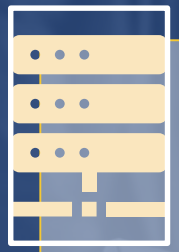
2019 Risk Management Maturity Benchmark Survey Results

Jack Freund, Ph.D.
Director, Risk Science, RiskLens
FAIR Institute Fellow

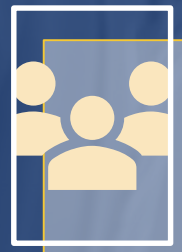
What does a mature risk management organization look like?

Appropriate policies and procedures are clearly defined and documented



Cost-effective security technologies are providing their intended value

An effective education and awareness program exists



Personnel roles and responsibilities are properly defined and staffed

Board of directors are getting the information they need

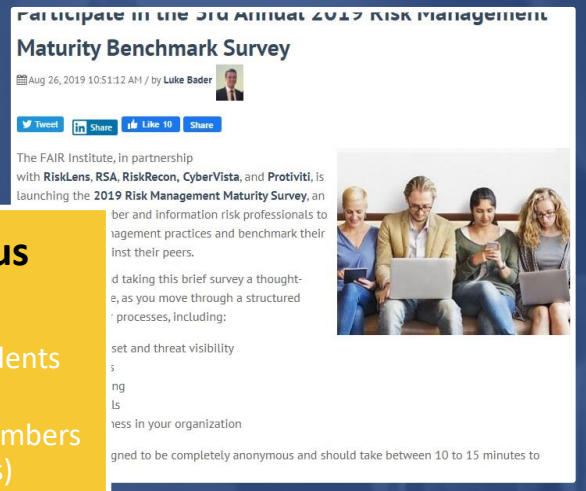
A risk register is used to track and report the most important risks

A clearly defined risk appetite actively drives decision-making

Meaningful metrics are leveraged to manage risk effectively

FAIR INSTITUTE

Risk Management Maturity Benchmark Survey


Maturity Benchmark Survey

Aug 26, 2019 10:51:12 AM / by Luke Bader

The FAIR Institute, in partnership with **RiskLens**, **RSA**, **RiskRecon, CyberVista**, and **Protiviti**, is launching the **2019 Risk Management Maturity Survey**, an

ber and information risk professionals to agement practices and benchmark their inst their peers.

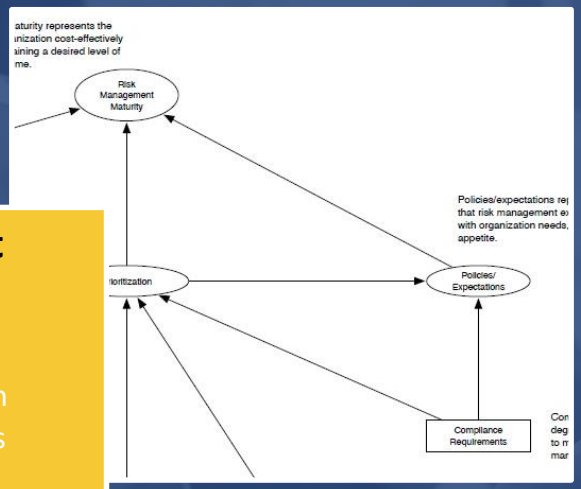
d taking this brief survey a thought- e, as you move through a structured processes, including:

set and threat visibility
ng
ls
ess in your organization

gned to be completely anonymous and should take between 10 to 15 minutes to

Anonymous Survey

- 211 respondents
- Mostly FAIR Institute members (anonymous)



Risk Mgmt Maturity Ontology

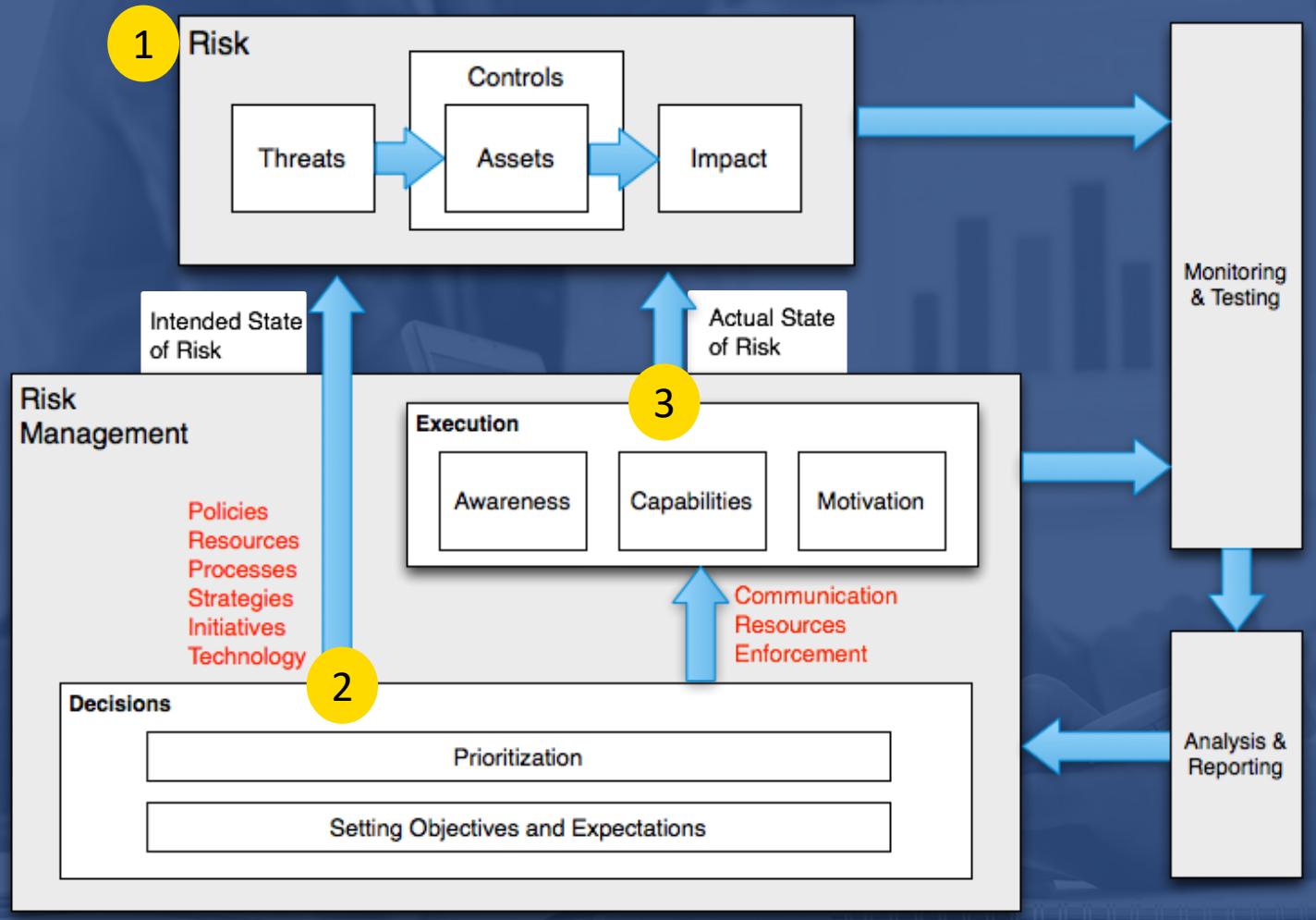
- Prioritization
- Expectations
- Execution

Report

- Slide deck
- Webinar
- Written Report

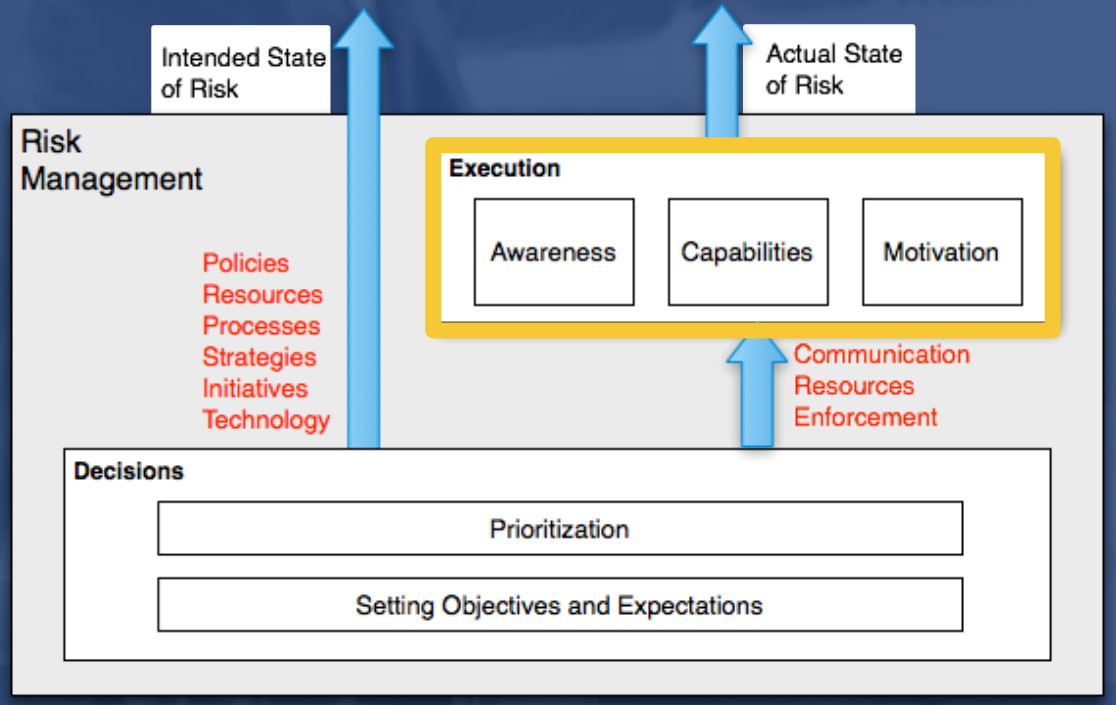
FAIR INSTITUTE

Risk Management Landscape



FAIR INSTITUTE

Assessing Execution RMM Factors

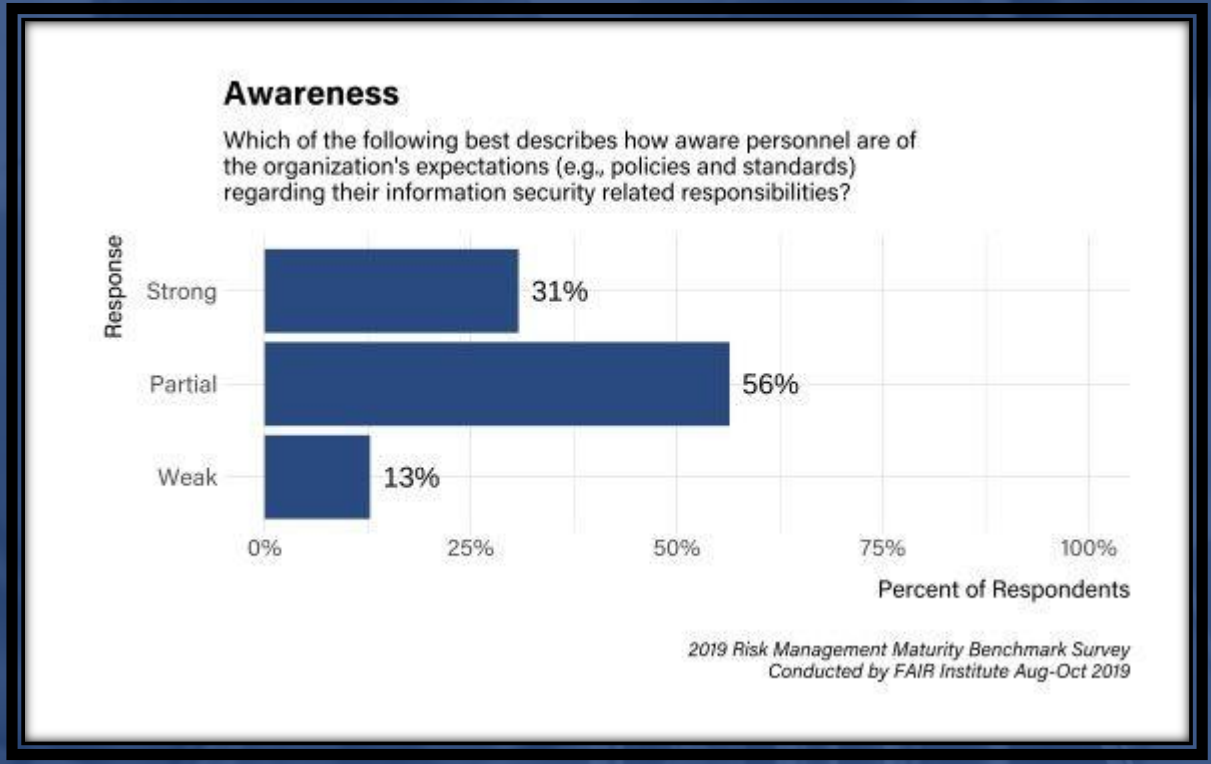


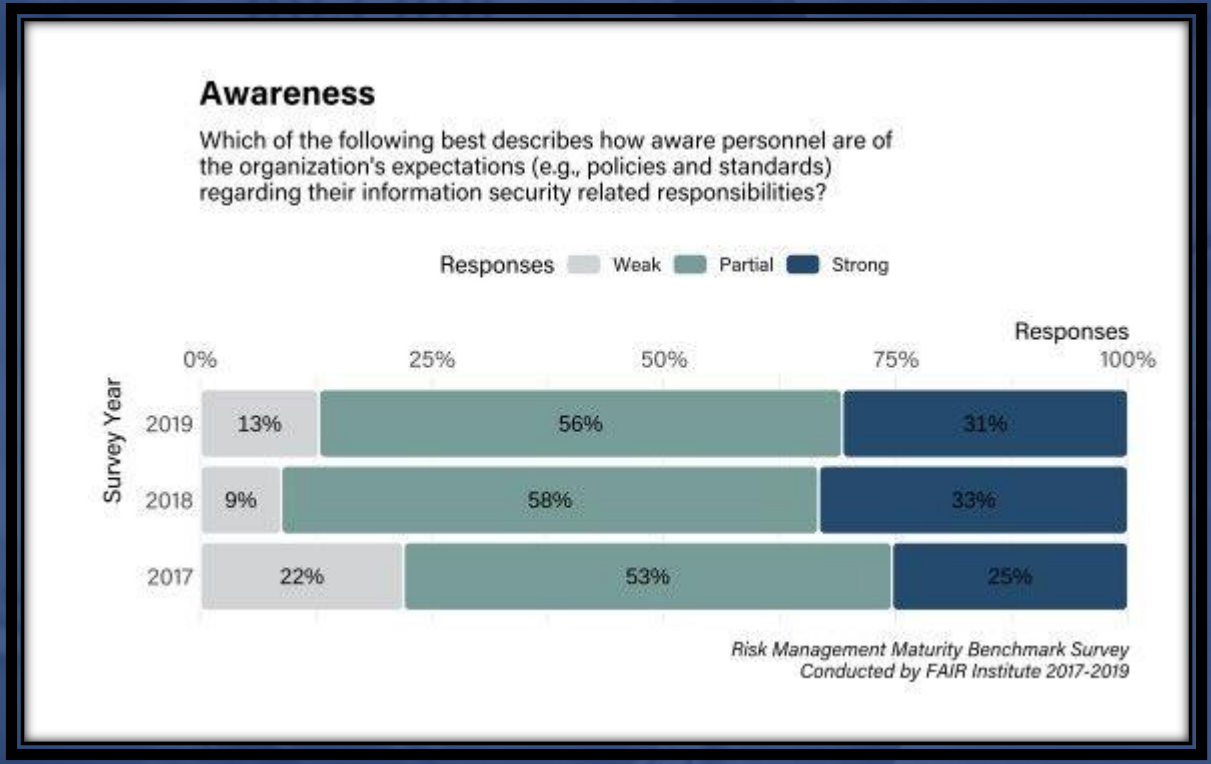
Awareness
The probability that personnel are aware of their risk management roles and responsibilities, and the specific expectations of organization leadership.

Capability
The probability that personnel have the necessary skills and resources to successfully execute their roles and responsibilities.

Motivation
The probability that personnel are appropriately incentivized to fulfill their risk management responsibilities

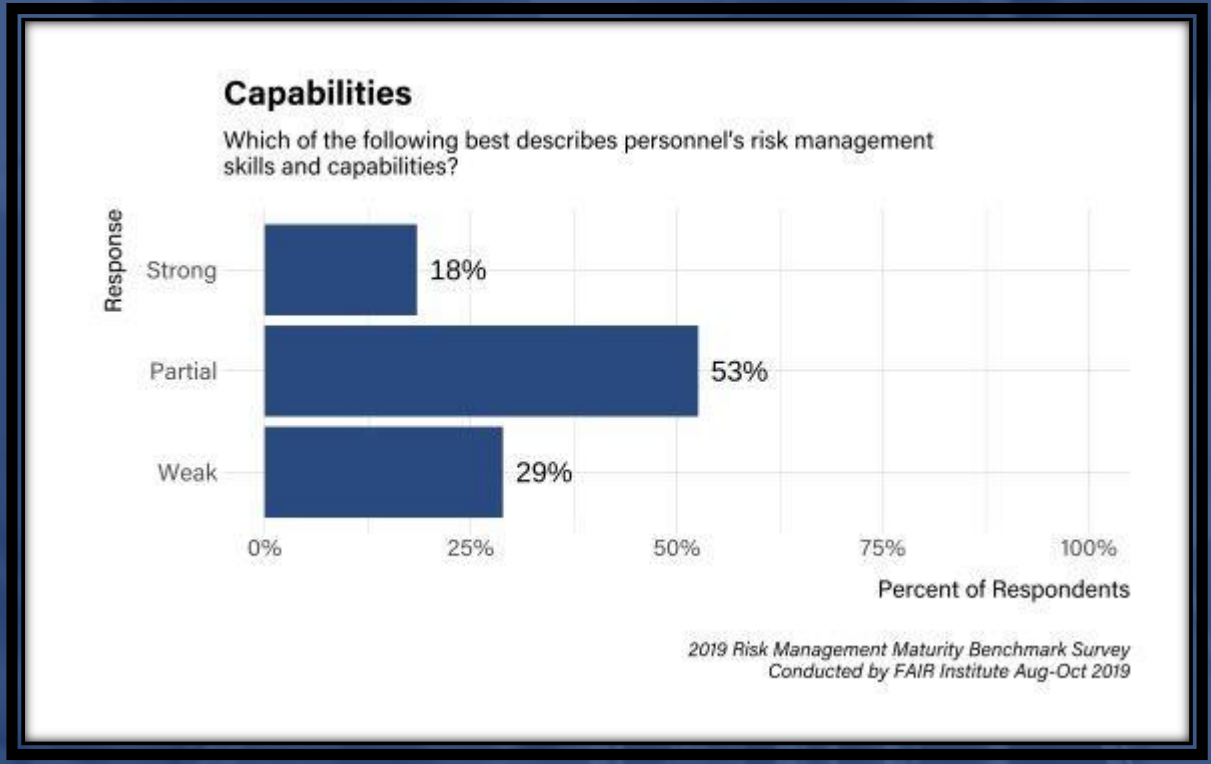
Execution: Awareness Results

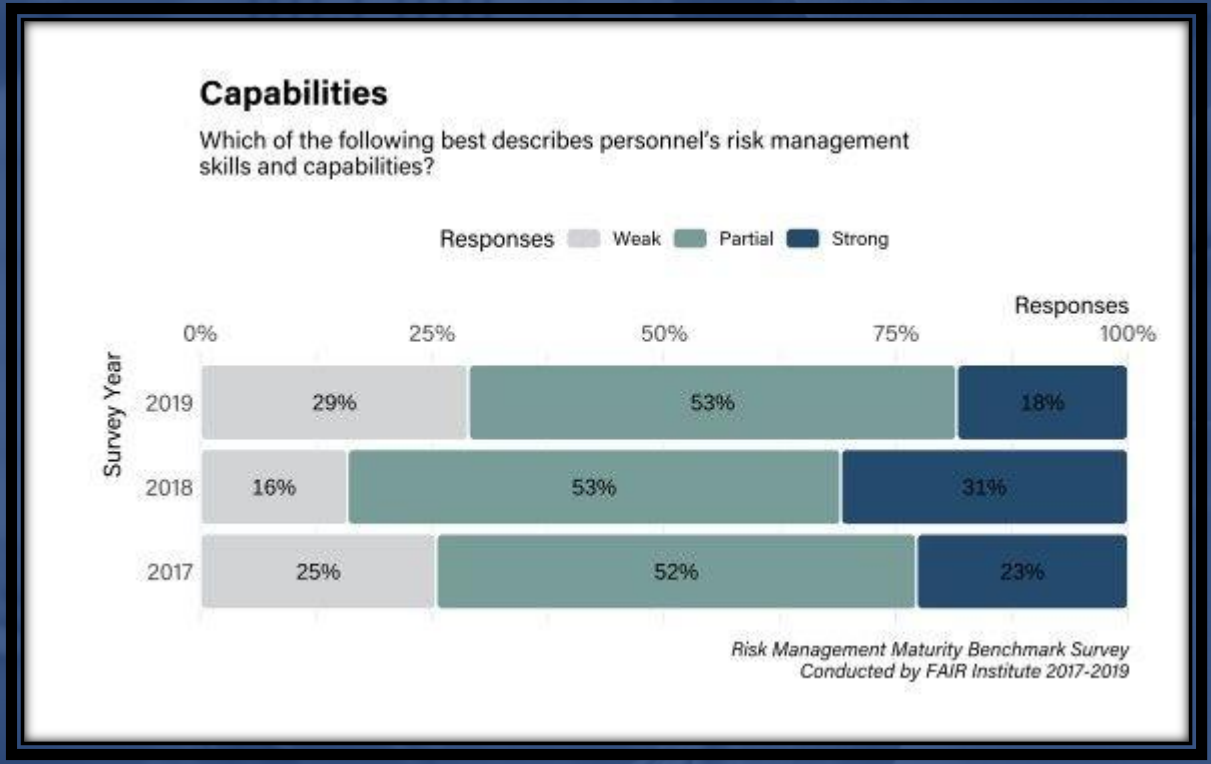




- YOY, Strong are down 2%
- YOY, Partial are down 2%
- YOY, Weak responses are up 4%
- Requires better communication and reporting of security requirements

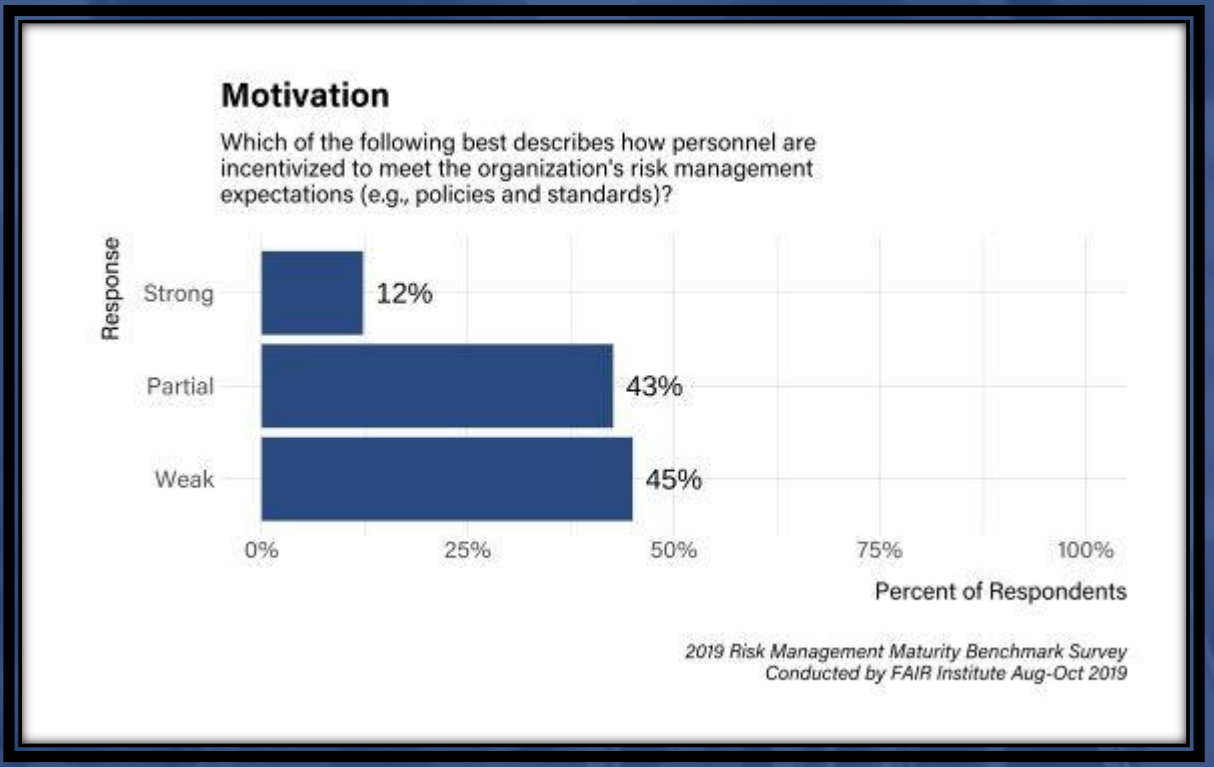
Execution: Capabilities Results

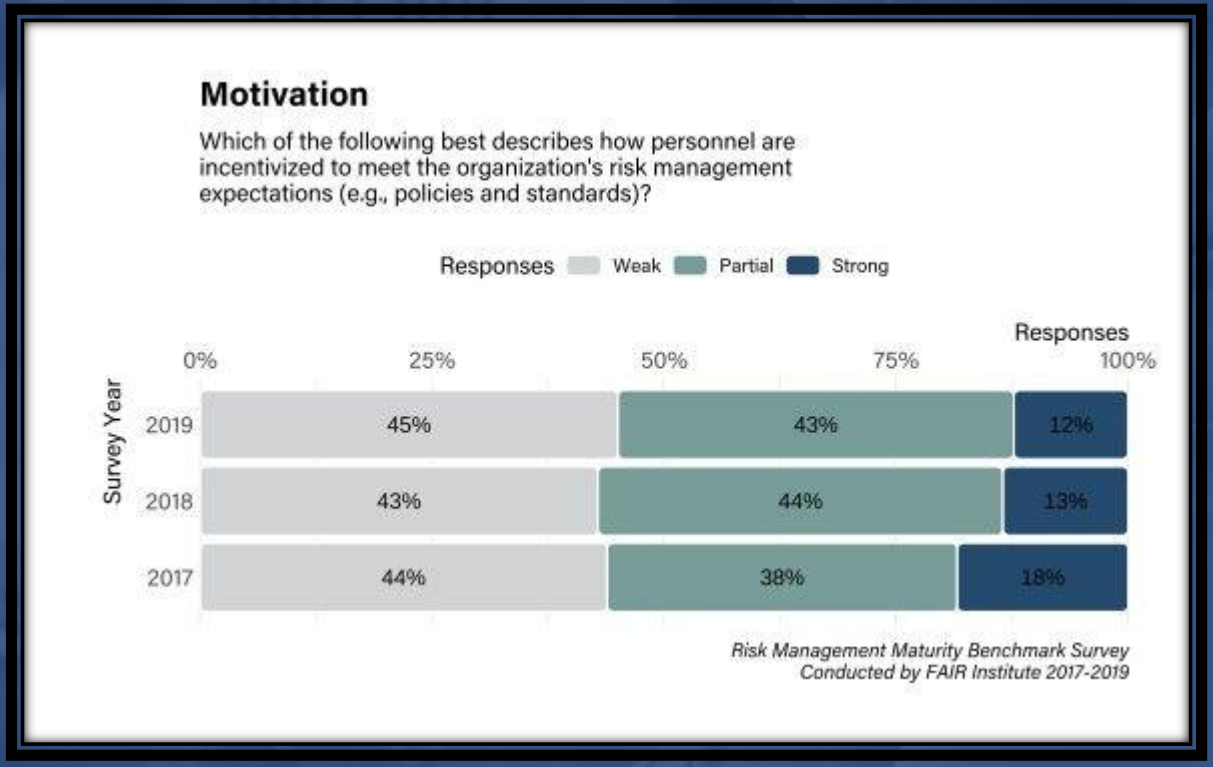




- YOY, Strong are down 13%
- YOY, Partial are flat
- YOY, Weak responses are up 13%
- Training programs and skills uplift can improve results

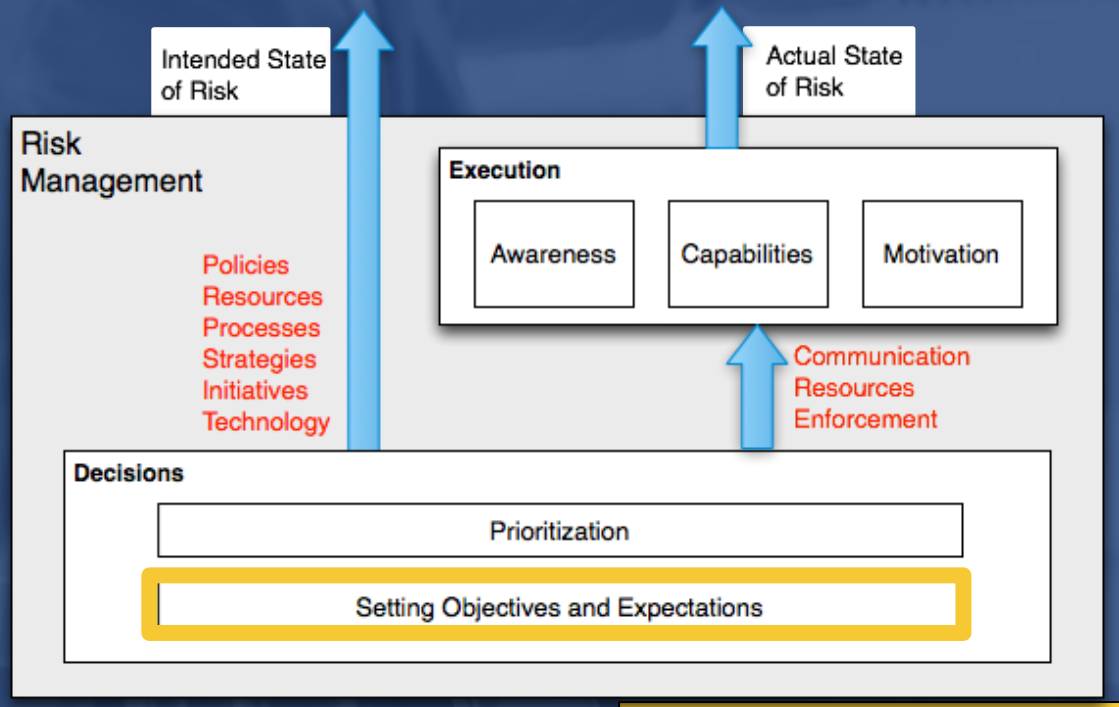
Execution: Motivation Results





- YOY, Strong are down 1%
- YOY, Partial are down 1%
- YOY, Weak responses are up 2%
- Nearly half of respondents say their org needs better motivation

Assessing Objective/Expectation RMM Factors



Compliance Requirements

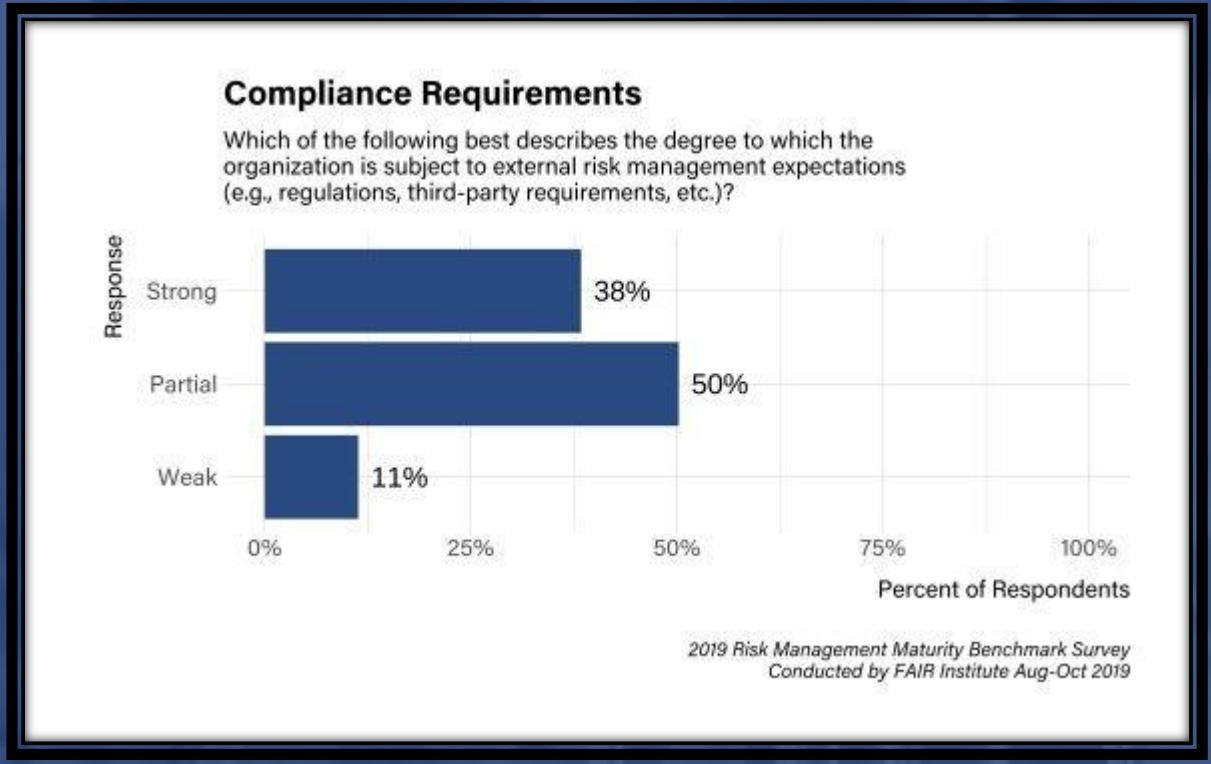
The degree to which an organization is subject to meaningfully enforced external risk management expectations.

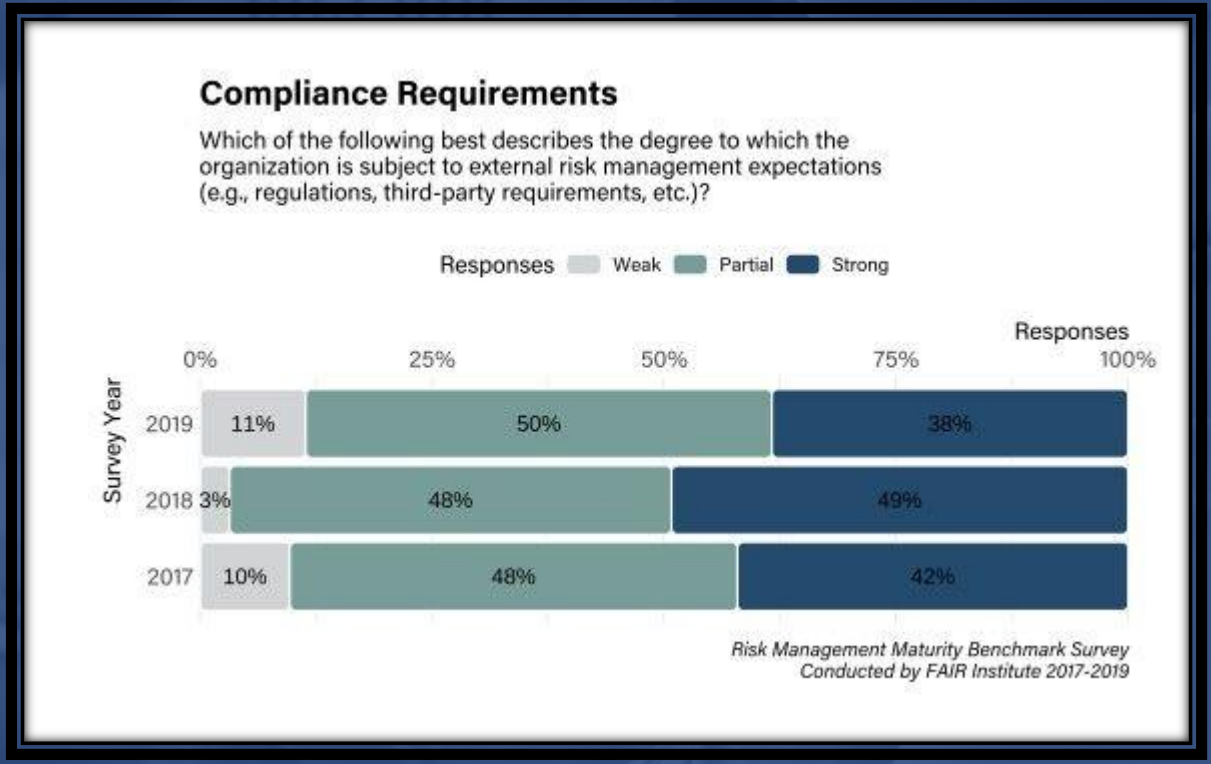
Prioritization

The probability that decision-makers are provided with the information needed to establish priorities and choose solutions, both at a strategic and operational level.

FAIR INSTITUTE

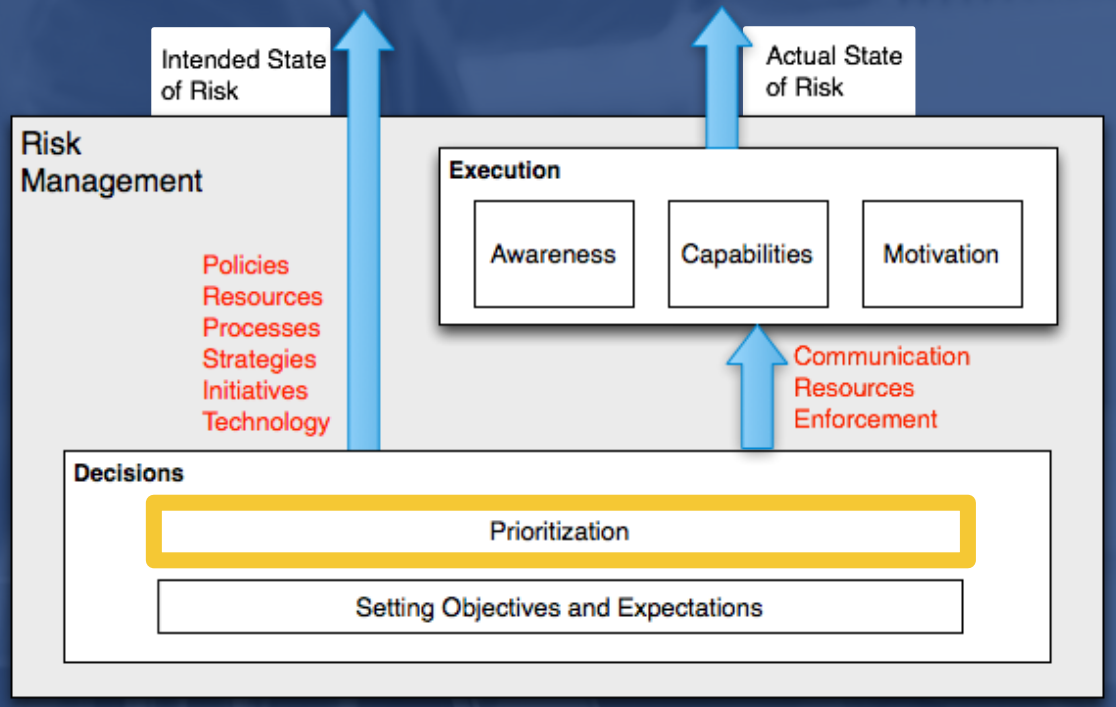
Decisions: Compliance Requirements Results





- YOY, Strong are down 11%
- YOY, Partial are up 2%
- YOY, Weak responses are up 8%
- Likely explainable by variation in respondents

Assessing Prioritization RMM Factors



Compliance Requirements

The degree to which an organization is subject to meaningfully enforced external risk management expectations.

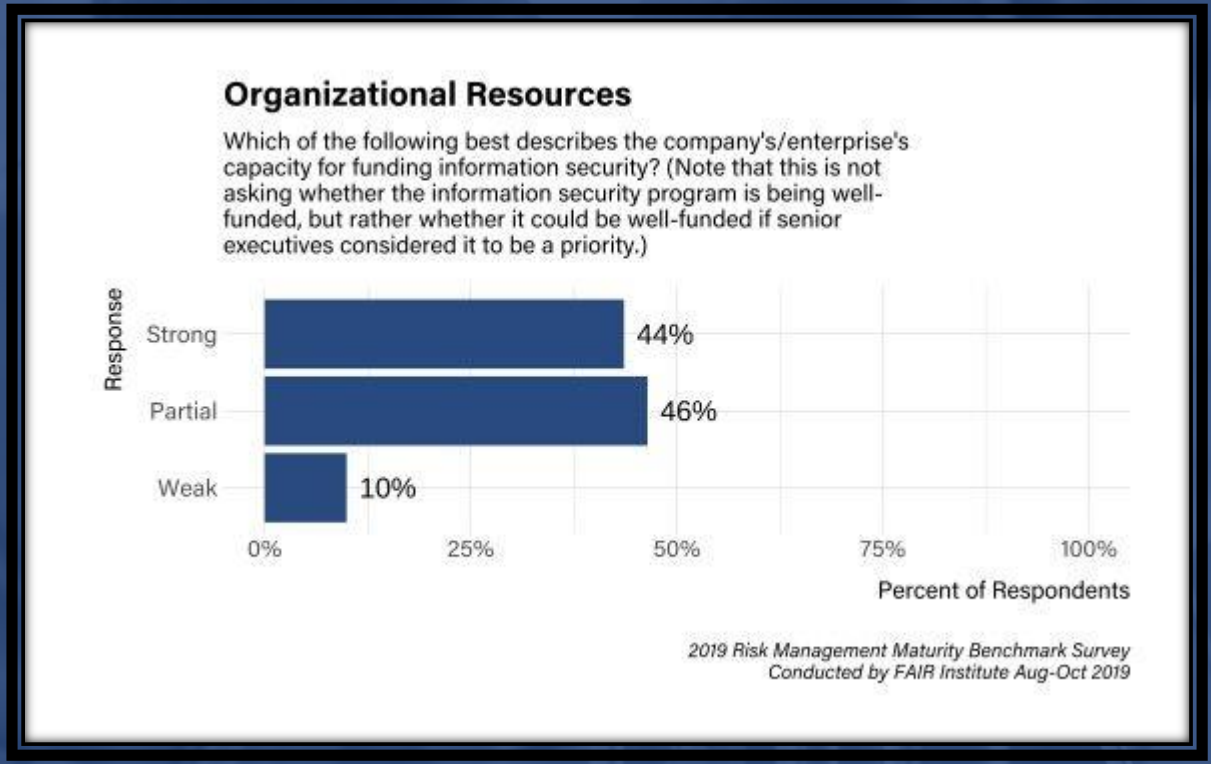
Organizational Resources

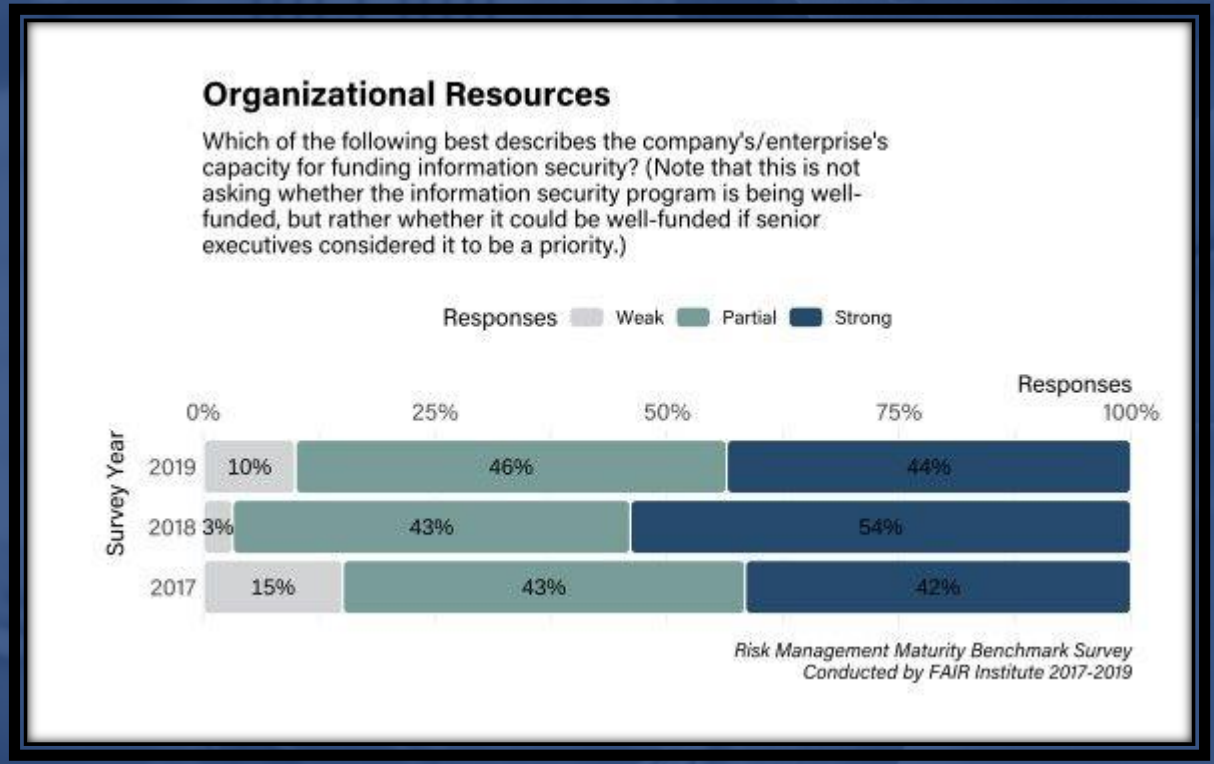
The probability that the organization has sufficient financial resources to meet its risk management needs and obligations given other organization imperatives.

Risk Landscape Intelligence

The probability that decision-makers are provided with the information needed to establish priorities and choose solutions, both at a strategic and operational level.

Decisions: Organizational Resources Results

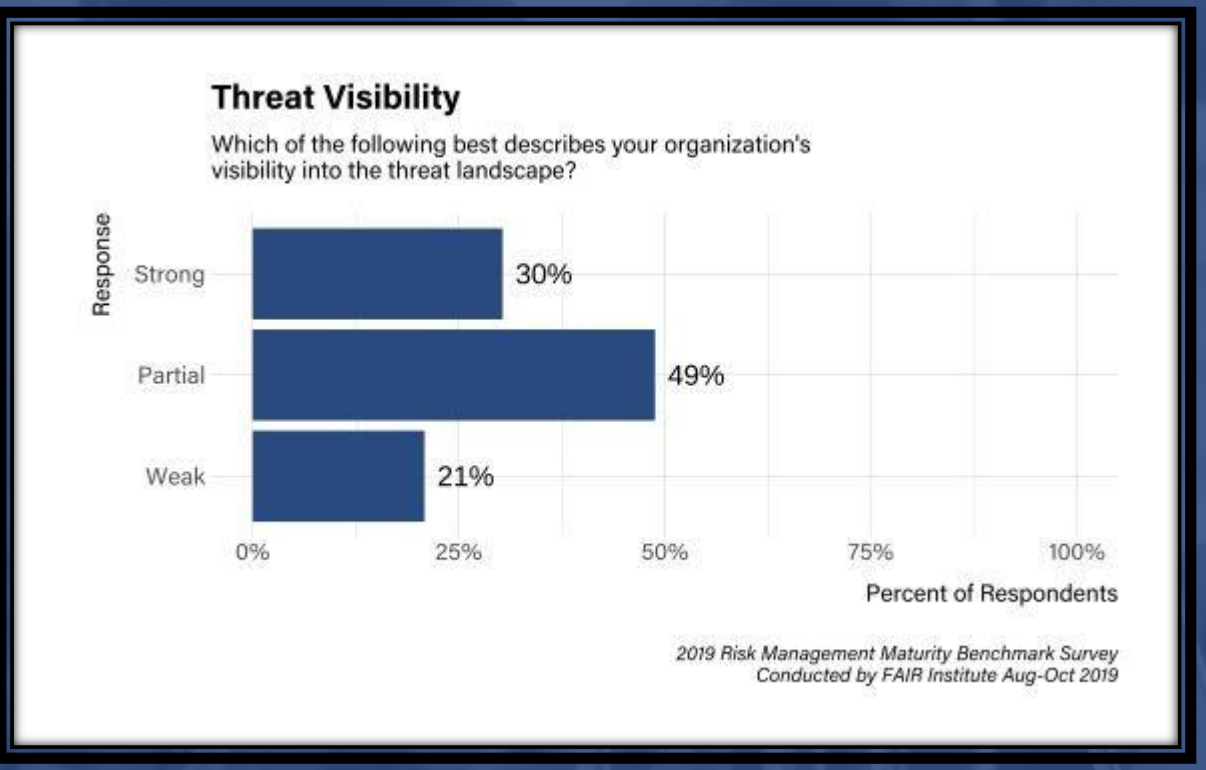




- YOY, Strong are down 10%
- YOY, Partial are up 3%
- YOY, Weak responses are up 7%
- ~90% say org is at least partially capable of funding infosec program

FAIR INSTITUTE

Decisions: Threat Visibility

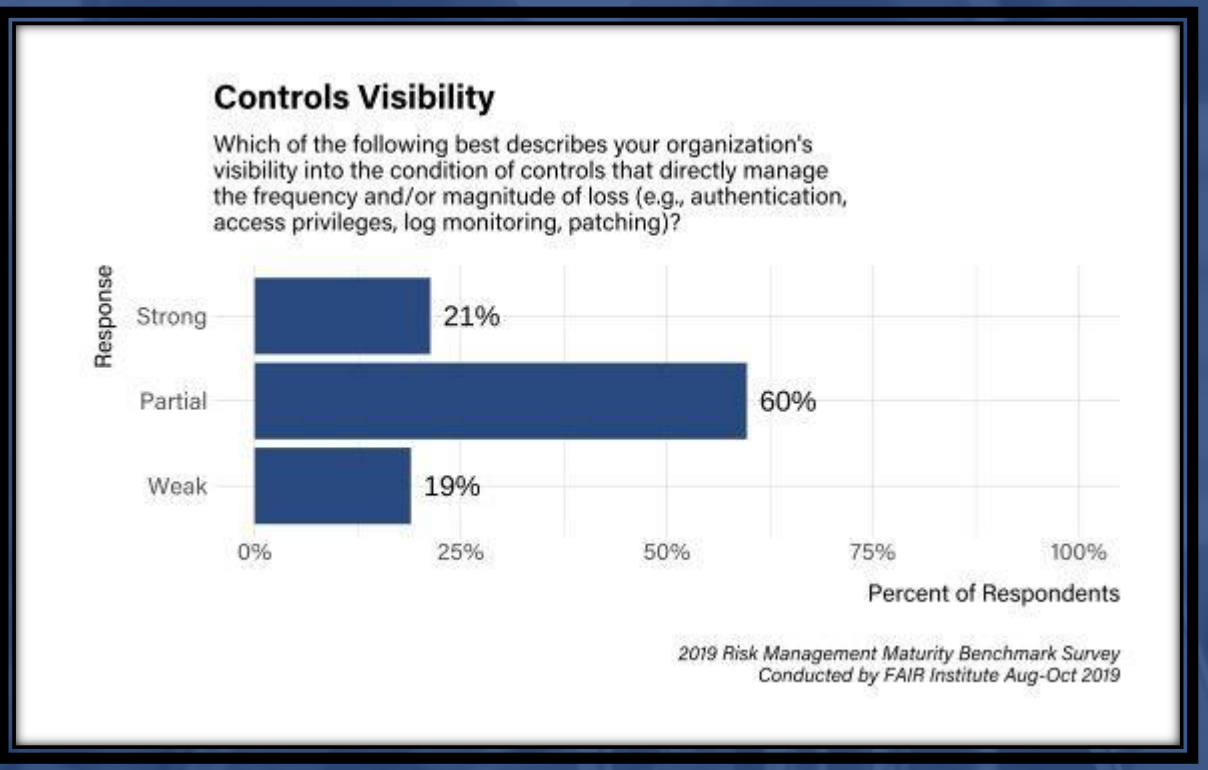


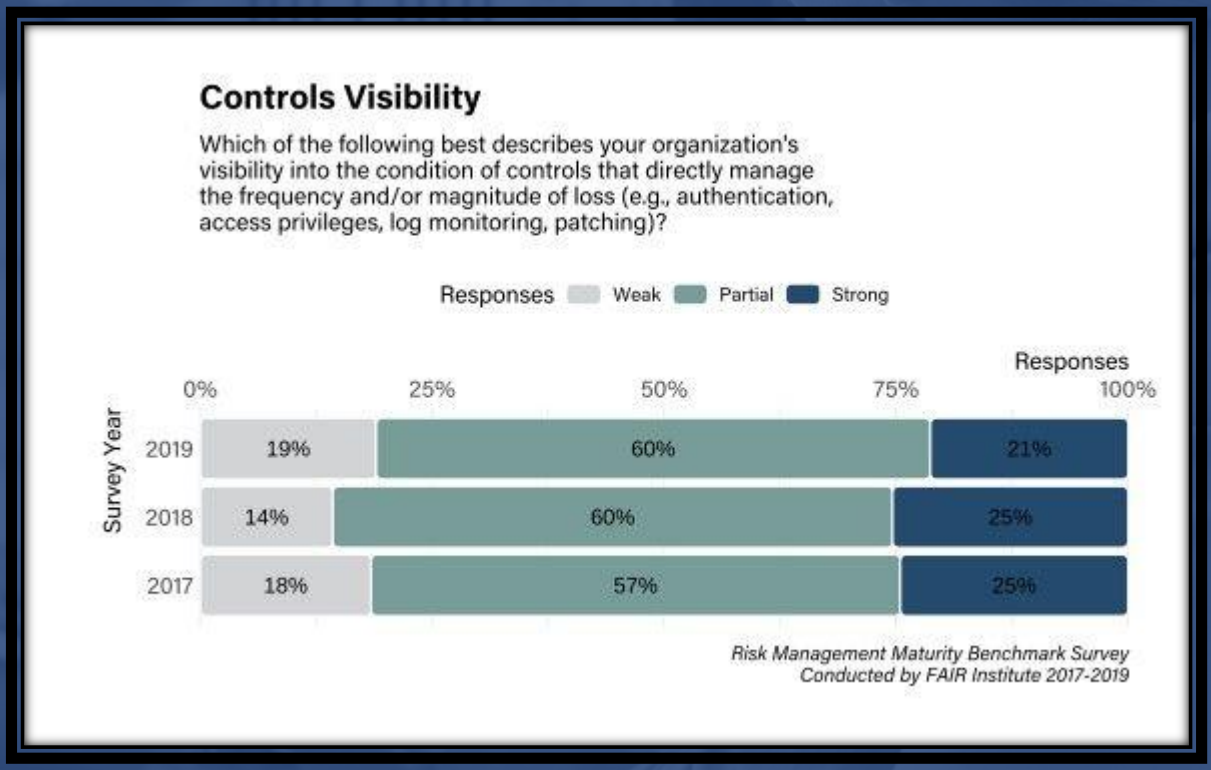
- YOY, Strong are up 2%
- YOY, Partial are down 4%
- YOY, Weak responses are up 2%
- Maintained growth from 2017

Decisions: Asset Visibility

- YOY, Strong are up 1%
- YOY, Partial are down 1%
- YOY, Weak responses are up 1%
- Still relatively flat. Perhaps good viz on crown jewels despite shadow IT?

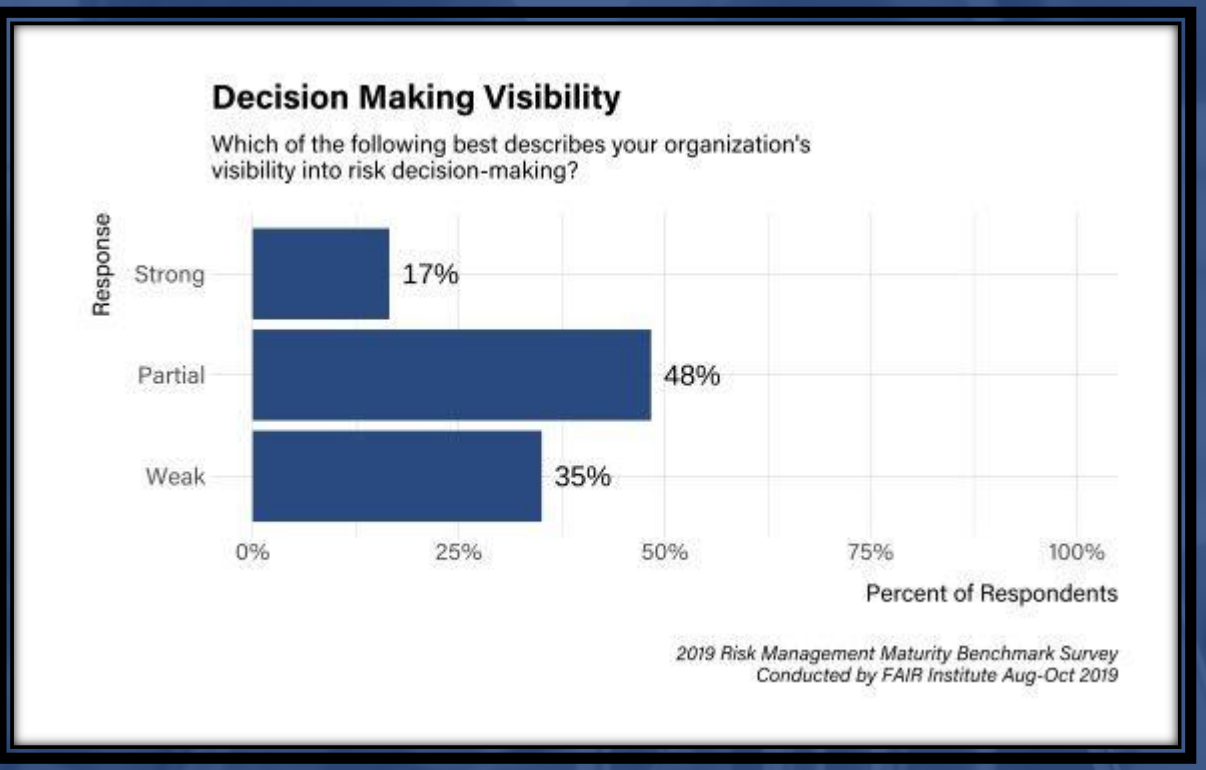
Decisions: Controls Visibility





- YOY, Strong are down 4%
- YOY, Partial are flat
- YOY, Weak responses are up 5%
- Generally good understanding of controls, frameworks, and compliance

Decisions: Decision Making Visibility

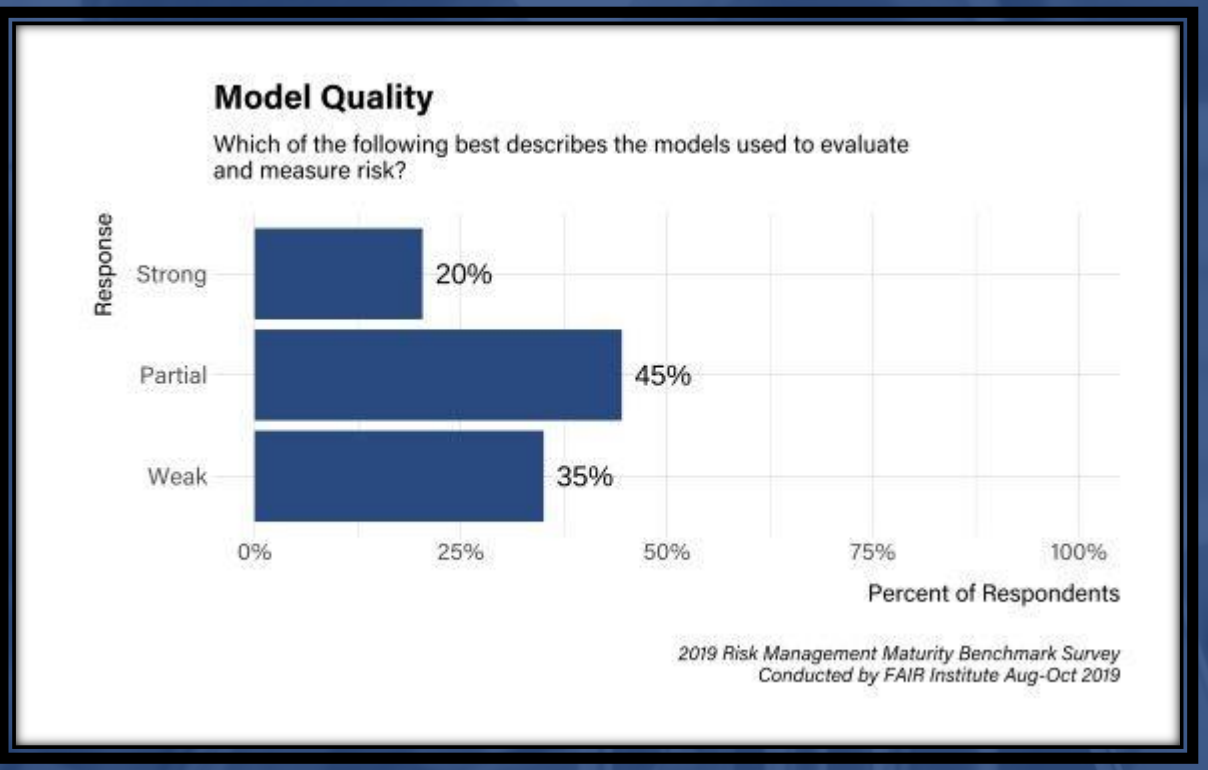


- YOY, Strong are up 1%
- YOY, Partial are down 2%
- YOY, Weak responses are up 1%
- Respondents know how their orgs make decisions; a third do not

Decisions: Execution Visibility

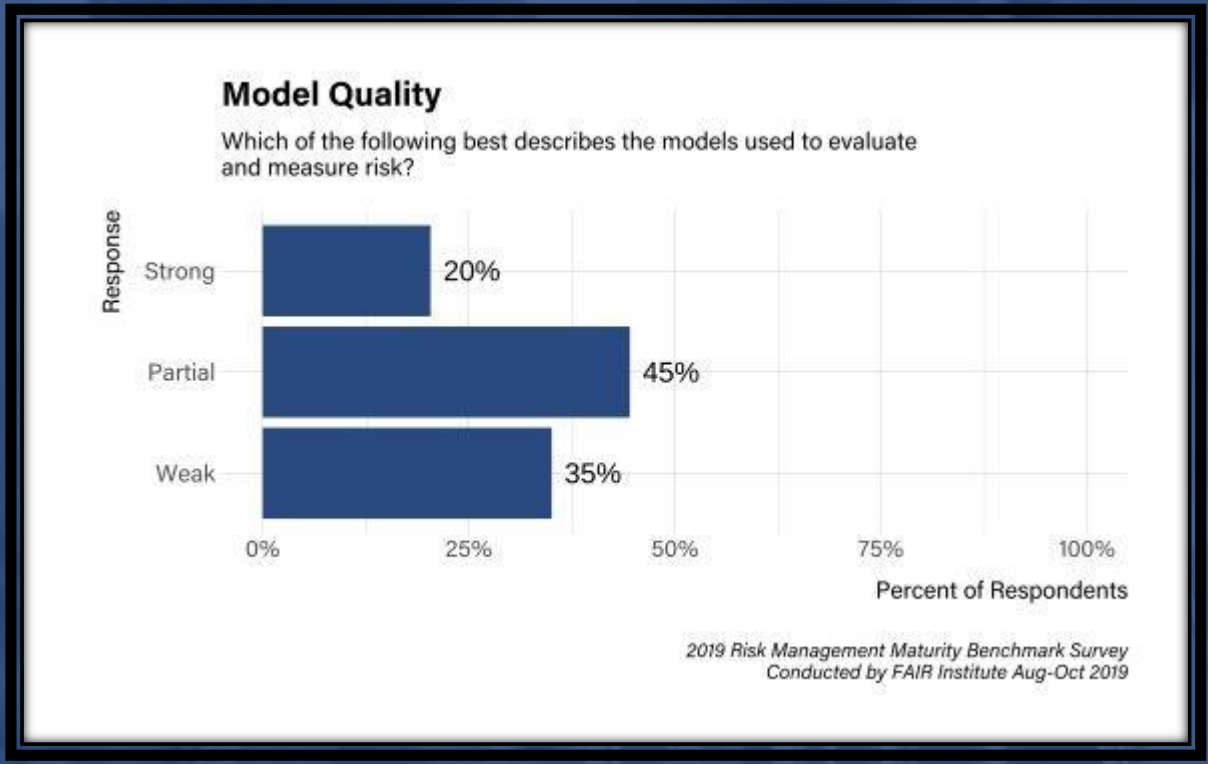
- YOY, Strong are up 1%
- YOY, Partial are down 1%
- YOY, Weak responses are flat
- Respondents know where noncompliance is; a quarter do not

Decisions: Model Quality



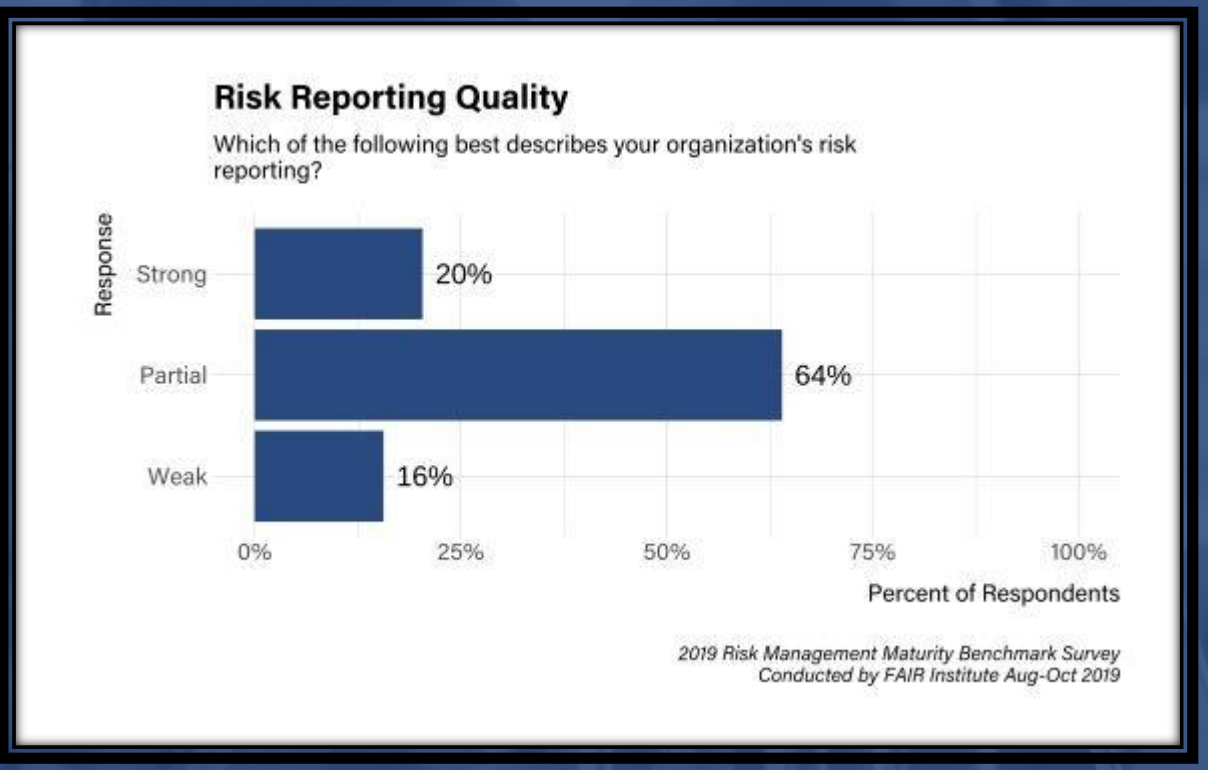
- YOY, Strong are up 6%
- YOY, Partial are down 6%
- YOY, Weak responses are flat
- Model quality continues to increase! A third still use weak models

New for 2019: Model Validity



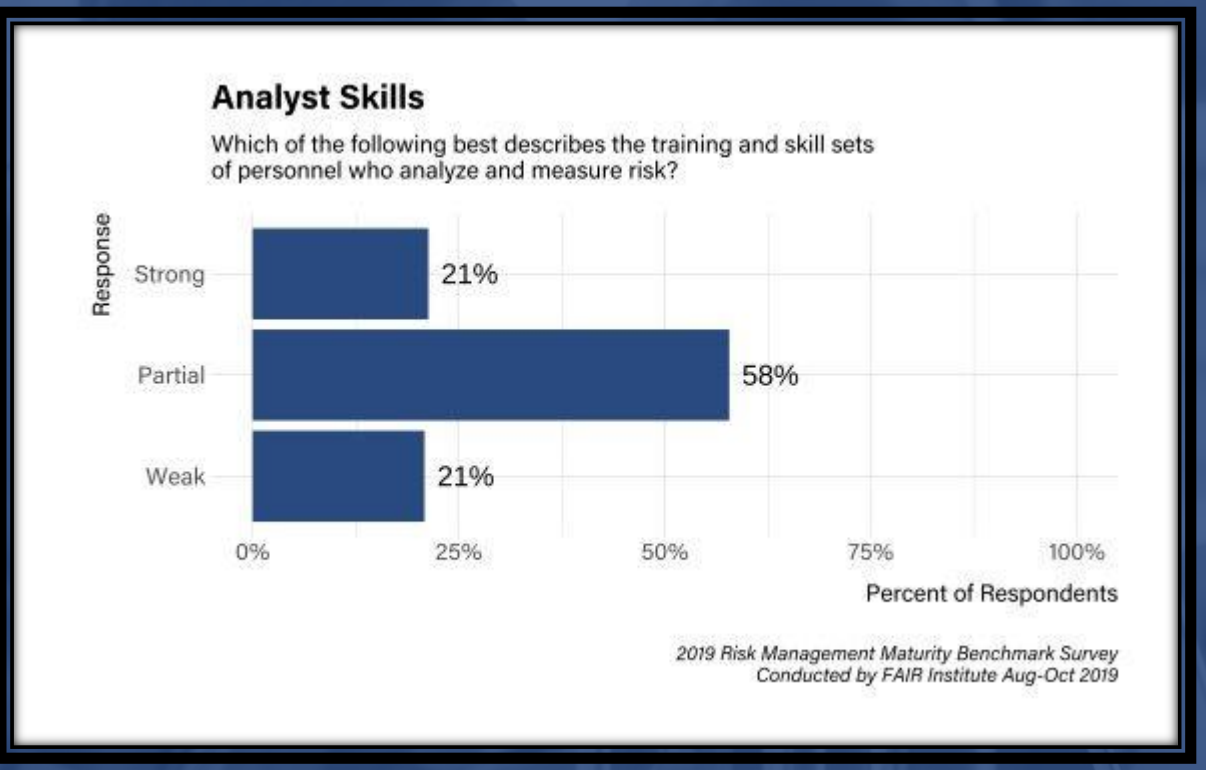
- 65% say they are using partial to high quality models
- 71% say they have good processes to manage model validity
- Validity ensures the implemented model represents reality, enumerates biases and assumptions, and model undergoes regular testing to ensure the results are reliable
- All organizational models for decision making need to undergo validity testing

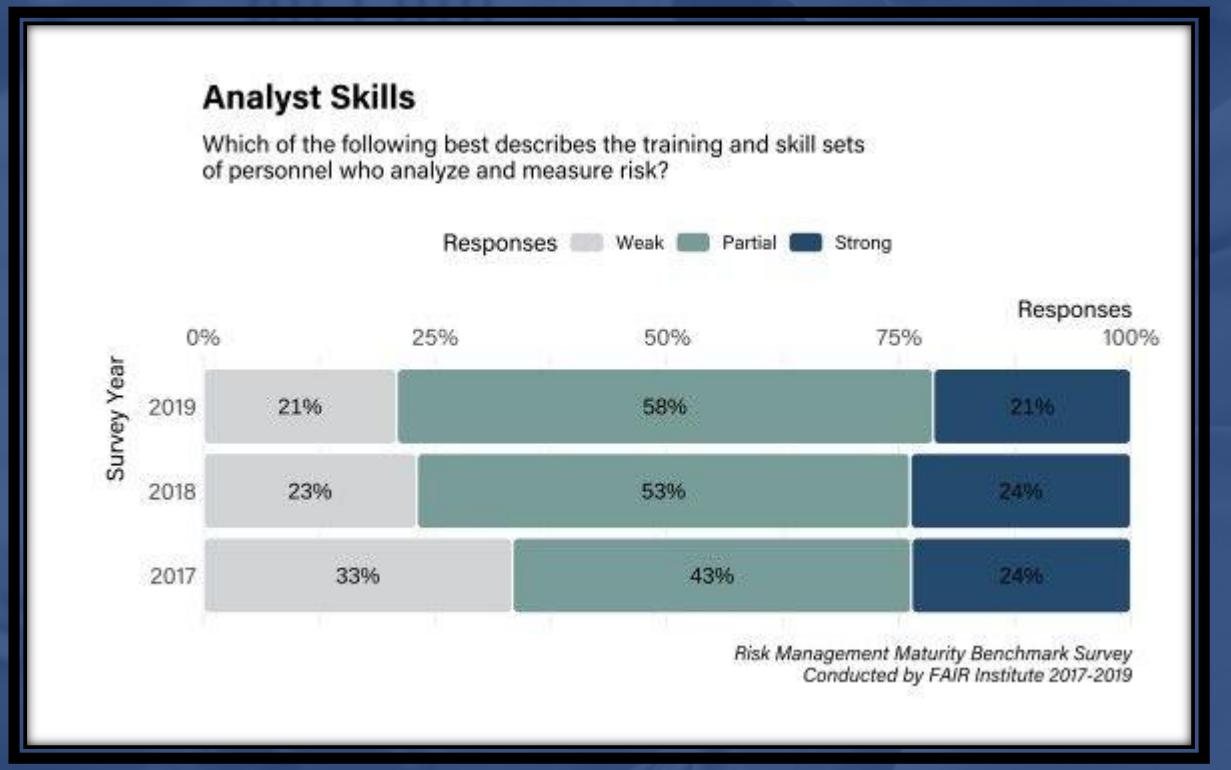
Decisions: Risk Reporting Quality



- YOY, Strong are up 5%
- YOY, Partial are down 8%
- YOY, Weak responses are up 3%
- Risk reporting is improving!

Decisions: Analyst Skills

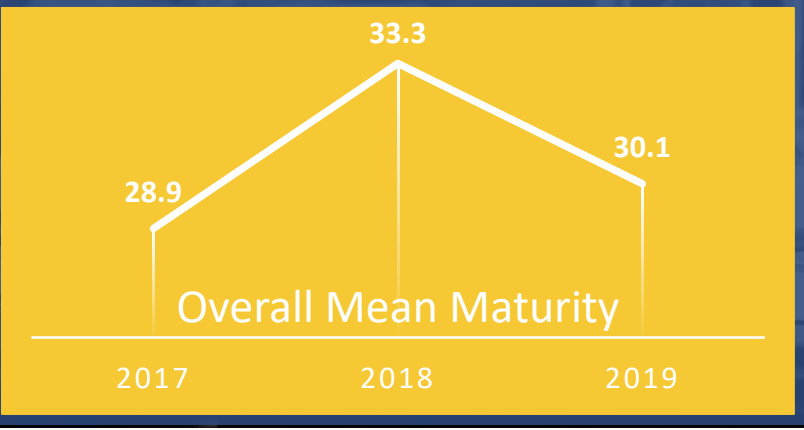


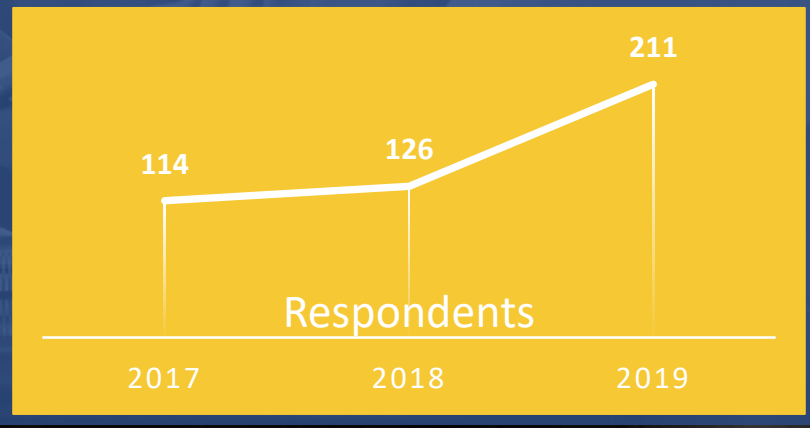


- YOY, Strong are down 3%
- YOY, Partial are up 5%
- YOY, Weak responses are down 2%
- Analyst skills are flat; keep improving your staff with training and uplift

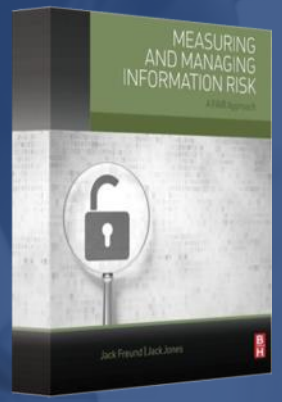
Summary

- Mean maturity score is down from 2018 to 30.1, but not in a statistically significant way but there was a large increase in respondents this year (211)
- Like last year, the most weakly rated domain was Motivation (45% weak), with a tie for second most weak for Model Quality and Decision Making Visibility (35% weak)
- Organizational Resources was the strongest rated domain (44% Strong), with Compliance Requirements the second strongest (38% Strong)
- Policy Expectations stands out as a sub-domain-score that declined the most in 2019 (59.2) vs prior years (68.4 in 2018, 31.4 in 2017), however it still remains the highest rated sub-domain
- Maturity mean in banking was the highest (37.5) and Manufacturing the lowest (14.1)
- In the new multi-select demographic questions top mentions include
  - 36% report using FAIR as a risk quantification model
  - 71% report using NIST CSF as a risk management framework
  - However, only 17% report using quantitative reports showing the organization's economic loss exposure to the Board, vs 60% using narratives and 48% still using heat maps





FAIR RESOURCES



FAIR BOOK

FAIR BLOG

RESOURCE LIBRARY

FAIR TRAINING & CERTIFICATION

FAIR-U TOOL

FAIR UNIVERSITY CURRICULUM