



---

# 2019 Risk Management Maturity Benchmark Survey Results

---

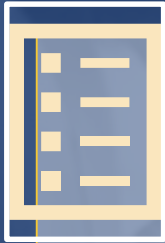
**Jack Freund, Ph.D.**

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

# Risk Management Maturity Benchmark Survey

Participate in the 5th Annual 2019 Risk Management 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 annual survey for risk professionals to benchmark their practices and benchmark their peers.

By taking this brief survey a thoughtful, as you move through a structured process, including:

- Set and threat visibility
- Prioritization
- Policies/expectations
- Compliance requirements

Designed to be completely anonymous and should take between 10 to 15 minutes to complete.

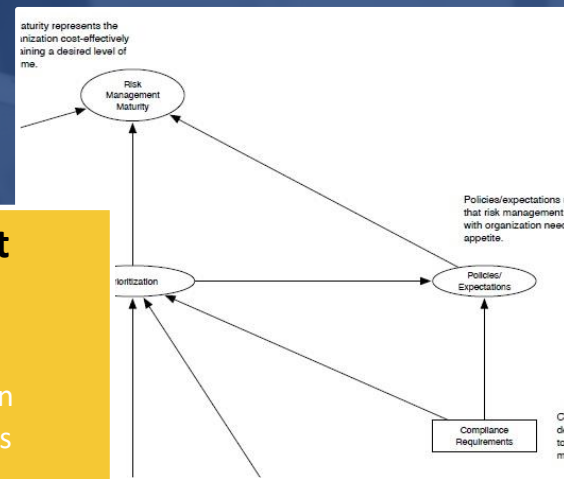


## Anonymous Survey

- 211 respondents
- Mostly FAIR Institute members (anonymous)

## Risk Mgmt Maturity Ontology

- Prioritization
- Expectations
- Execution

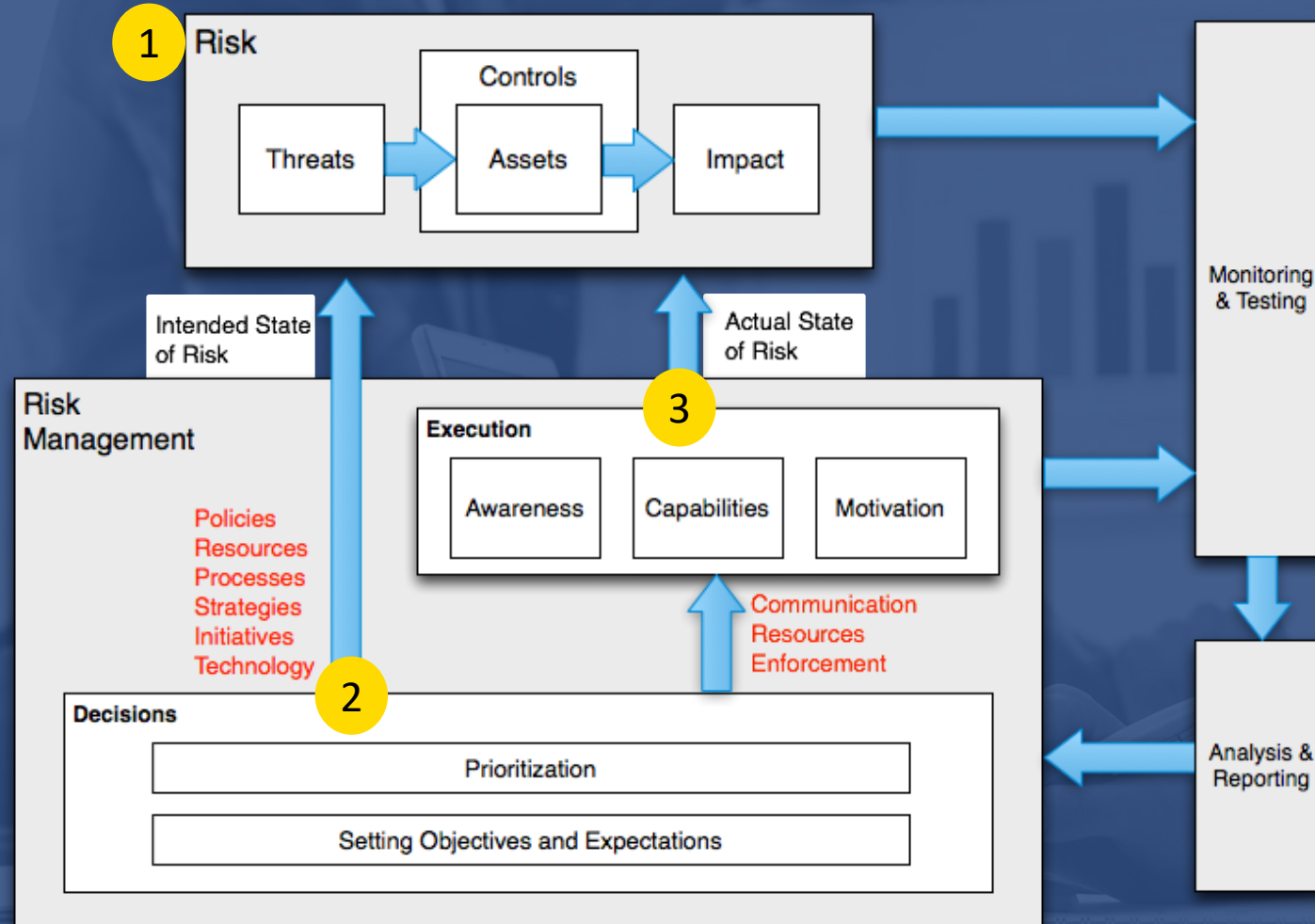


## Report

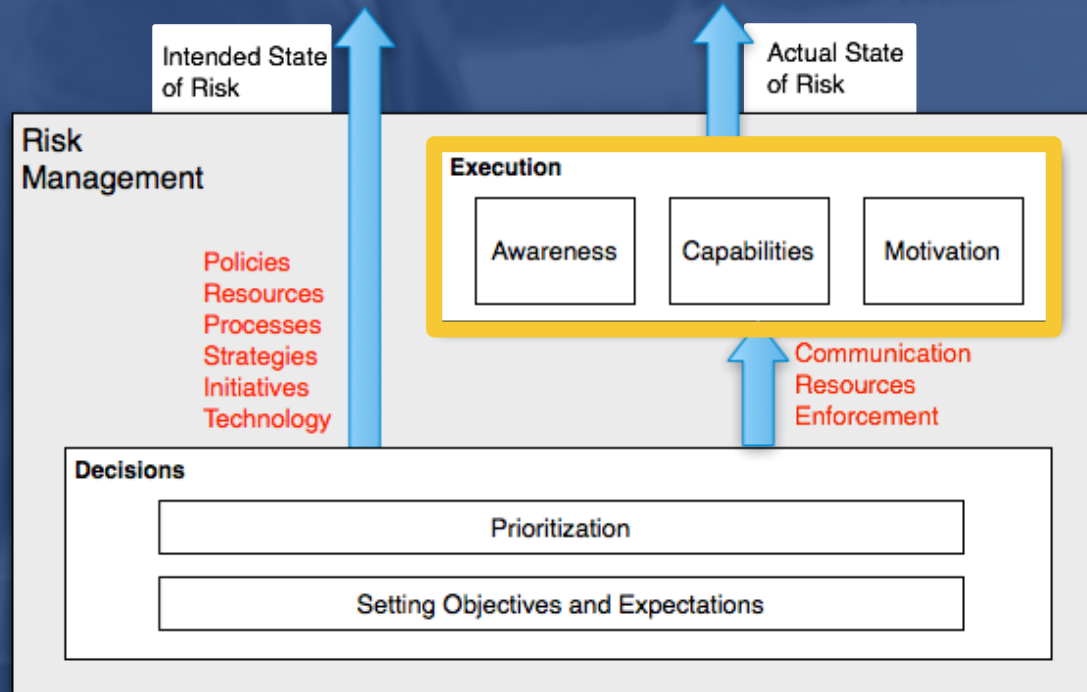
- Slide deck
- Webinar
- Written Report



# Risk Management Landscape



# 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

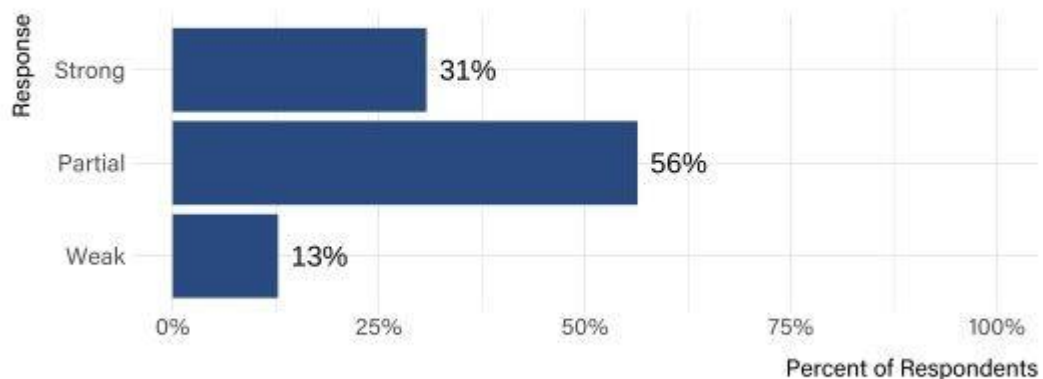
The probability that personnel are appropriately incentivized to fulfill their risk management responsibilities

# Execution: Awareness Results



## Awareness

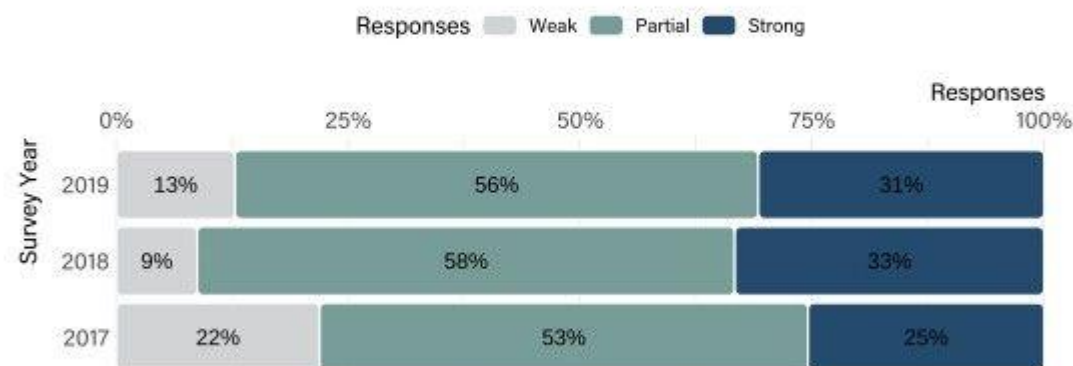
Which of the following best describes how aware personnel are of the organization's expectations (e.g., policies and standards) regarding their information security related responsibilities?



2019 Risk Management Maturity Benchmark Survey  
Conducted by FAIR Institute Aug-Oct 2019

## Awareness

Which of the following best describes how aware personnel are of the organization's expectations (e.g., policies and standards) regarding their information security related responsibilities?



Risk Management Maturity Benchmark Survey  
Conducted by FAIR Institute 2017-2019

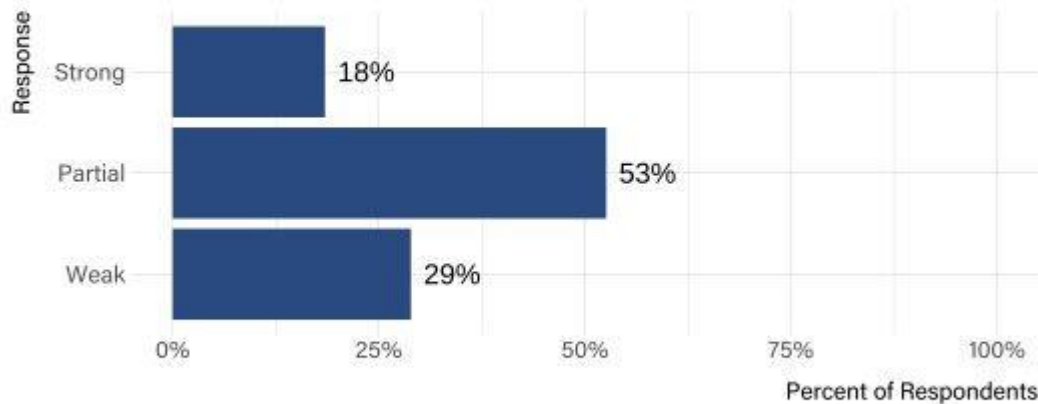
- YOY, Strong are down 2%
- YOY, Partial are down 2%
- YOY, Weak responses are up 4%
- Requires better communication and reporting of security requirements

# Execution: Capabilities Results



## Capabilities

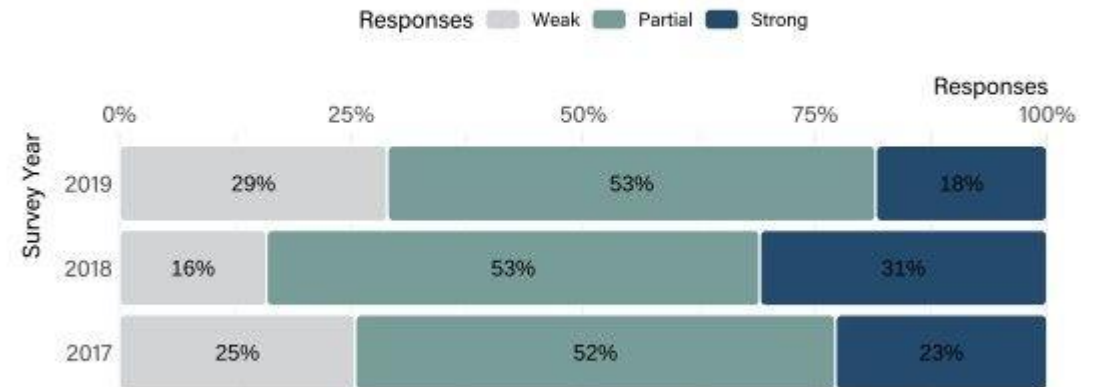
Which of the following best describes personnel's risk management skills and capabilities?



2019 Risk Management Maturity Benchmark Survey  
Conducted by FAIR Institute Aug-Oct 2019

## Capabilities

Which of the following best describes personnel's risk management skills and capabilities?



Risk Management Maturity Benchmark Survey  
Conducted by FAIR Institute 2017-2019

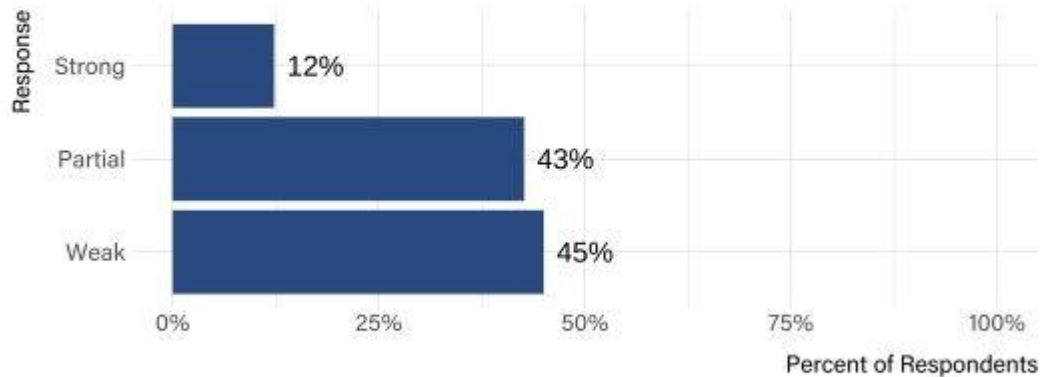
- YOY, Strong are down 13%
- YOY, Partial are flat
- YOY, Weak responses are up 13%
- Training programs and skills uplift can improve results

# Execution: Motivation Results



## Motivation

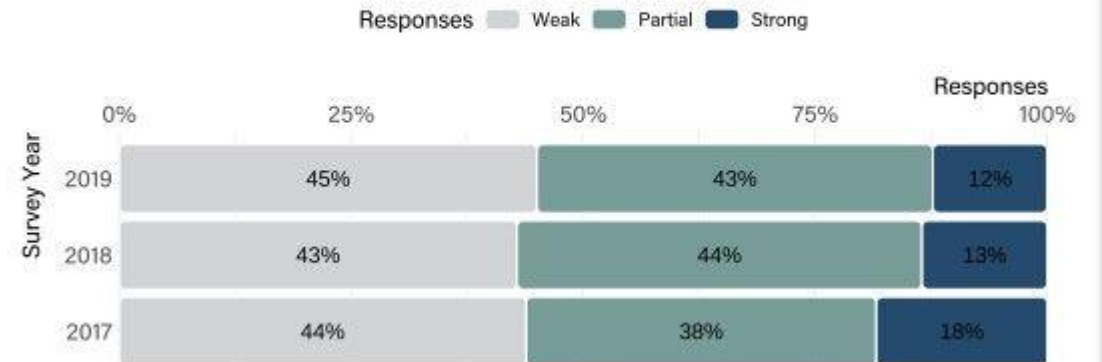
Which of the following best describes how personnel are incentivized to meet the organization's risk management expectations (e.g., policies and standards)?



2019 Risk Management Maturity Benchmark Survey  
Conducted by FAIR Institute Aug-Oct 2019

## Motivation

Which of the following best describes how personnel are incentivized to meet the organization's risk management expectations (e.g., policies and standards)?

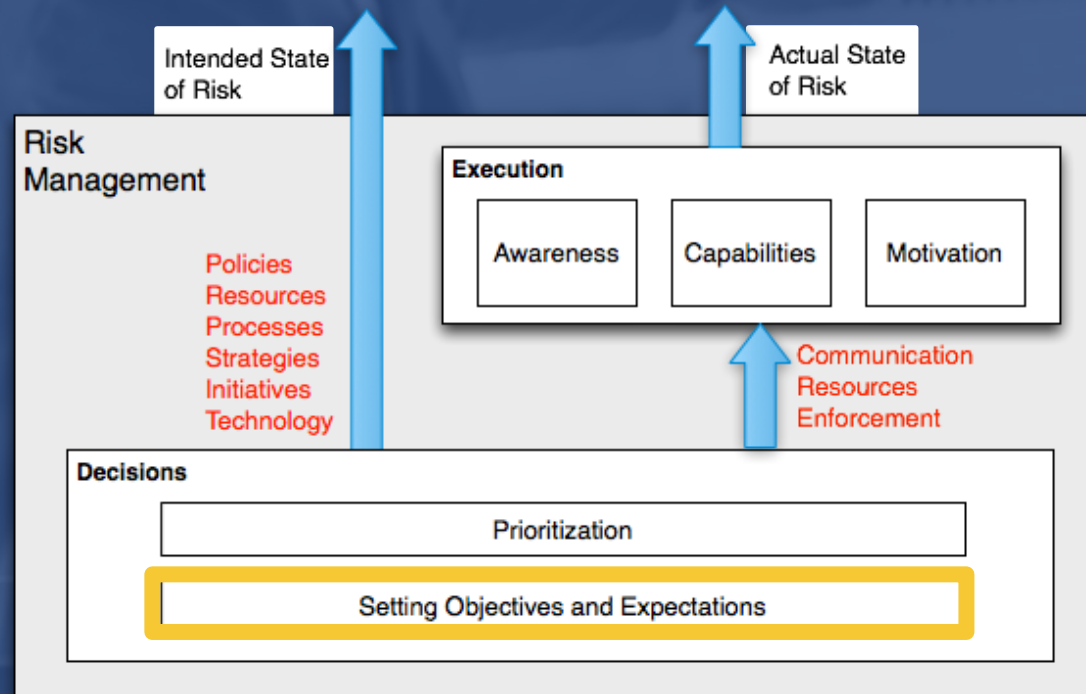


Risk Management Maturity Benchmark Survey  
Conducted by FAIR Institute 2017-2019

- 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

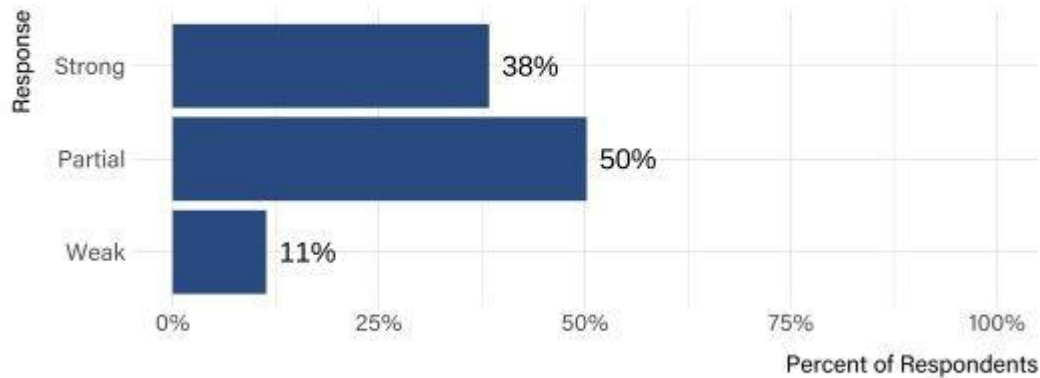
The probability that decision-makers are provided with the information needed to establish priorities and choose solutions, both at a strategic and operational level.

# Decisions: Compliance Requirements Results



## Compliance Requirements

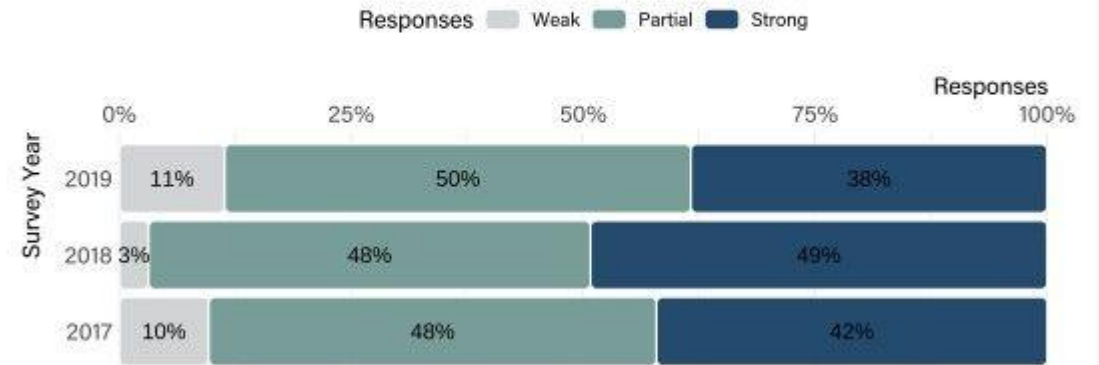
Which of the following best describes the degree to which the organization is subject to external risk management expectations (e.g., regulations, third-party requirements, etc.)?



2019 Risk Management Maturity Benchmark Survey  
Conducted by FAIR Institute Aug-Oct 2019

## Compliance Requirements

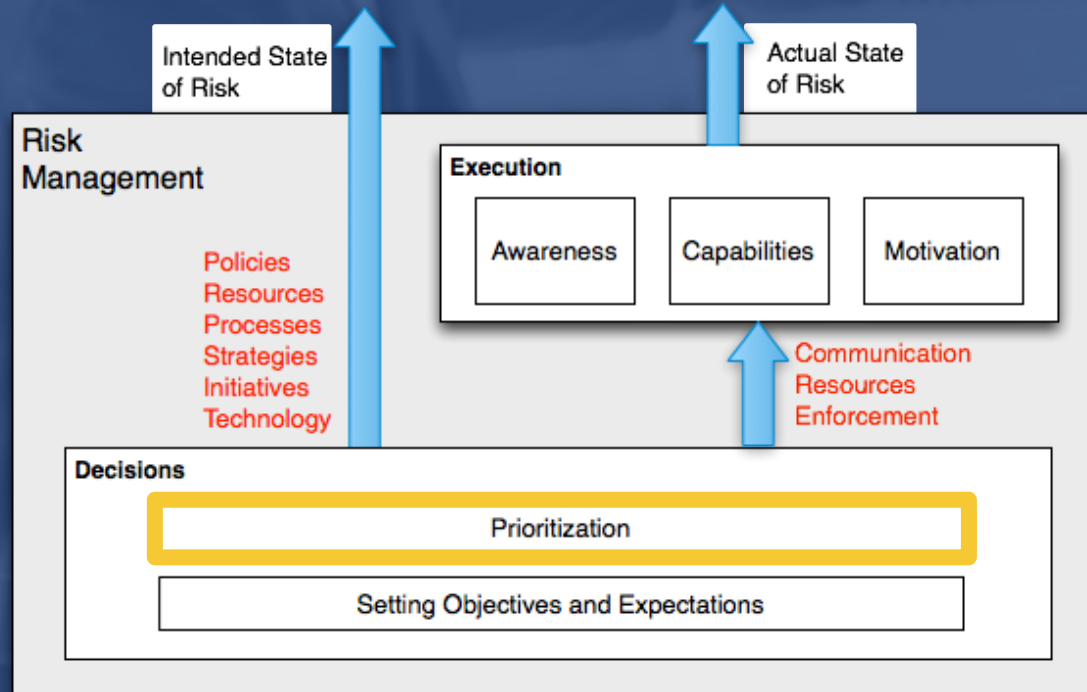
Which of the following best describes the degree to which the organization is subject to external risk management expectations (e.g., regulations, third-party requirements, etc.)?



Risk Management Maturity Benchmark Survey  
Conducted by FAIR Institute 2017-2019

- 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

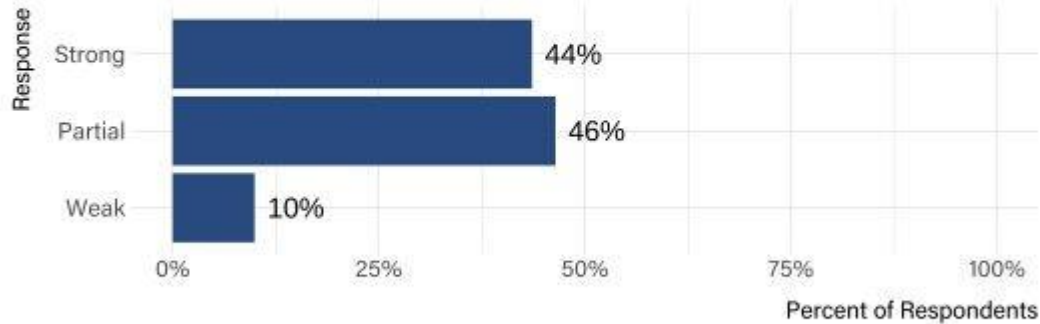
The probability that decision-makers are provided with the information needed to establish priorities and choose solutions, both at a strategic and operational level.

# Decisions: Organizational Resources Results



## Organizational Resources

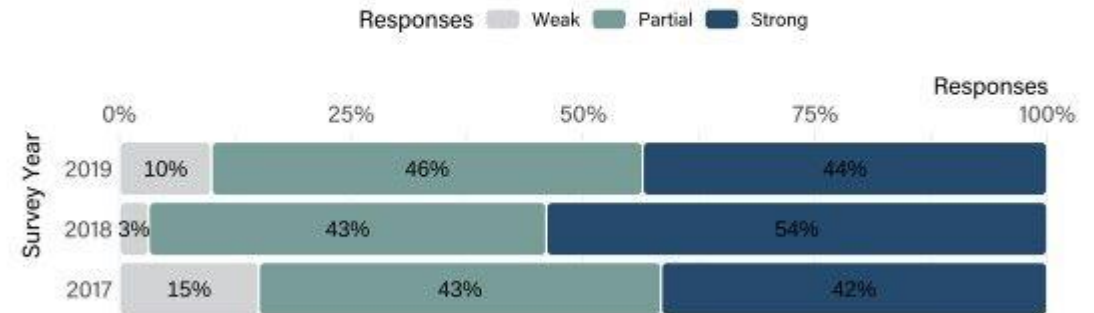
Which of the following best describes the company's/enterprise's capacity for funding information security? (Note that this is not asking whether the information security program is being well-funded, but rather whether it could be well-funded if senior executives considered it to be a priority.)



2019 Risk Management Maturity Benchmark Survey  
Conducted by FAIR Institute Aug-Oct 2019

## Organizational Resources

Which of the following best describes the company's/enterprise's capacity for funding information security? (Note that this is not asking whether the information security program is being well-funded, but rather whether it could be well-funded if senior executives considered it to be a priority.)



Risk Management Maturity Benchmark Survey  
Conducted by FAIR Institute 2017-2019

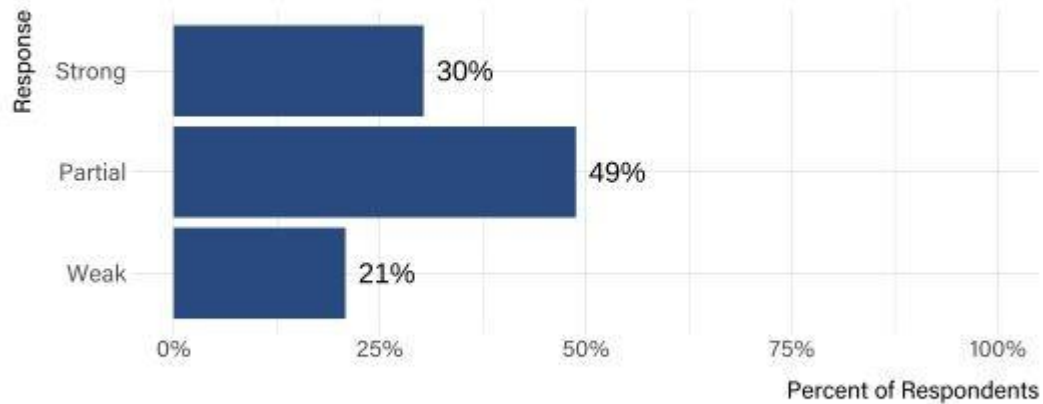
- YOY, Strong are down 10%
- YOY, Partial are up 3%
- YOY, Weak responses are up 7%
- ~90% say org is at least partially capable of funding infosec program

# Decisions: Threat Visibility



## Threat Visibility

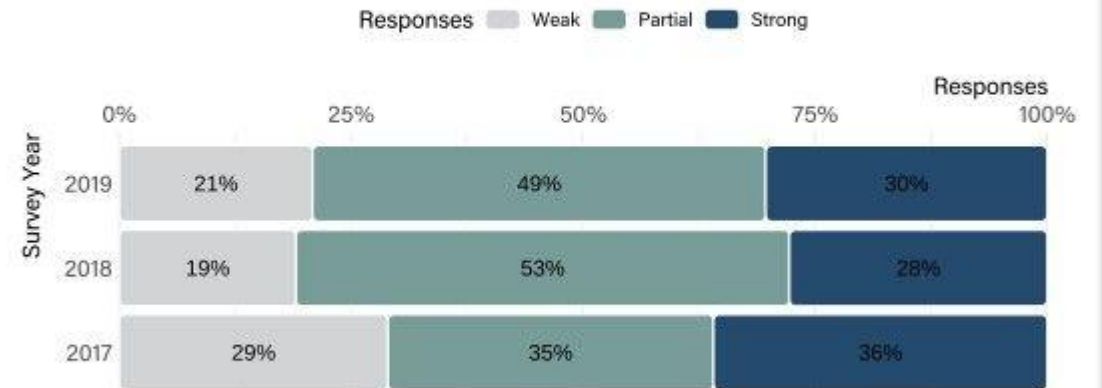
Which of the following best describes your organization's visibility into the threat landscape?



2019 Risk Management Maturity Benchmark Survey  
Conducted by FAIR Institute Aug-Oct 2019

## Threat Visibility

Which of the following best describes your organization's visibility into the threat landscape?



Risk Management Maturity Benchmark Survey  
Conducted by FAIR Institute 2017-2019

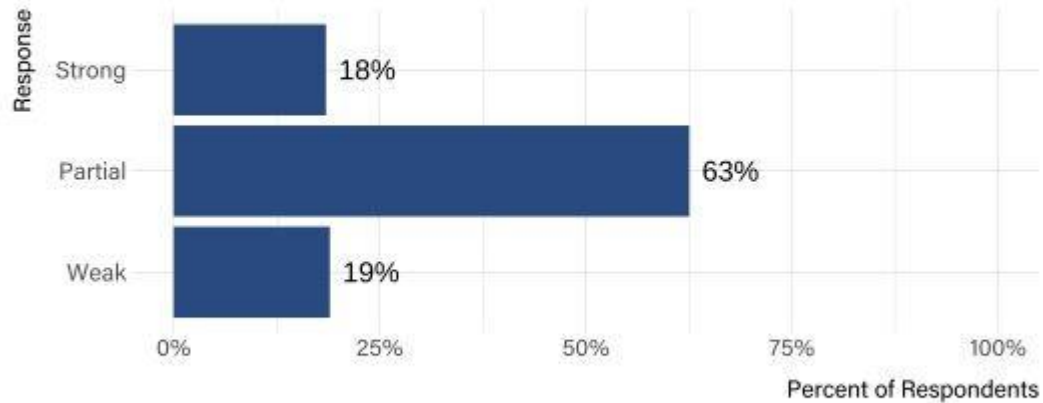
- YOY, Strong are up 2%
- YOY, Partial are down 4%
- YOY, Weak responses are up 2%
- Maintained growth from 2017

# Decisions: Asset Visibility



## Asset Visibility

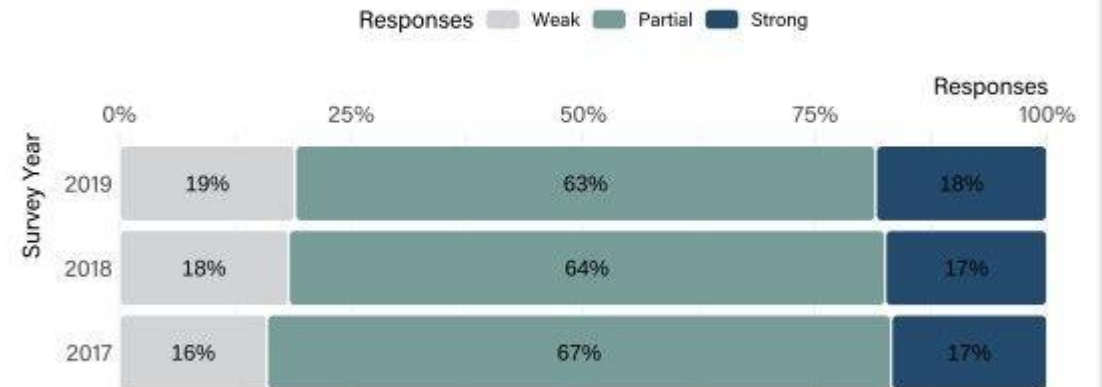
Which of the following best describes your organization's visibility into its system and information assets?



2019 Risk Management Maturity Benchmark Survey  
Conducted by FAIR Institute Aug-Oct 2019

## Asset Visibility

Which of the following best describes your organization's visibility into its system and information assets?



Risk Management Maturity Benchmark Survey  
Conducted by FAIR Institute 2017-2019

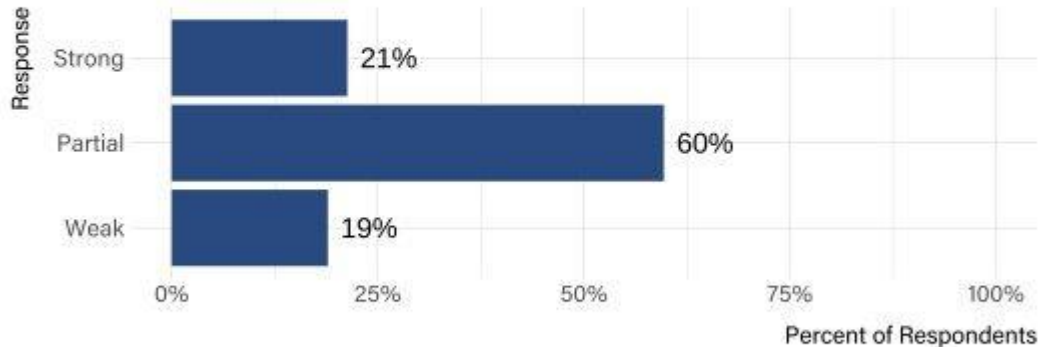
- YOY, Strong are up 1%
- YOY, Partial are down 1%
- YOY, Weak responses are up 1%
- Still relatively flat. Perhaps good viz on crown jewels despite shadow IT?

# Decisions: Controls Visibility



## Controls Visibility

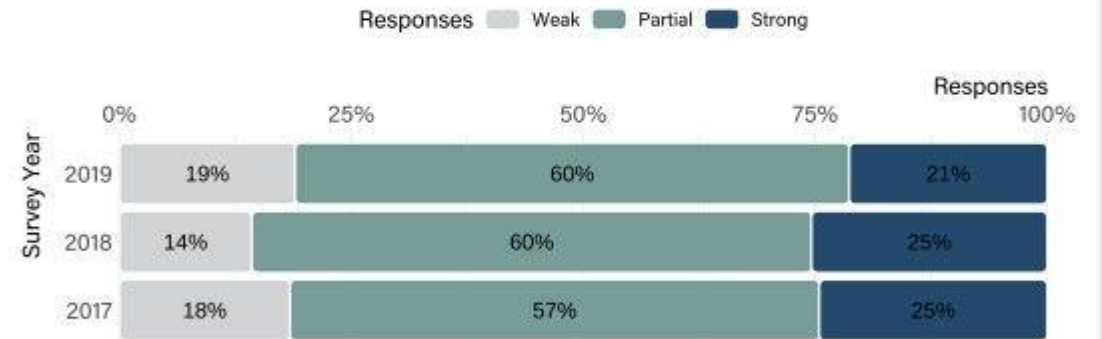
Which of the following best describes your organization's visibility into the condition of controls that directly manage the frequency and/or magnitude of loss (e.g., authentication, access privileges, log monitoring, patching)?



2019 Risk Management Maturity Benchmark Survey  
Conducted by FAIR Institute Aug-Oct 2019

## Controls Visibility

Which of the following best describes your organization's visibility into the condition of controls that directly manage the frequency and/or magnitude of loss (e.g., authentication, access privileges, log monitoring, patching)?



Risk Management Maturity Benchmark Survey  
Conducted by FAIR Institute 2017-2019

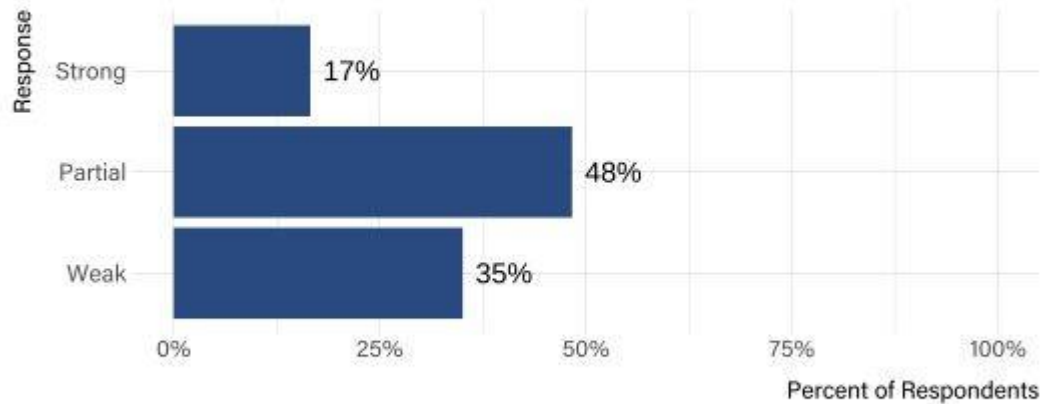
- YOY, Strong are down 4%
- YOY, Partial are flat
- YOY, Weak responses are up 5%
- Generally good understanding of controls, frameworks, and compliance

# Decisions: Decision Making Visibility



## Decision Making Visibility

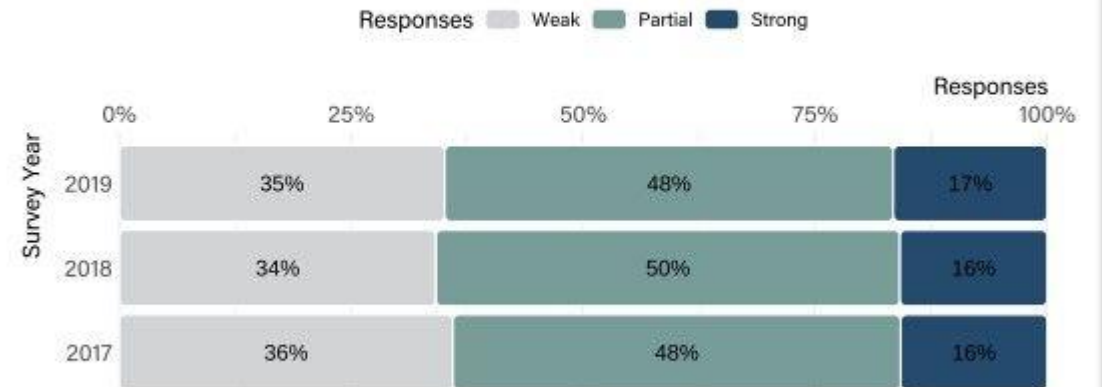
Which of the following best describes your organization's visibility into risk decision-making?



2019 Risk Management Maturity Benchmark Survey  
Conducted by FAIR Institute Aug-Oct 2019

## Decision Making Visibility

Which of the following best describes your organization's visibility into risk decision-making?



Risk Management Maturity Benchmark Survey  
Conducted by FAIR Institute 2017-2019

- 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

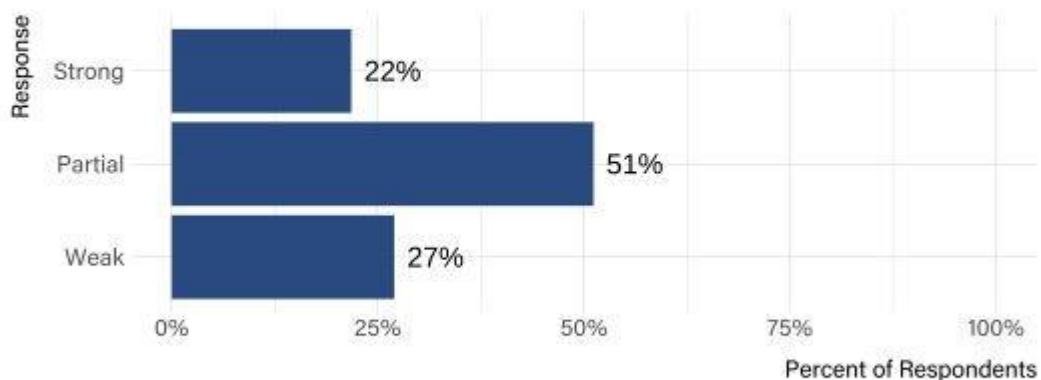


# Decisions: Execution Visibility



## Execution Visibility

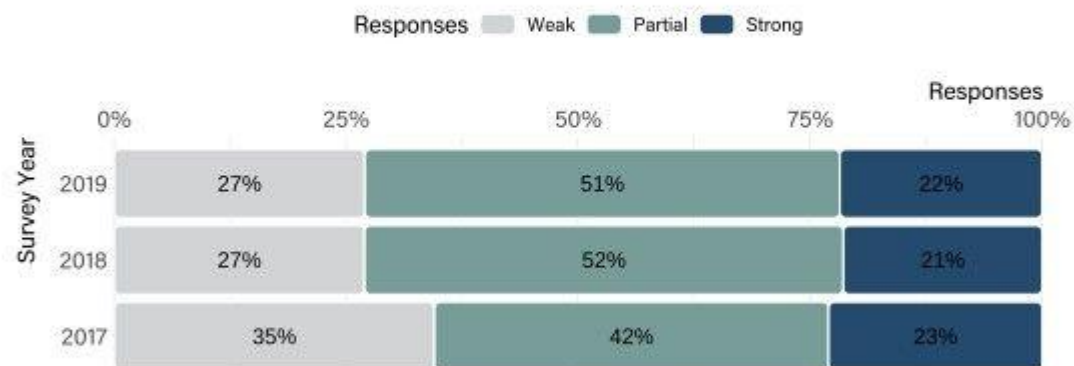
Which of the following best describes your organization's visibility into why conditions exist that are not compliant with organization policy?



2019 Risk Management Maturity Benchmark Survey  
Conducted by FAIR Institute Aug-Oct 2019

## Execution Visibility

Which of the following best describes your organization's visibility into why conditions exist that are not compliant with organization policy?



Risk Management Maturity Benchmark Survey  
Conducted by FAIR Institute 2017-2019

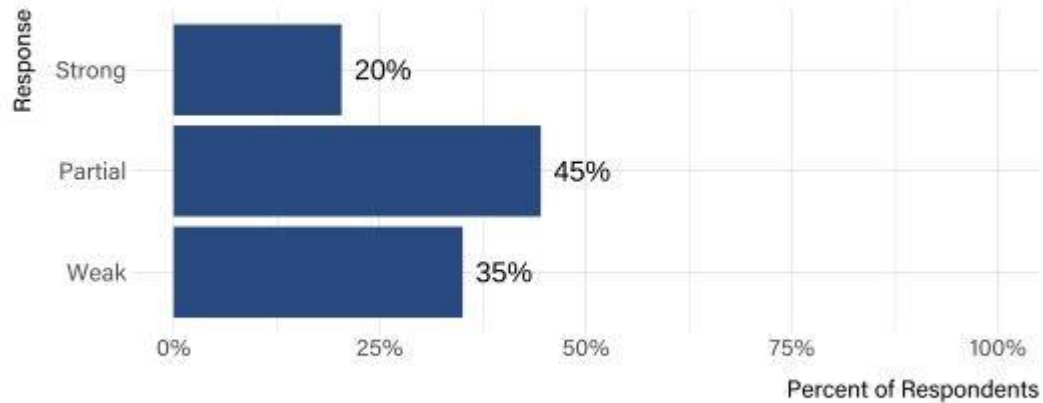
- YOY, Strong are up 1%
- YOY, Partial are down 1%
- YOY, Weak responses are flat
- Respondents know where noncompliance is; a quarter do not

# Decisions: Model Quality



## Model Quality

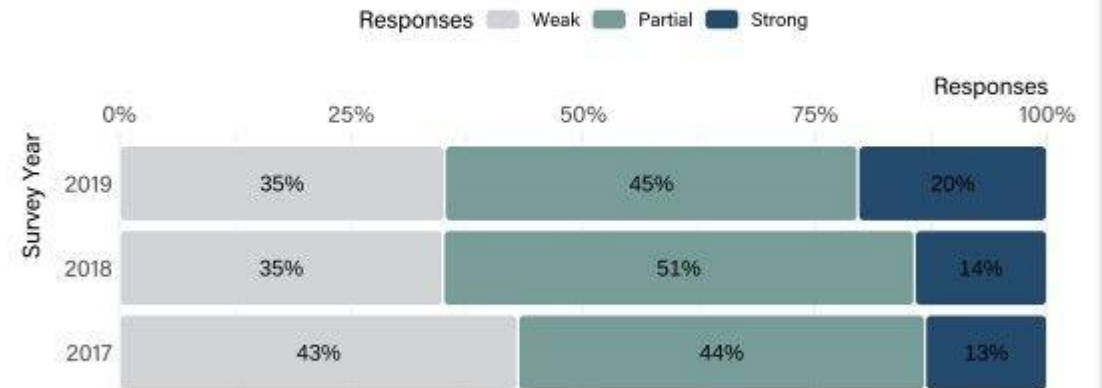
Which of the following best describes the models used to evaluate and measure risk?



2019 Risk Management Maturity Benchmark Survey  
Conducted by FAIR Institute Aug-Oct 2019

## Model Quality

Which of the following best describes the models used to evaluate and measure risk?



Risk Management Maturity Benchmark Survey  
Conducted by FAIR Institute 2017-2019

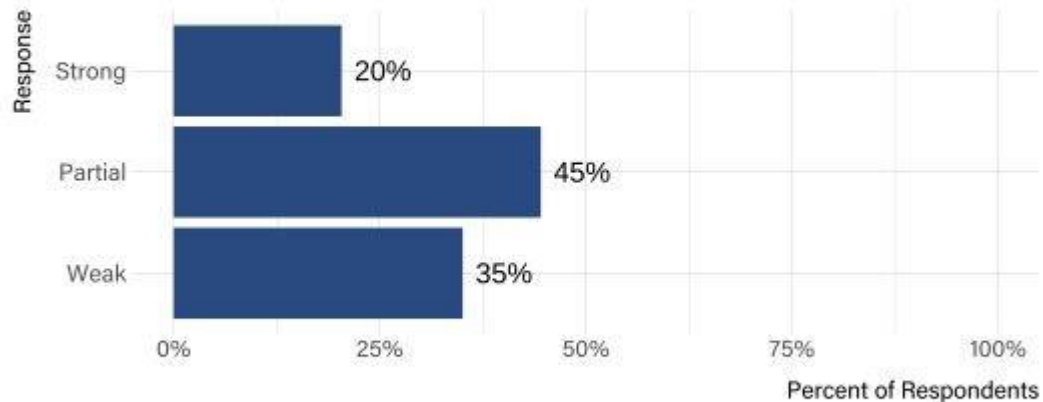
- YOY, Strong are up 6%
- YOY, Partial are down 6%
- YOY, Weak responses are flat
- Model quality continues to increase! A third still use weak models

# New for 2019: Model Validity



## Model Quality

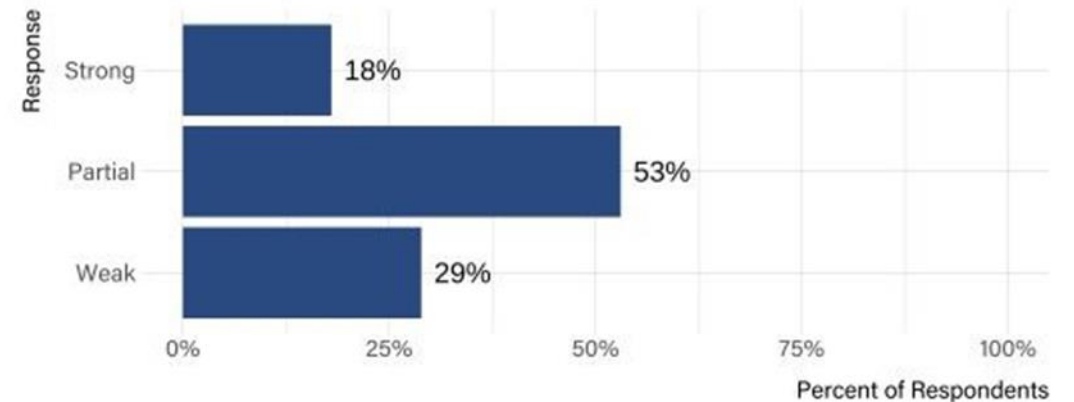
Which of the following best describes the models used to evaluate and measure risk?



2019 Risk Management Maturity Benchmark Survey  
Conducted by FAIR Institute Aug-Oct 2019

## Model Validity

Which of the following best describes your organization's processes for managing the risk model's validity?



2019 Risk Management Maturity Benchmark Survey  
Conducted by FAIR Institute Aug-Oct 2019

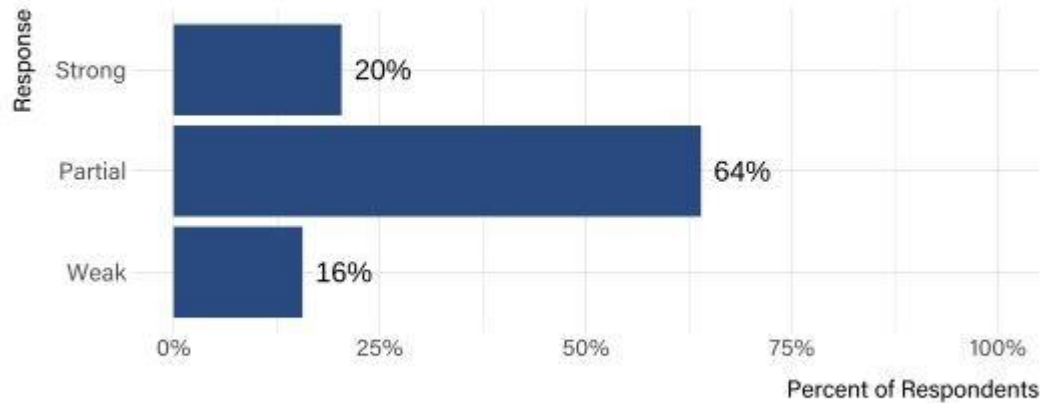
- 65% say they are using partial to high quality models
- 71% say they have good processes to manage model validity
- Validity ensures the implemented model represents reality, enumerates biases and assumptions, and model undergoes regular testing to ensure the results are reliable
- All organizational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

# Decisions: Risk Reporting Quality



## Risk Reporting Quality

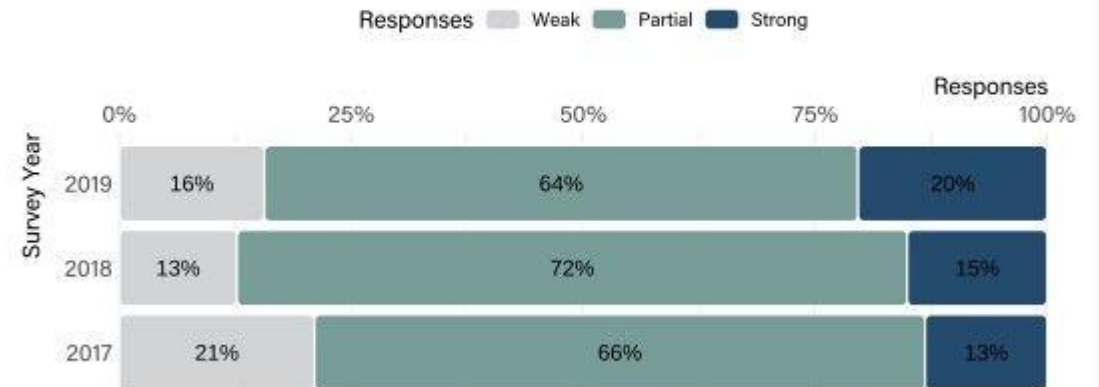
Which of the following best describes your organization's risk reporting?



2019 Risk Management Maturity Benchmark Survey  
Conducted by FAIR Institute Aug-Oct 2019

## Risk Reporting Quality

Which of the following best describes your organization's risk reporting?



Risk Management Maturity Benchmark Survey  
Conducted by FAIR Institute 2017-2019

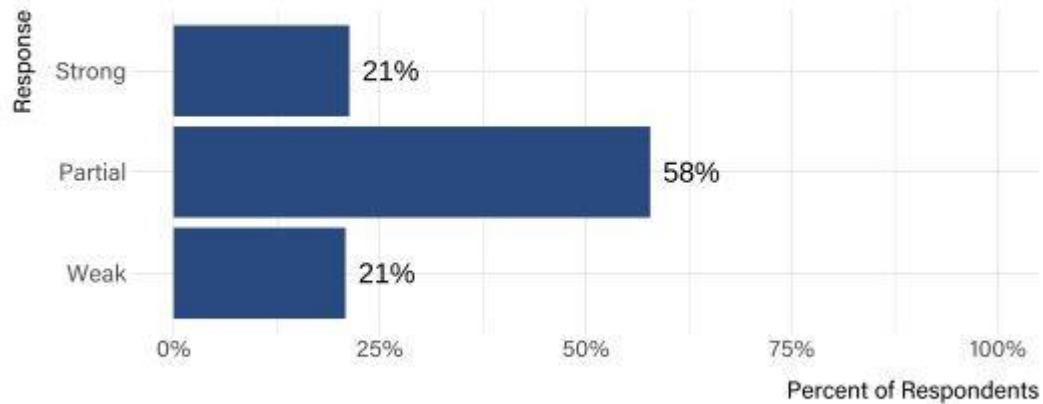
- YOY, Strong are up 5%
- YOY, Partial are down 8%
- YOY, Weak responses are up 3%
- Risk reporting is improving!

# Decisions: Analyst Skills



## Analyst Skills

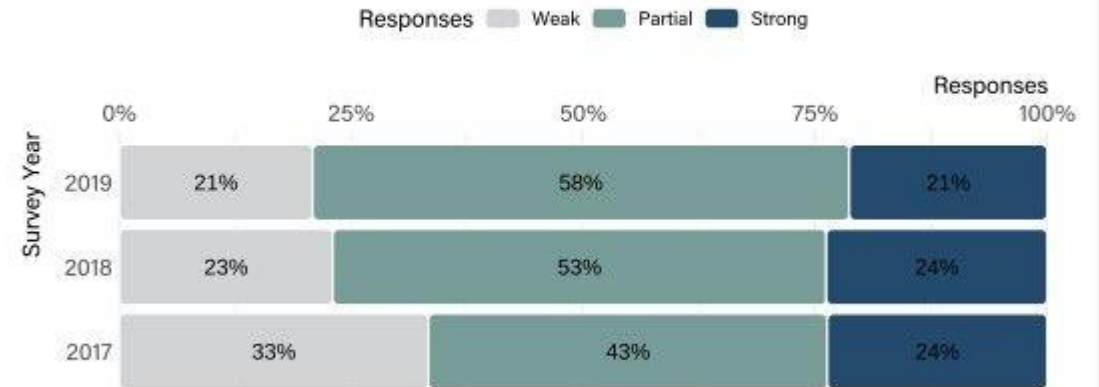
Which of the following best describes the training and skill sets of personnel who analyze and measure risk?



2019 Risk Management Maturity Benchmark Survey  
Conducted by FAIR Institute Aug-Oct 2019

## Analyst Skills

Which of the following best describes the training and skill sets of personnel who analyze and measure risk?

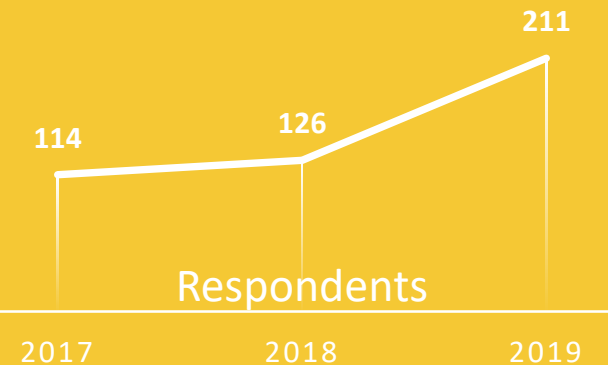
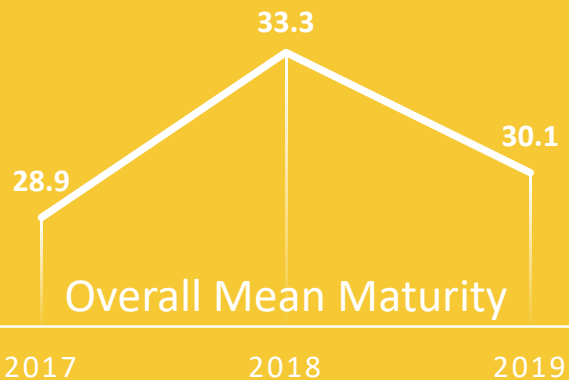


Risk Management Maturity Benchmark Survey  
Conducted by FAIR Institute 2017-2019

- 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



BLOG



FAIR BLOG



RESOURCES



RESOURCE LIBRARY

FAIR  
ANALYSIS

FUNDAMENTALS

RiskLens Academy



FAIR TRAINING & CERTIFICATION

FAIR



POWERED  
BY RISKLENS

FAIR-U TOOL

FAIR  
UNIVERSITY

CURRICULUM



FAIR UNIVERSITY CURRICULUM