Risk Quantification Introduction - FIS

May 5, 2021

Board directors are looking to understand the magnitude of enterprise risk FIS is facing

What we heard

- Amount of data too much for board meeting dialog
- Communication needs additional structure
- Metrics presented require background to interpret
- Difficult to compare risk magnitude ("materiality") across categories

Baseline benchmarking needed to assess position within industry/comparison to peers (competitors)

How we understood the ask

Present the material risks FIS is facing – ideally with a measure of magnitude against an organizational "risk appetite"

Have a **structured framework to understand and discuss risk performance** (consistently used for discussion)

Measure progress against objectives and continue to hold individuals accountable – ideally also understanding how their organization compares with others and competitors

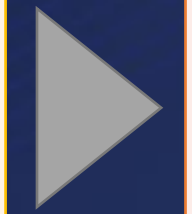
Have key decisions presented to the board – with options/implications and recommendations

Moving from implicit to explicit risk management

Implicit Risk Management
Traditional/Current Approach

Apply controls based on best practices and intuition with the hope that they will implicitly reduce our risk.

Risk reduction is expensive and hard to measure, as approach is unfocused.



Explicit Risk Management
Mature/Future Approach

Assess likely threats and map them to our most critical assets. Design controls explicitly targeted toward these threat and asset combinations.

Risk reduction is focused on the areas of greatest risk. Cost/benefit can be quantified.

FIS aligns to ISO 31000 Risk Management Framework

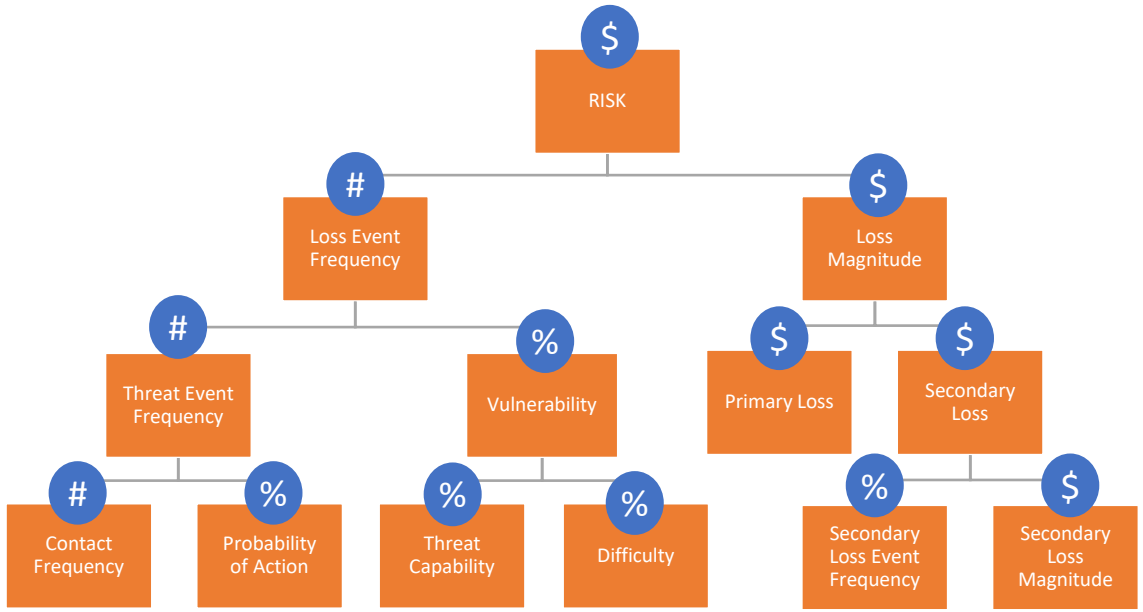
"The risk management process should be an integral part of management and decision-making and integrated into the structure, operations and processes of the organization."

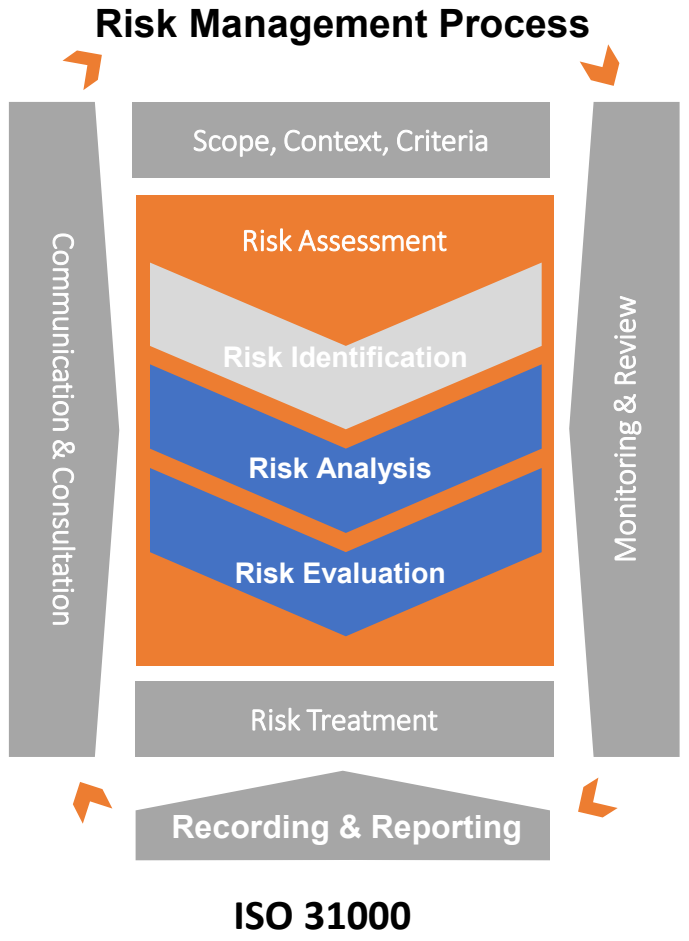
Where FAIR Fits in the ERM Framework

Risk Management is fundamentally about making decisions

- Which risk issues are most critical (prioritization)
- Which risk issues are not worth treating (risk acceptance)
- How much to spend on the risk issues that require treatment (budgeting)

Decomposing Risk with the FAIR Model

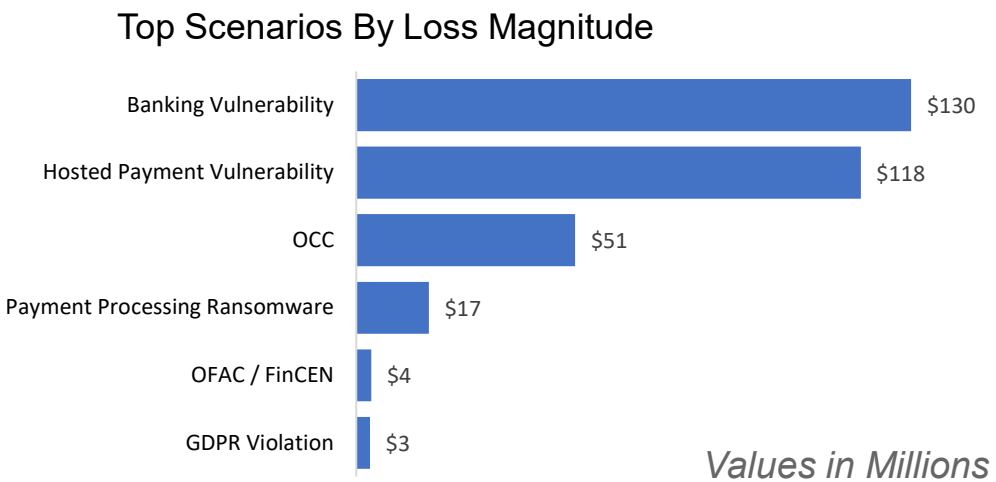




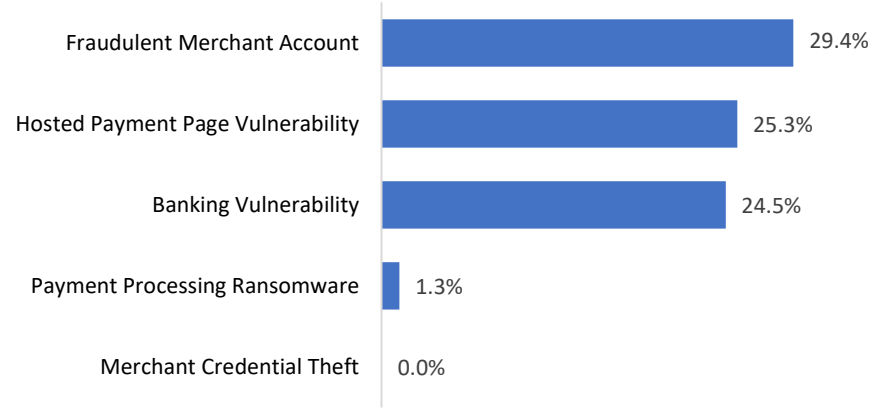
FAIR stands for Factor Analysis of Information Risk

Phase 1 Results: Top Risks Overview

What single event could cost us the most?



Which scenarios are likely to cost more than $25M next year?



Which scenarios have the greatest annualized loss estimate?

Scenario	Asset	Threat	Threat Type	Loss Effect	Minimum	10th %	Most Likely	Average	90th %	Maximum
Banking Vulnerability	Consumer PII	External	Malicious	Loss of Confidentiality	$0	$0	$0	$51.1M	$188.2M	$863.M
Hosted Payment Page Vulnerability	Consumer PII	External	Malicious	Direct Financial Loss	$0	$0	$0	$35.1M	$139.3M	$664M
Fraudulent Merchant Account	Funds	External	Malicious	Direct Financial Loss	$261.9K	$3.6M	$2.6M	$19.5M	$41.4M	$94.5M
Merchant Account Stolen Credentials	Funds	External	Malicious	Direct Financial Loss	$2.1K	$182.2K	$159.5K	$2.1M	$5.3M	$32.6M
DDoS (Nation State)	Payment Processing	External	Malicious	Loss of Availability	$0	$0	$0	$1.6M	$3.8M	$11.1M

Early Lessons Learned

- Executive sponsorship is critical
- Transformation requires top-down and bottom-up approach
- Educating analysts and identifying talent is crucial to roll-out
- Communication plan must be comprehensive and robust