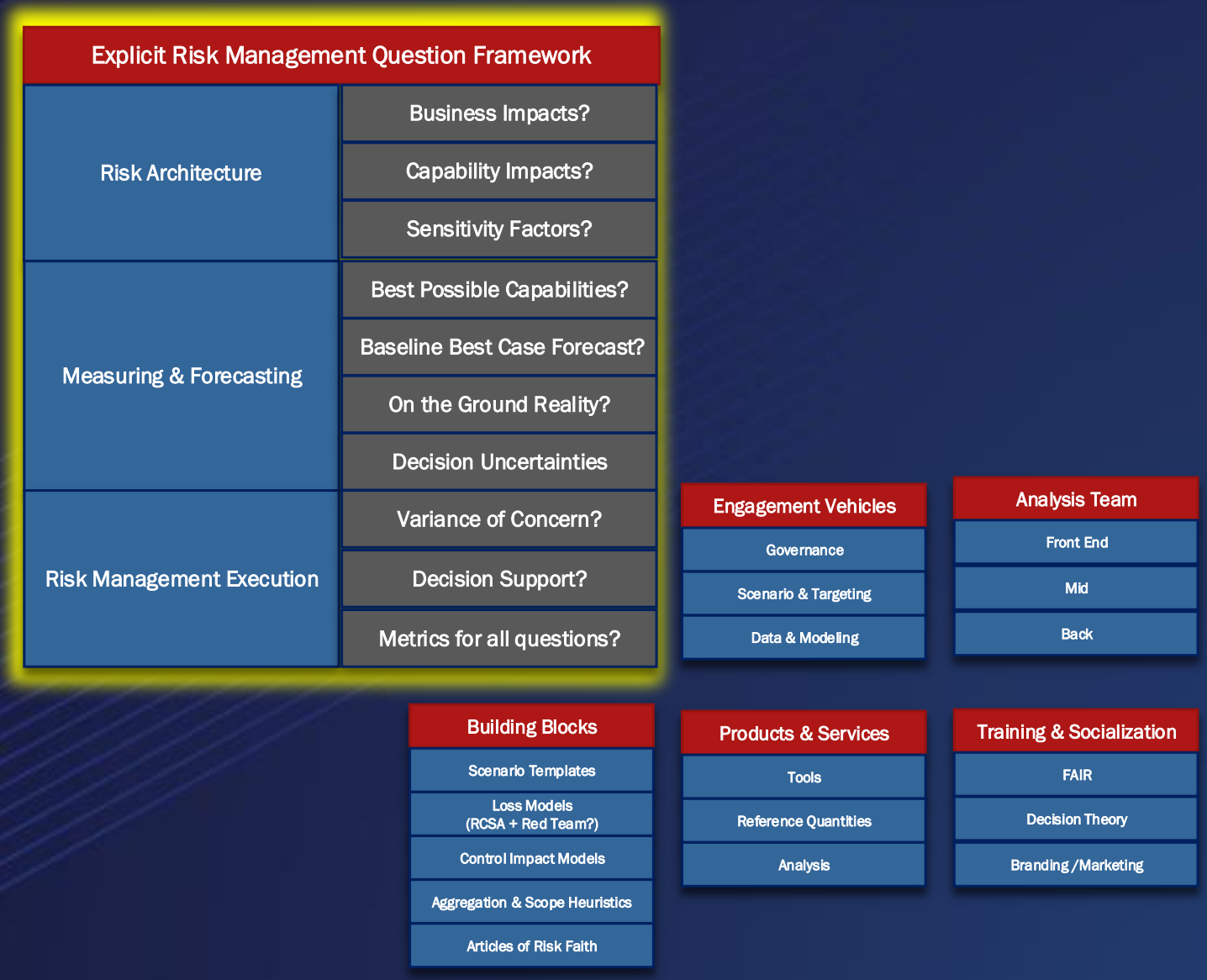
Decomposition		
Converging Skills	T Shaped	Pairing

"Obvious" Skills	
FAIR	InfoSec
Cognitive Science	"MBA" / Business Ops
Facilitation	Decomposition

Less Obvious Skills	
Teaching	Modeling
Conflict Mgt	Anthropology
Comms	Hacker Mindset
Library Sci	

Yes. These, too.	
Storytelling	Kindness
Empathy	Humor
Curiosity	

Working Model of a FAIR Program



Working Model of a FAIR Program

Explicit Risk Management Question Framework
- Risk Architecture
- Measuring & Forecasting
- Risk Management Execution

Engagement Vehicles
- Governance
- Scenario & Targeting
- Data & Modeling

Analysis Team
- Front End
- Mid
- Back

Building Blocks
- Scenario Templates
- Loss Models (RCSA + Red Team?)
- Control Impact Models
- Aggregation & Scope Heuristics
- Articles of Risk Faith
  - We believe what?
  - Meme/Tokenization
  - Measurable Attributes
  - Data/Estimation

Products & Services
- Tools
- Reference Quantities
- Analysis

Training & Socialization
- FAIR
- Decision Theory
- Branding /Marketing

Working Model of a FAIR Program

FAIR CONFERENCE 2019

Explicit Risk Management Question Framework
Risk Architecture
Measuring & Forecasting
Risk Management Execution

Engagement Vehicles
Governance
Scenario & Targeting
Data & Modeling

Analysis Team
Front End
Mid
Back

Building Blocks
Scenario Templates
Loss Models (RCSA + Red Team?)
Control Impact Models
Aggregation & Scope Heuristics
Articles of Risk Faith

Products & Services
Tools
Reference Quantities
Analysis

Training & Socialization
FAIR
Decision Theory
Branding /Marketing

Working Model of a FAIR Program

FAIR CONFERENCE 2019

Explicit Risk Management Question Framework
- Risk Architecture
- Measuring & Forecasting
- Risk Management Execution

Building Blocks
- Scenario Templates
- Loss Models (RCSA + Red Team?)
- Control Impact Models
- Aggregation & Scope Heuristics
- Articles of Risk Faith

Engagement Vehicles
- Governance
- Scenario & Targeting
- Data & Modeling

Products & Services
- Tools
- Reference Quantities
- Analysis

Analysis Team
- Front End
- Mid
- Back

Training & Socialization
- FAIR
- Decision Theory
- Branding /Marketing

Working Model of a FAIR Program

FAIR CONFERENCE 2019

Explicit Risk Management Question Framework

- Risk Architecture
- Measuring & Forecasting
- Risk Management Execution

Building Blocks

- Scenario Templates
- Loss Models (RCSA + Red Team?)
- Control Impact Models
- Aggregation & Scope Heuristics
- Articles of Risk Faith

Engagement Vehicles

- Governance
- Scenario & Targeting
- Data & Modeling

Products & Services

- Tools
- Reference Quantities
- Analysis

Analysis Team

- Front End
- Mid
- Back

Training & Socialization

- FAIR
- Decision Theory
- Branding /Marketing

Working Model of a FAIR Program

FAIR CONFERENCE 2019

Explicit Risk Management Question Framework
Risk Architecture
Measuring & Forecasting
Risk Management Execution

Engagement Vehicles
Governance
Scenario & Targeting
Data & Modeling

Analysis Team
Front End
Mid
Back

Building Blocks
Scenario Templates
Loss Models (RCSA + Red Team?)
Control Impact Models
Aggregation & Scope Heuristics
Articles of Risk Faith

Products & Services
Tools
Reference Quantities
Analysis

Training & Socialization
FAIR
Decision Theory
Branding /Marketing