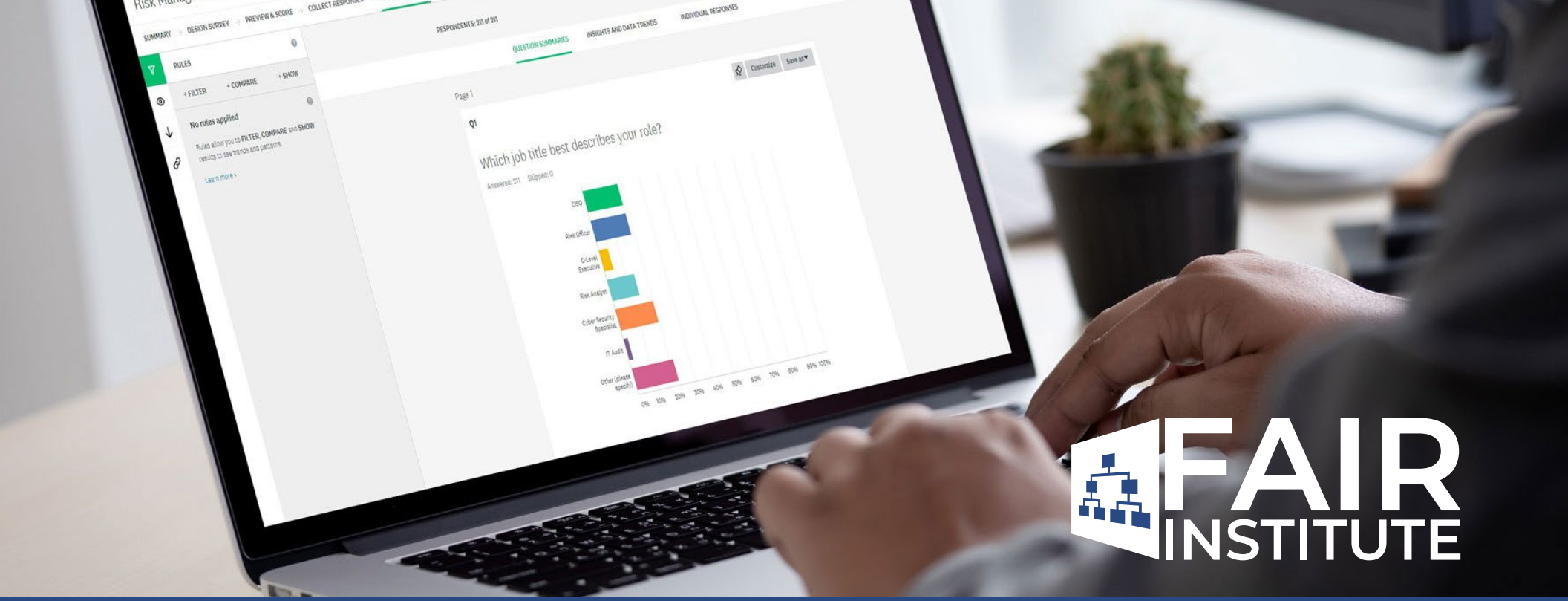


2019 Cyber Risk Management Maturity Benchmark Survey Results

Created for the FAIR Institute

*by **Jack Freund** Ph.D., FAIR Institute Fellow*

Sponsored by

RiskLens, RSA, RiskRecon, CyberVista, and Protiviti

Table of Contents

Introduction

Welcome to the third annual Risk Management Maturity Benchmark survey results, conducted by the FAIR Institute with generous sponsorship from RiskLens, RSA, RiskRecon, CyberVista, and Protiviti. This survey was created to help practitioners and their organizations improve the practice of risk management. That simply put, yet audacious goal is furthered through the continued educational offerings of the FAIR Institute and measured through these surveys and accompanying analysis.

In this third installment of the report, you will find a comparison of results year over year, information about how the questions and the model relate to one another, and information about a new question that was added as a trial to better understand how organizational model risk management views the cyber risk models in use in their organizations. Lastly, the report offers three areas for organizations that want to improve their risk management practice.

YAMM?

In information security broadly, and risk management specifically, it's important to ask why do we need "yet another maturity model" (YAMM)? Every model should ask itself this important question to better understand its purpose and goals, and if its continued existence is in furtherance of those goals. The FAIR Institute's Risk Management Maturity (RMM) framework is not above such self-evaluation. Many security and risk maturity models suffer from a disconnect between the reality of how the world works and the mechanics that attempt to emulate that in a model. A classic example of this phenomenon is that many security maturity scores are based on the number or degree to which security controls are implemented in an organization. The implicit model mechanics in cases like these purports that the more security "things" exist, the better the maturity of the organization. Such a straight-line, linear relationship is a model assumption that needs to be tested against reality to determine if such a principle actually exists in the real world.

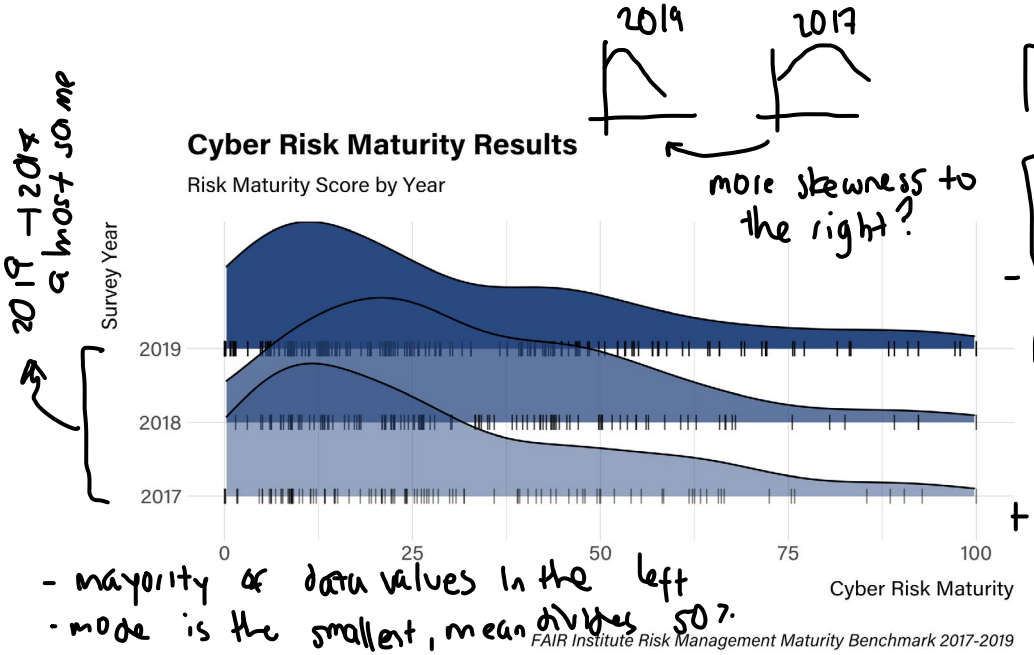
Security practitioners have undoubtedly encountered examples of this spurious understanding of information security. It assumes, at its core, that in order to be more secure that one must procure and provision more and more controls. This approach is diametrically opposed to the very thing it is purporting to measure: risk reduction. Indeed, many modern standards and public security policies are recognizing the importance of the need for a "risk-based approach" to allocating scarce resources to secure our computing environments.

It's in this environment that the FAIR Institute's Risk Management Maturity Model was released and continues to gain attention across the industry. It is the only risk maturity measurement built upon a solid model of how risk-based decision making occurs, focused on expectation setting and execution, two critical components of the risk management landscape.

More details about the model are available in the Appendix B and C, but for now let's focus on what the 2019 results told us about the practice of risk management.

2019 Summary Results

This is the largest sample size we've had in this survey with 211 respondents this year, up 85 from 2018 (126) and up 97 from 2017 (114). The average overall maturity dipped slightly from last year's results in a non-statistically significant way, however they are still above the first year's results. In 2019, the aggregate of the responses put maturity at 30.1 compared to 33.3 last year for a net loss of 3.2. 2017 results were at 28.9, so overall results are still up 1.2 from that evaluation. Given this is not a longitudinal survey (same respondents over time), there is a high probability that these results represent 1) new respondents who have not taken the survey before, 2) returning respondents that are at the same organization they were at in previous years, or 3) returning respondents that are at a new organization this year. In each case, there are variations that would cause the respondents to represent the maturity of their organizations differently. Some may have implemented additional changes in the organizations to grow maturity, some may have stopped certain practices (for example at the behest of a new senior leader), or others still may find themselves in an entirely new organization that has not endeavored to improve their risk management maturity. Given the possible shifts in respondent demographics, a 9.61% decrease in overall maturity since 2018 can fairly be called 'reasonably flat" from last year, especially when that same number represents a 4.15% increase over the baseline number from 2017.



Component	2017	2018	2019
Overall Risk Maturity	28.9	33.3	30.1
Execution	30.8	36.2	31.6
Prioritization	40.3	46.2	41.5
Policies Expectations	61.4	68.4	59.2
Risk Landscape Intelligence	33.7	37.6	38.3
Risk Management Analysis Quality	37.6	41.5	41.4
Risk Management Data Quality	42.1	44	44.1
Risk Analysis Quality	39.6	44.1	43.9
Risk Data Quality	52.3	53.2	51.9

When considering the domains that comprise this overall score, the reigning champion for best opportunity for improvement for the third year running is Motivation (45% weak), and a tie for second best area for improvement is in model quality and decision making visibility (each coming in at 35% weak). Again, we discovered that organizational resources and compliance requirements were the strongest domains (44% and 38% strong respectively), showing that the organizations represented here are well resourced and also highly regulated.

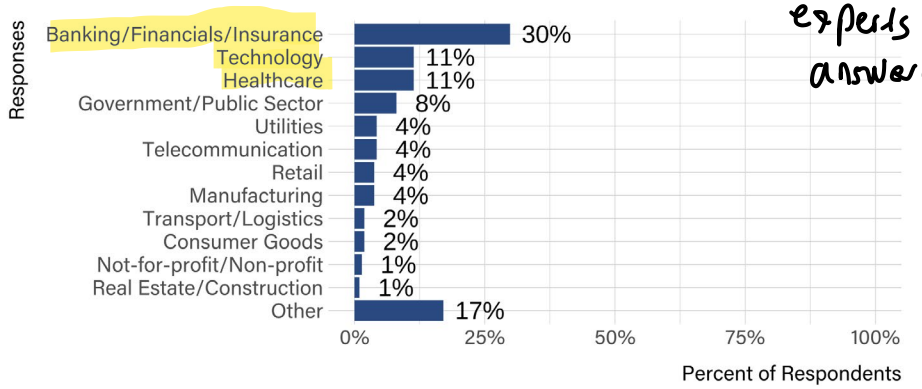
At a subdomain level, results were down to flat. The biggest decline was in policy exceptions. This category is driven by compliance requirements and the ability for the organization to manage priorities well. As it's unlikely that the respondent's organizations have less compliance requirements, this shift can be explained mostly by variation in respondents as the underlying scores for prioritization were mostly flat. Despite representing the largest decline, it remains the highest rated sub-domain

Demographics

As mentioned, this year we had a much higher response rate than previous years at 211 respondents. Regardless there was no statistical difference in the demographics of the respondents this year versus prior years. There were many industries represented, however 30% of respondents worked in financial services. Over half of the respondents worked for organizations with greater than $1B in annual revenue/results of operations. Respondents in roles such as specialist, analyst, or audit represent 36% of the responses, while people in executive roles comprised 41%.

Industry

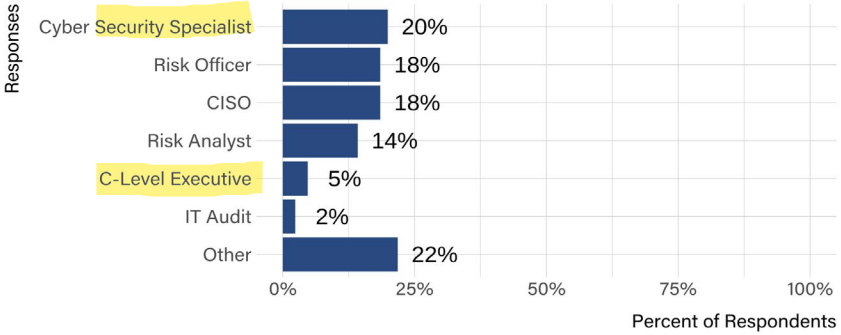
Which of the following best describes your industry?



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

Job Title

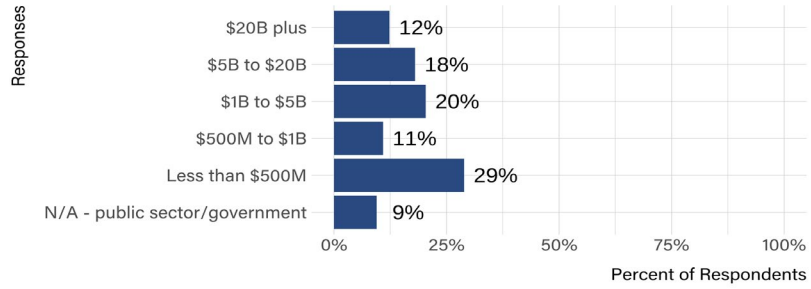
Which job title best describes your role?



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

Annual Revenue

What was the annual revenue/results of operations (ROO) for your organization last year in USD?

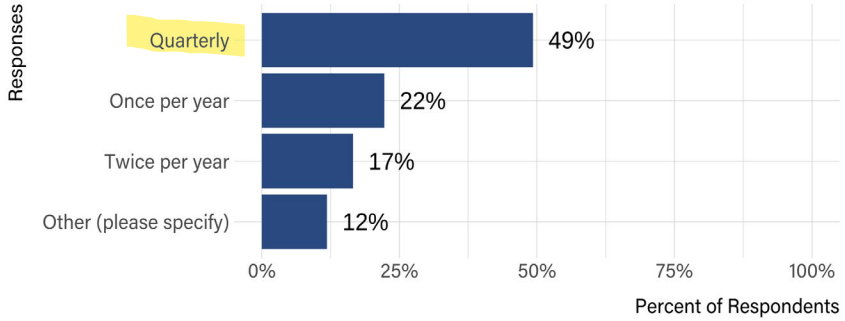


2019 Risk Management Maturity Benchmark Survey
Conducted by FAIR Institute Aug-Oct 2019

Reporting to the board appears to happen mostly quarterly for the respondents (49%) with another 39% reporting on cybersecurity once or twice annually. Those boards appear to have limited information security background, with just a third of respondents saying their boards have experience in the field. Most respondents said their boards don't have that background or they are unsure if they do (66%). Most respondents reported that their boards are satisfied with current cyber risk reporting (74%) with the remaining quarter of respondents saying their boards want better reporting. There is an interesting juxtaposition of response here vis-a-vis boards. most go to their boards four times a year to talk about cybersecurity. Only about one in three have a cyber background, but the vast majority are comfortable with the reporting. In some ways, this scenario appears to be a case of the innovation quote often attributed to Henry Ford: "If I had asked people what they wanted, they would have said faster horses." It is an open question whether the boards receiving regular cyber risk reporting are happy with the results because they don't know they should be expecting more.

Frequency of Reporting to Board

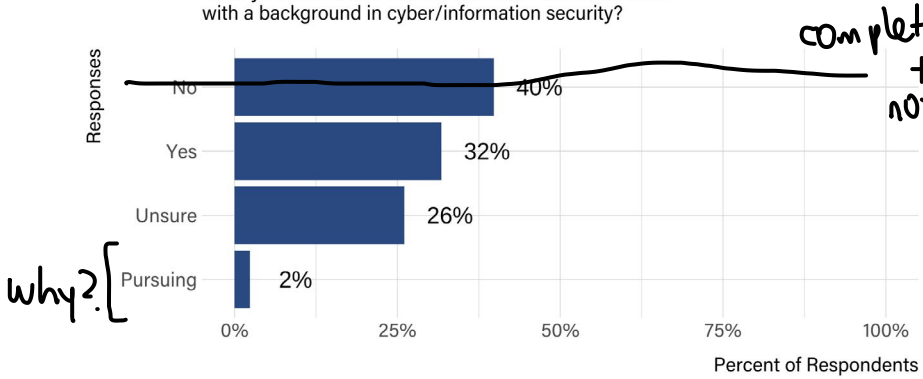
Which of the following best approximates how frequently your organization report on information/cyber security risk to the board of directors?



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

Board Includes Member with InfoSec Background

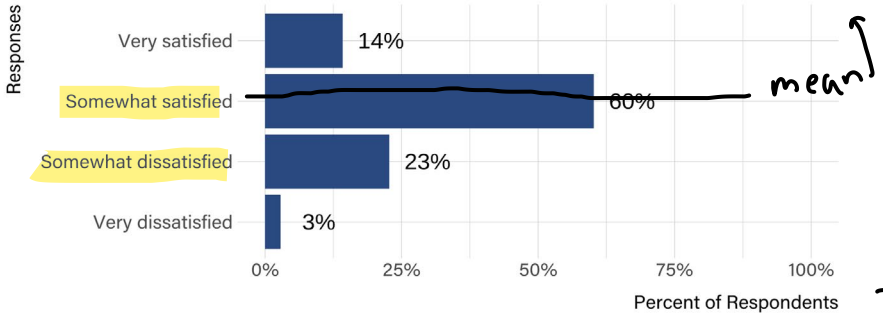
Does your Board of Directors have at least one member with a background in cyber/information security?



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

Board Satisfaction

How satisfied do you believe your Board of Directors are with current level of information risk reporting?

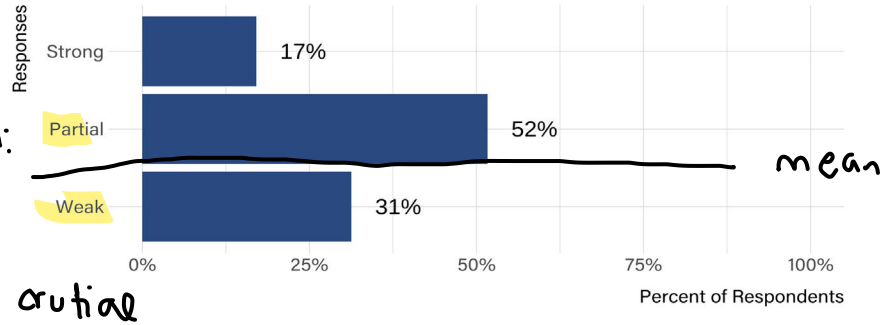


2019 Risk Management Maturity Benchmark Survey
Conducted by FAIR Institute Aug-Oct 2019

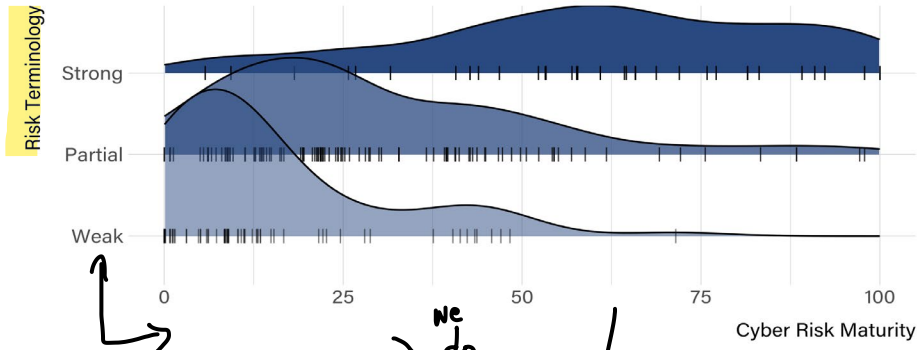
Whether your board is satisfied or not with the risk reporting it receives, one foundational way to improve board-level risk communication is by standardizing the use of risk terms, where only 17% said they have strong terminology usage. Information security is replete with conflation of the terms risk, threat, and vulnerability. To be sure, if you take a list of systems with missing patches to the board, you are certainly not talking about risk unless those systems are mapped to risk scenarios showing potential economic loss. Standardizing that communication into cyber induced risk to business objectives or mission risk seriously upgrades the level of conversation with boards.

Risk Terminology

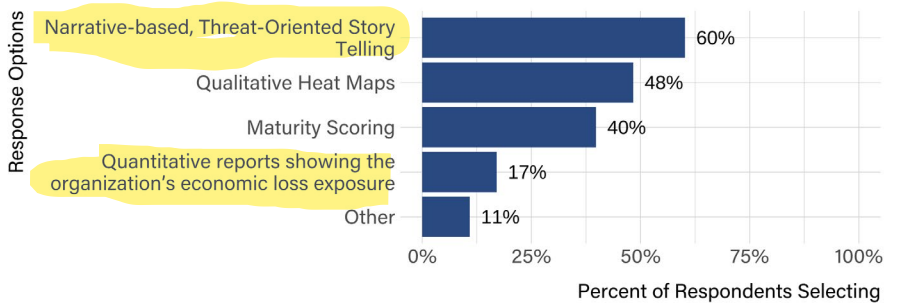
Risk Terminology: Which of the following best fits your organization's current usage of risk terminology?



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



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

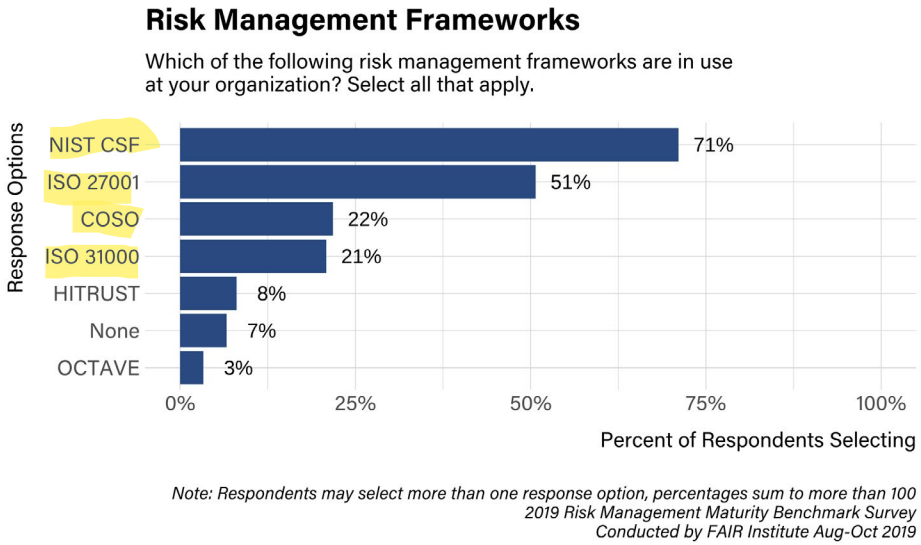


Note: Respondents may select more than one response option, percentages sum to more than 100
2019 Risk Management Maturity Benchmark Survey
Conducted by FAIR Institute Aug-Oct 2019

As a case in point, many respondents (60%) indicated their risk reporting relies on narrative storytelling, talking to board directors about threats. Just under half are using colored risk labels and heatmaps. Further, 40% indicated they use maturity reports to discuss their cybersecurity. Only 17% reported that they are using forecasted economic loss exposure in their board level risk reporting. This of course begs the question posed above: are boards aware that they could have economic impact reports as a part of their cybersecurity risk reporting?

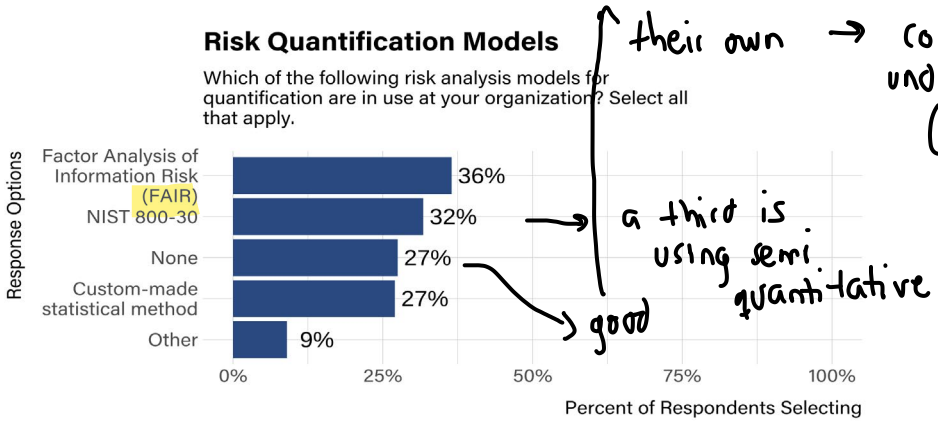
The great thing about standards...

A first for our respondents this year was the ability to represent the multiple frameworks they may be using. Organizations can choose to base their risk management practices on a single framework or multiple. Some will map between several to show compliance across a number of different frameworks. This year, we asked which models are being used for risk management and risk quantification. Far and away, NIST CSF is the most widely used framework for management, with 71% of respondents saying they use it. Other winners were ISO 27001 with over half saying they employ that model, and COSO and ISO 31000 pulling in about a fifth of respondents (22% and 21% respectively).



Note: Respondents may select more than one response option, percentages sum to more than 100
2019 Risk Management Maturity Benchmark Survey
Conducted by FAIR Institute Aug-Oct 2019

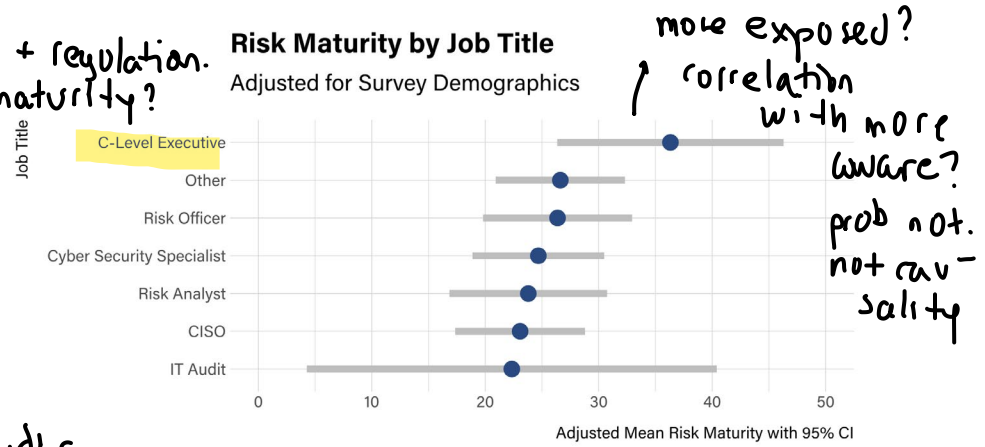
For those that were using risk quantification methods (about a quarter said they weren't - 27%), FAIR was the most widely used model at 36%. 32% claimed to use NIST 800-30 for quantification, although that document, Guide for Conducting Risk Assessments contains example tables for what they term semi-quantitative risk assessments only. There are no explicit fully quantitative examples. However, 27% did indicate they have developed their own custom-made statistical methods, which would fit under NIST 800-30.



Note: Respondents may select more than one response option, percentages sum to more than 100
2019 Risk Management Maturity Benchmark Survey
Conducted by FAIR Institute Aug-Oct 2019

Other Observations

We produced some marginal means charts this year to better explain the differences in responses by certain demographics. One standout this year by job title was that C-Level execs average risk score was markedly higher than all others, which were closely grouped (36.3 compared to 30.1 overall). CISOs had a much poorer view of their programs overall at 23.1. It should also come as no surprise that those organizations with revenue/results of operations over $20B scored higher than all others. Further, those in the financial services and technology industries have higher mean maturity scores, likely from the high levels of regulation and risk to which they are exposed.



Adjusted for Survey Year, Industry, and Annual Revenue
Risk Management Maturity Benchmark Survey
Conducted by FAIR Institute 2017-2019

company w/ $: better maturity : CEOs are pressured to solve immediacy (reactive) (not risk-based)

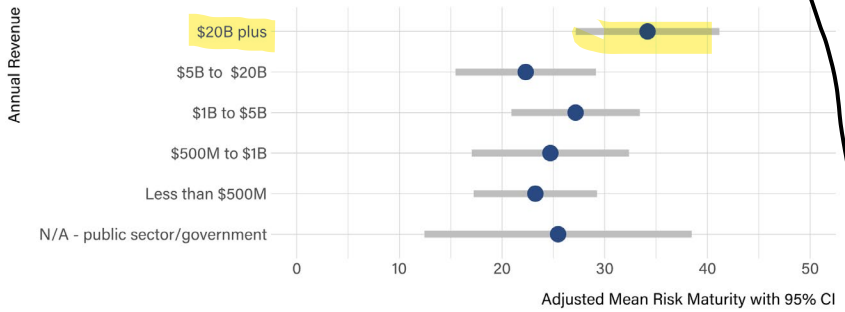
conclusion : not so good

Conclusions and where to go from here

If the aggregate results here represented a single organization, we'd not think very highly of their risk management practices. Taking these results to heart and working to build an improved risk management program can yield much improved decision-making capabilities for your organization.

Risk Maturity by Annual Revenue

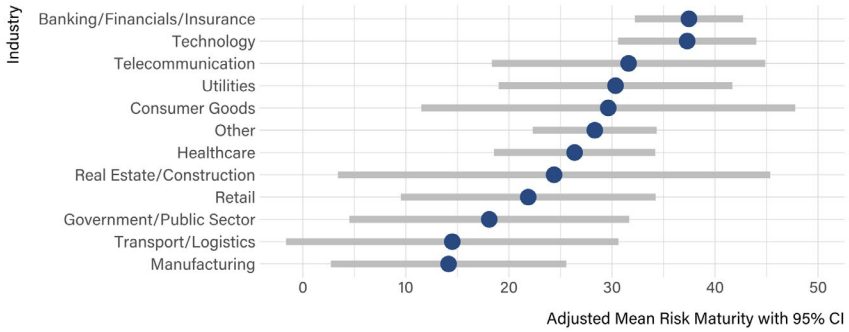
Adjusted for Survey Demographics



Adjusted for Survey Year, Industry, and Job Title
Note: Public Sector Goverment only available in 2019
Risk Management Maturity Benchmark Survey
Conducted by FAIR Institute 2017-2019

Risk Maturity by Industry

Adjusted for Survey Demographics



Adjusted for Survey Year, Job Title, and Annual Revenue
Risk Management Maturity Benchmark Survey
Conducted by FAIR Institute 2017-2019

Recommendation #1 - Incent your organization to meet expectations

The best opportunity for improvement is to create an environment where everyone in the organization wants to adhere to the expectations that are set by policies and standards. When diagnosing security failures (execution analysis), we need to ensure there is awareness of and capability to meet the expectations set in those documents. Most of the time, the trouble lies in a lack of motivation to adhere to them. This is not a result of purposeful sabotage or outright incompetence. Instead, we often expect those required to execute against these requirements to juggle multiple priorities. As a result, many business aligned leaders choose to solve business problems first, rather than adhering to strict security rules. To this end, alleviating the political pressure in the organization against prioritizing reasonable security is paramount. We need to adjust security expectations to a level that businesses can adopt alongside their other priorities. Lastly, casting information security risk in the language of business (as discussed elsewhere here) helps align the business and security teams to the same level.

to less incomp- not preparing

lack of experts : how do we talk in the same lang?

Recommendation #2 - Document and educate teams on decisioning processes

It's often the case that those in high levels of the organization don't always choose the security thing that is recommended to them. When this is met with consternation by the security staff, there exists a huge disconnect in the understanding of the organizational decisioning processes. Often there is a separation between how the security teams rank order priorities and how the organization views those rankings. This fundamental misalignment between business and security is at the root of this disconnect on visibility. Correcting this requires a common denominator of risk be used to link security concerns to the organizational goals or mission risk and that framework be made clear to the organization.

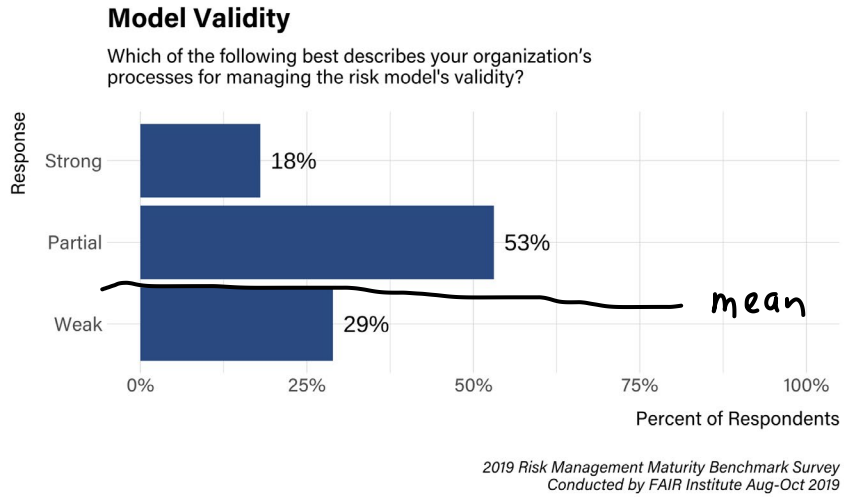
Recommendation #3 - Use high quality risk models

If we are relying on our risk models to help direct priorities, then any errors in those models will cascade into errors in our priorities. It's well established that simply following a process (any process) will make the participants feel as if they have received value from it. So, in this respect, it doesn't matter which methodology is used to measure risk as the organization will have perceived value. However, that is not the metric that should be applied. You need to compare the decisions resulting from the model against random and/or unsupported decision making. If your decisions with the model are no better than those without, you need a higher quality model. Simply put, your model needs to employ measures that have valid units associated with them, such as frequency or probability, as well as measuring impact using financial values to reflect the impact the organization will have if it materializes.

avoid semi-quant models, use financial terms

The new question posed this year about model validity was added to better understand how well organizations are testing the models they use for risk management. Sadly, only 18% said they have strong model validity. The rest have little to no oversight over whether their models are implemented correctly, account for bias, or represent reality. Although formalized model validation practices mostly exist in financial services, this has many benefits for those in other industries. For instance, those 18% that said they have strong validity practices also reported that they have stronger risk terminology usage and more satisfied boards comprised of at least one member with a background in cybersecurity that get risk reports at least quarterly. Taking steps to document and audit the way cyber risk models are implemented, how they account for bias, and conduct back testing to see it they correctly predict loss are fundamental for improving risk management practices overall.

relate / link many correlations + terminology + satisf (expert) + valid practices



As a profession, cybersecurity cares about the state of technology in their organizations. Many often feel personally accountable for blocking all attacks headed their way. This is an important mindset to have when in the trenches with responsibility for keeping the bad guys out. However, risk-based thinking augments this by overlaying an important realistic factor: on a long enough timeline, such defensive tactics will fail and when they do, risk managers want their organizations to be prepared. High quality models that reflect the economic reality of such incursions are a centerpiece for bringing the reality of cybersecurity to the business, enabling them to make better, well-informed decisions to direct the resources of the organization to the highest priority activities.

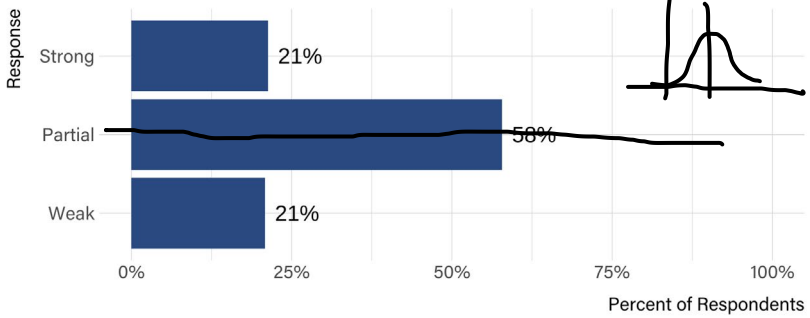
risk mgmt → better decisions

Appendix A – Complete Results

This section shows complete results not already discussed

Analyst Skills

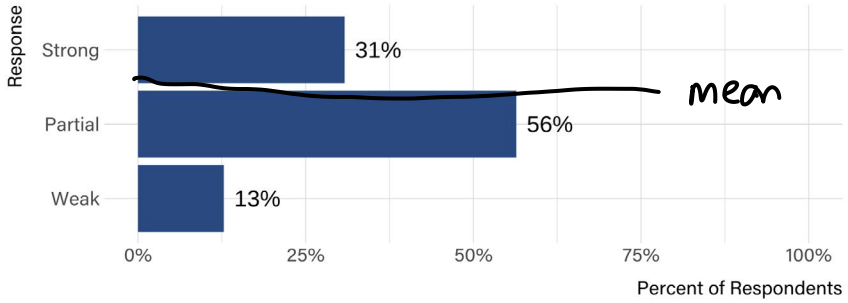
Which of the following best describes the training and skill sets of personnel who analyze and measure risk?



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

Awareness

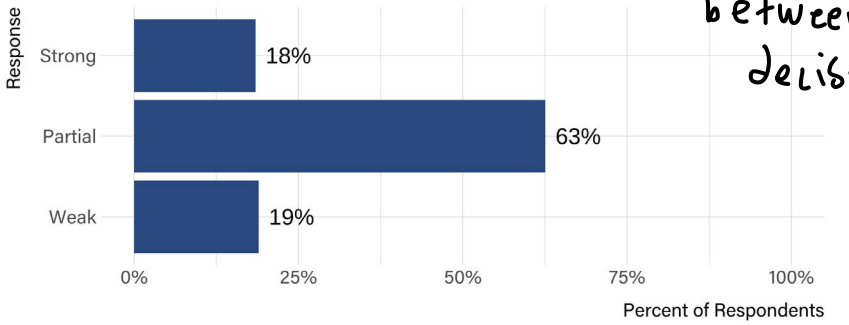
Which of the following best describes how aware personnel are of the organization's expectations (e.g., policies and standards) regarding their information security related responsibilities?



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

Asset Visibility

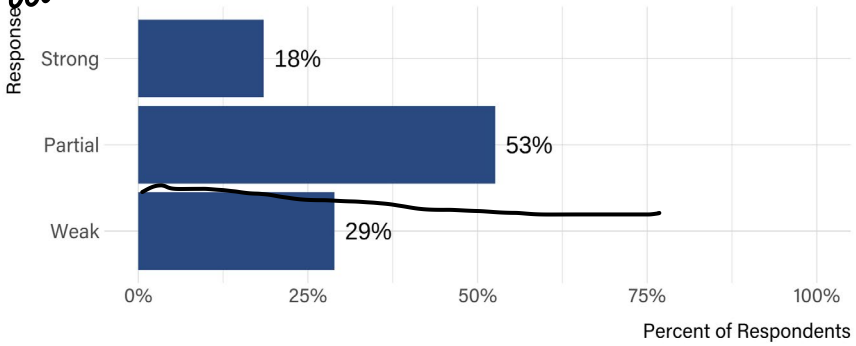
Which of the following best describes your organization's visibility into its system and information assets?



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

Capabilities

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

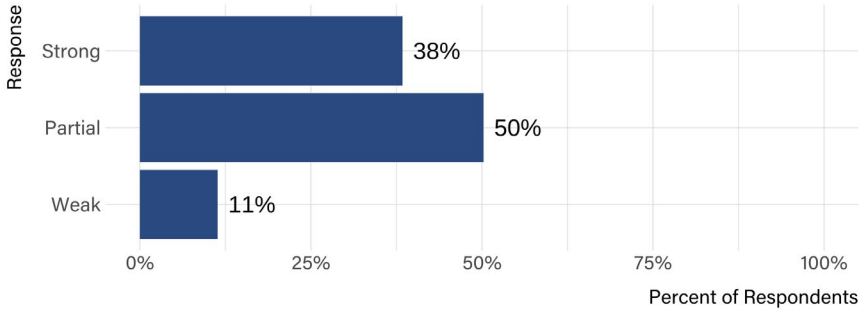


2019 Risk Management Maturity Benchmark Survey
Conducted by FAIR Institute Aug-Oct 2019

Compliance Requirements

strongly regulated

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.)?

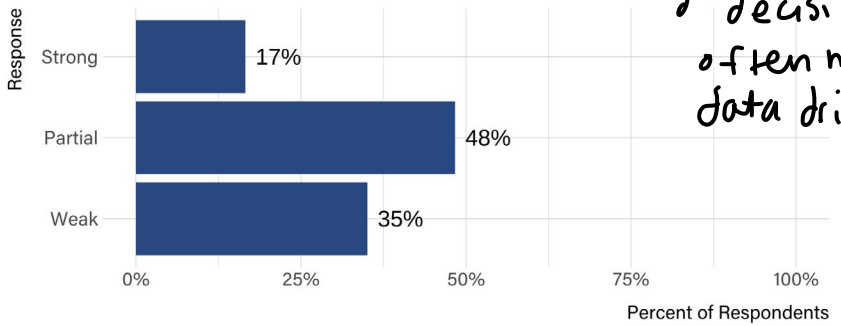


2019 Risk Management Maturity Benchmark Survey
Conducted by FAIR Institute Aug-Oct 2019

Decision Making Visibility → weak visibility

(unfundamented decisions, often not data driven)

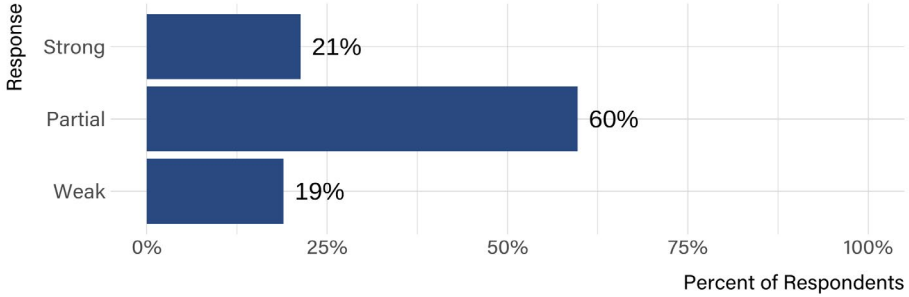
Which of the following best describes your organization's visibility into risk decision-making?



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

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)?

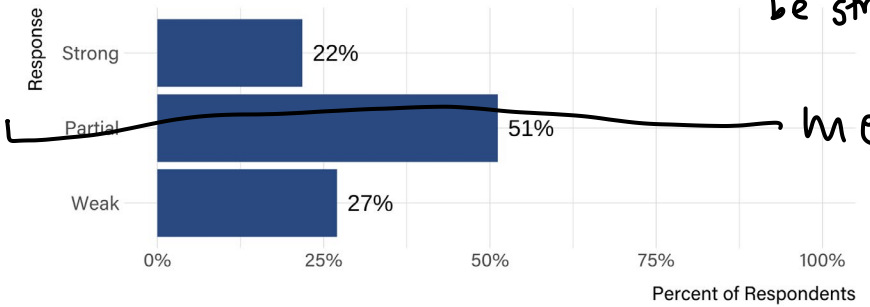


2019 Risk Management Maturity Benchmark Survey
Conducted by FAIR Institute Aug-Oct 2019

→ models treat execution visib with indifference (should be strong)

Execution Visibility

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



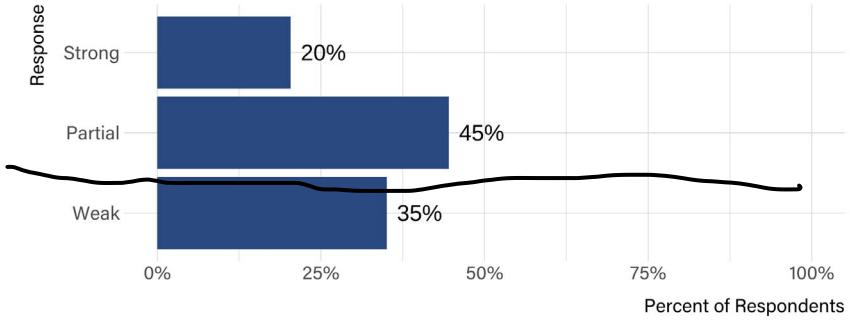
mean

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

Model Quality

due to lack of execution. analysis

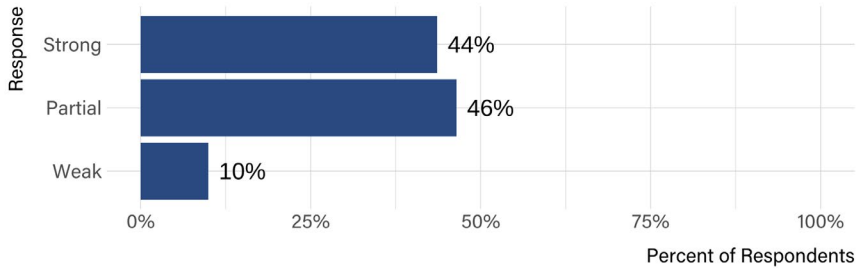
Which of the following best describes the models used to evaluate and measure risk?



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

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.)

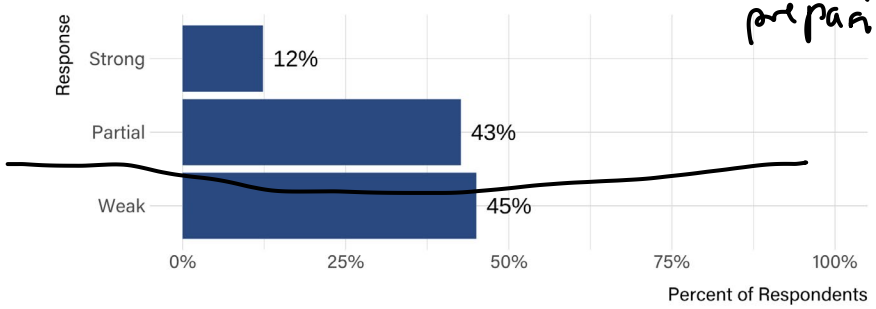


2019 Risk Management Maturity Benchmark Survey
Conducted by FAIR Institute Aug-Oct 2019

Motivation

they are not preparing

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

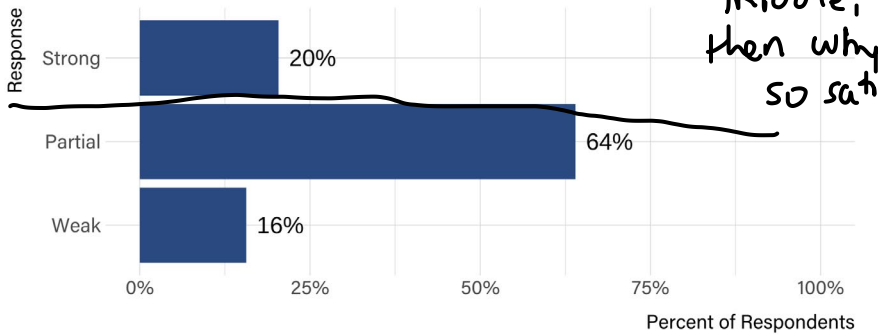


2019 Risk Management Maturity Benchmark Survey
Conducted by FAIR Institute Aug-Oct 2019

Risk Reporting Quality

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

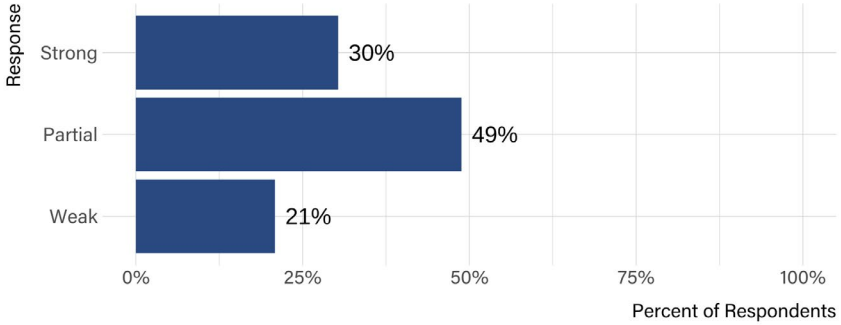
quality middle, then why so satisfied?



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?

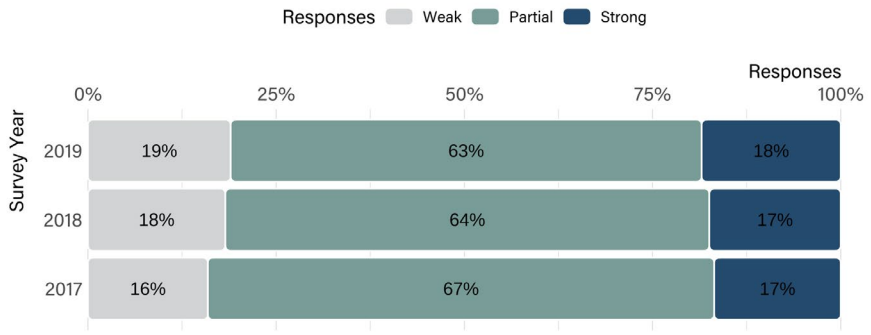


2019 Risk Management Maturity Benchmark Survey
Conducted by FAIR Institute Aug-Oct 2019

Asset Visibility

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

(stale)

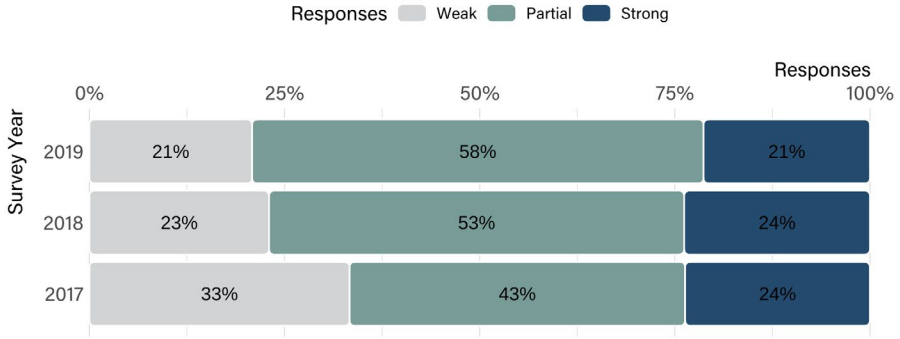


Risk Management Maturity Benchmark Survey
Conducted by FAIR Institute 2017-2019

experts that analyse are ok, but not (grow) the C-levels or boards

Analyst Skills

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

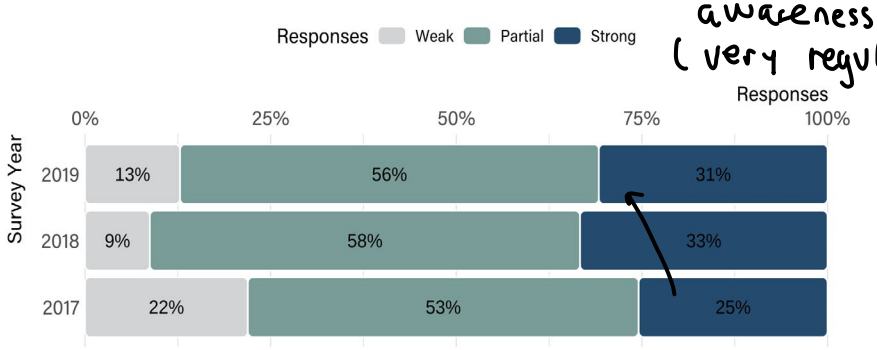


Risk Management Maturity Benchmark Survey
Conducted by FAIR Institute 2017-2019

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?

strong expect awareness (very regulated)



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

Capabilities

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

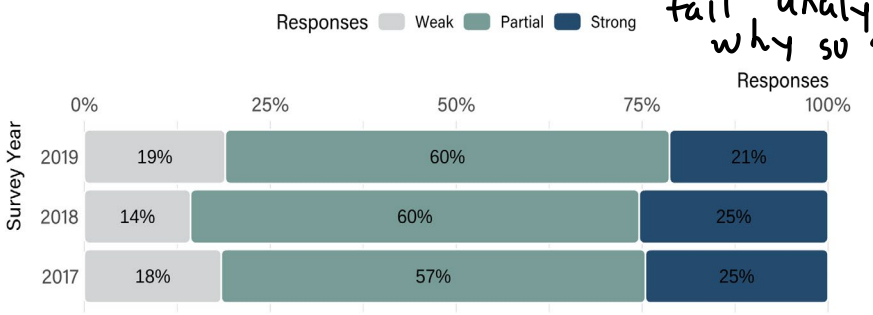
Risk Management Maturity Benchmark Survey
Conducted by FAIR Institute 2017-2019

personnel analysis skills grow, but past data doesn't?

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)?

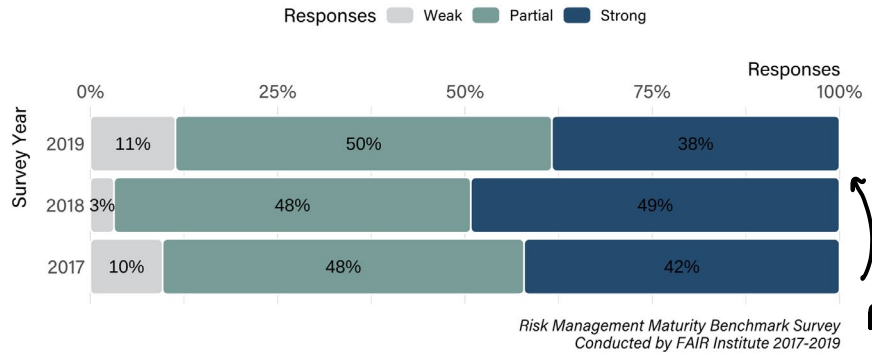
Stale : logs are important for fail analysis why so stale?



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

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.)?



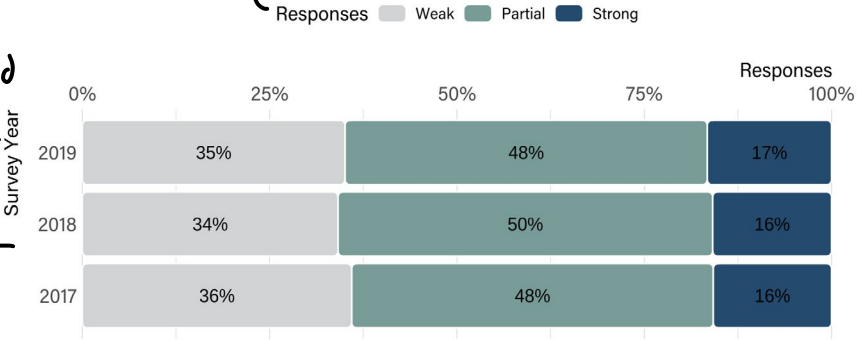
Risk Management Maturity Benchmark Survey
Conducted by FAIR Institute 2017-2019

reduced regulatory requirements. why?

Decision Making Visibility

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

stale

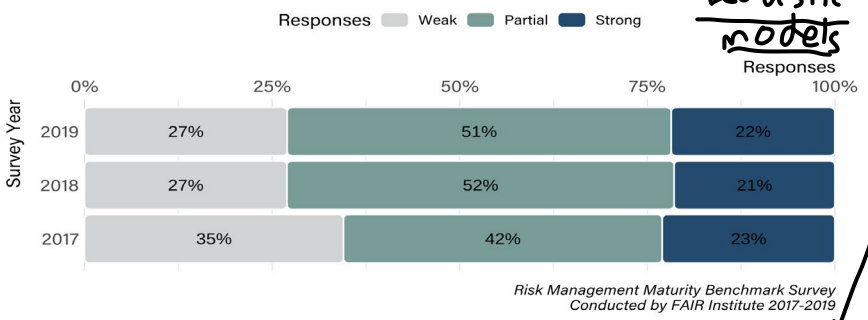


Risk Management Maturity Benchmark Survey
Conducted by FAIR Institute 2017-2019

maybe that's why so satisfied with reporting

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

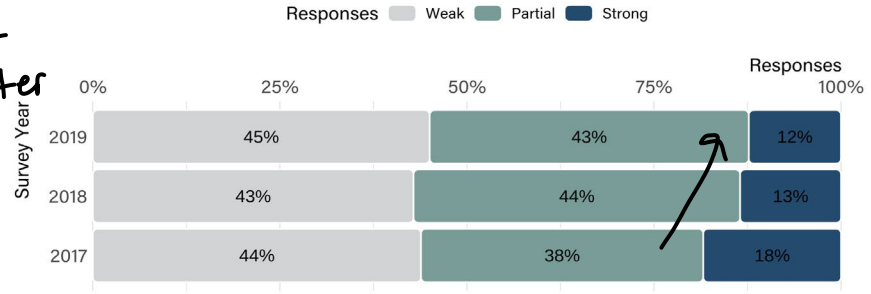
Model Quality

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

Motivation

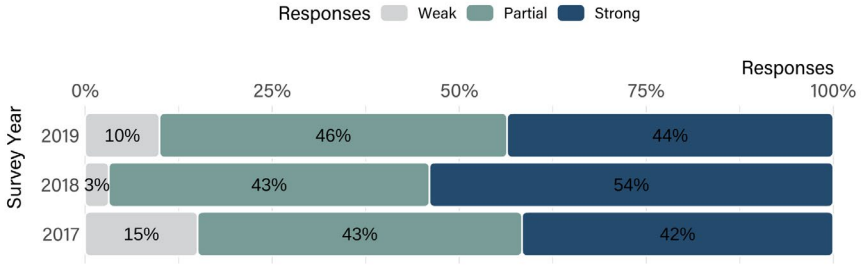
Which of the following best describes how personnel are incentivized to meet the organization's risk management expectations (e.g., policies and standards)?



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

Organizational Resources

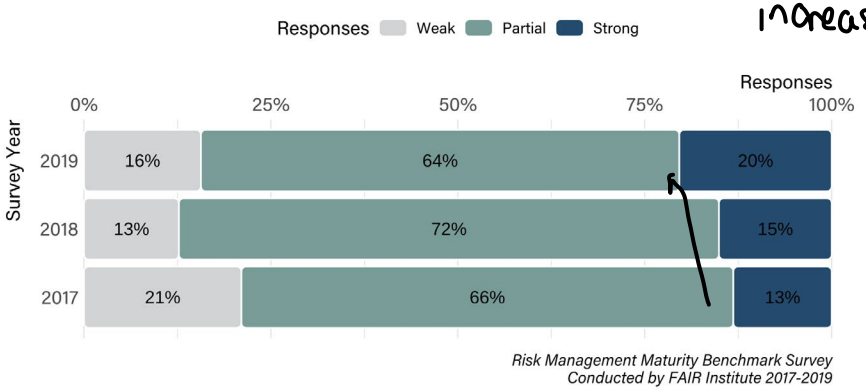
Which of the following best describes the company's/enterprise's capacity for funding information security? (Note that this is not asking whether the information security program is being well-funded, but rather whether it could be well-funded if senior executives considered it to be a priority.)



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

Risk Reporting Quality

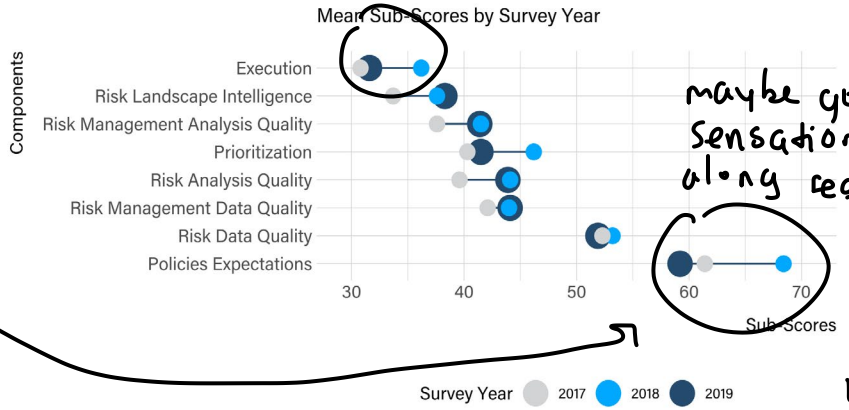
Which of the following best describes your organization's risk reporting?



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

Risk Maturity Model Components

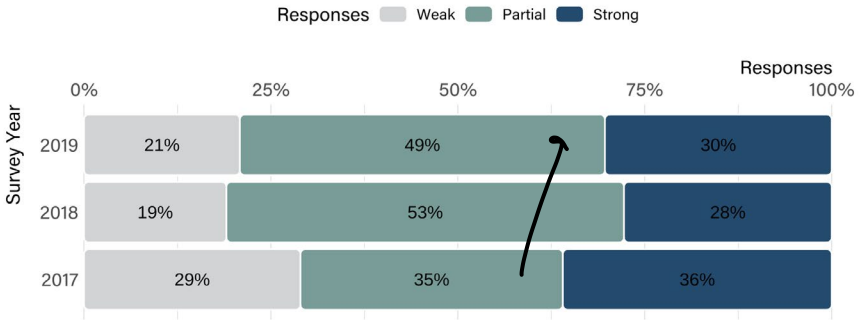
Mean Sub-Scores by Survey Year



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

Threat Visibility

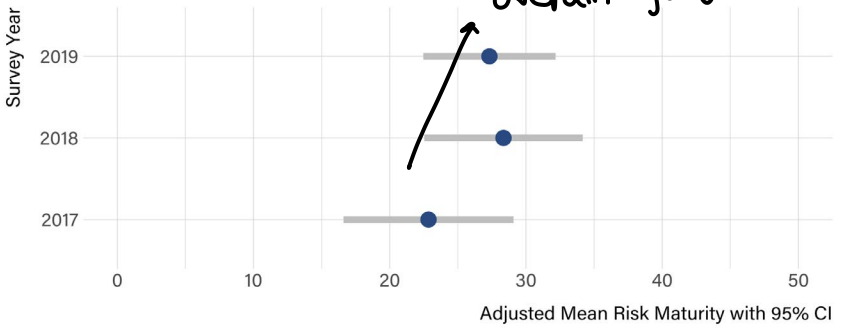
Which of the following best describes your organization's visibility into the threat landscape?



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

Risk Maturity by Year

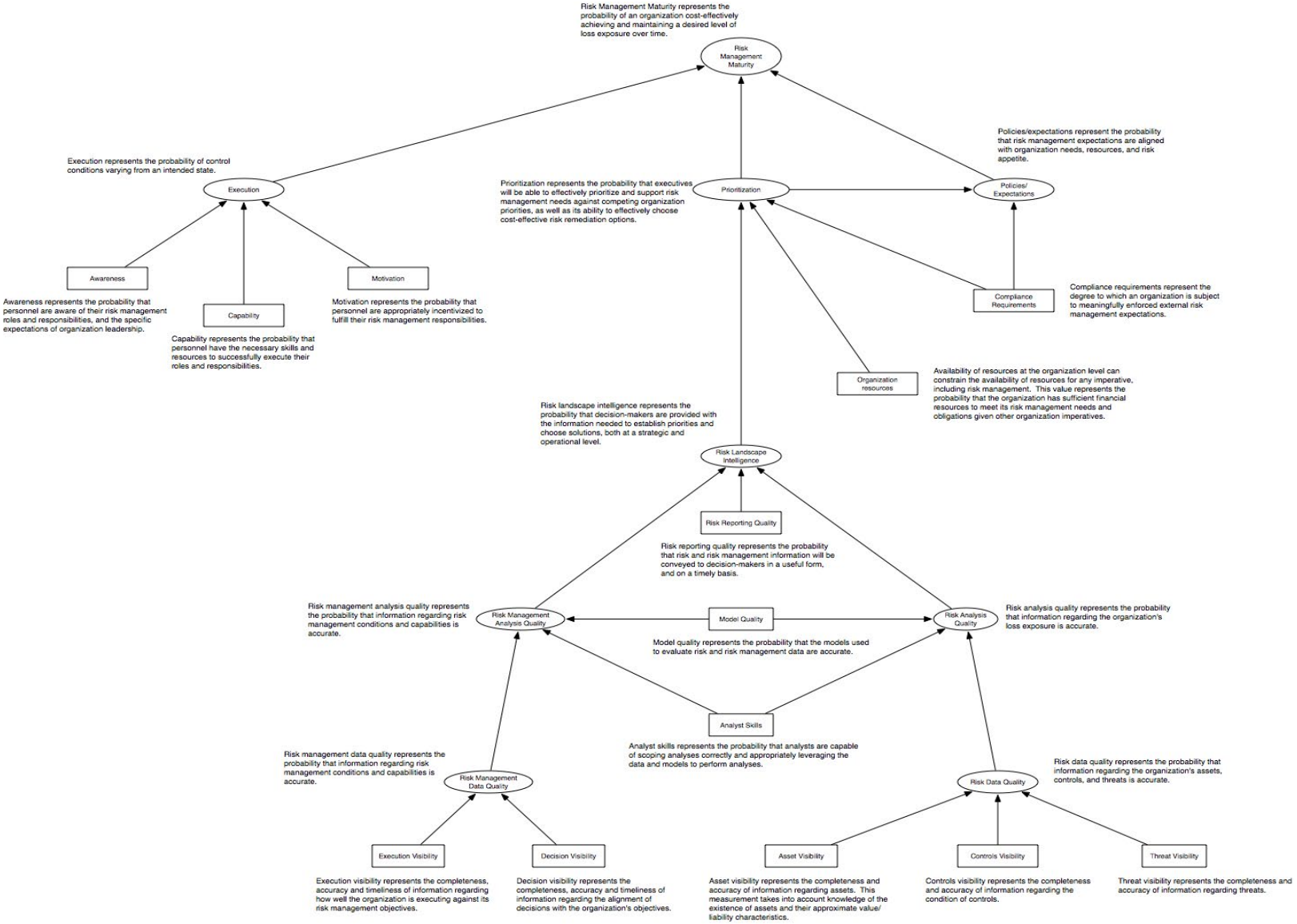
Adjusted for Survey Demographics



Adjusted for Job Title, Industry, and Annual Revenue
Risk Management Maturity Benchmark Survey
Conducted by FAIR Institute 2017-2019

Appendix B – Model Ontology

This diagram illustrates the relationship between the elements in the model.



Appendix C – Survey Limitations

Despite efforts to provide greater clarity and rigor in this analysis, this model and the data applied to it are subject to many of the same challenges faced by any other analysis — particularly survey-based studies. These challenges include:

- Because many of the respondents are believed to be members of the FAIR Institute (responses were anonymous), their selection was not truly random, therefore, the data may not perfectly reflect the profession as a whole. In fact, the scores in this survey are somewhat higher than we have encountered in organizations we've evaluated outside of the survey.

- Respondents came from various roles within their organizations, and with different tenures, which means the accuracy of their responses may be constrained by an incomplete or inaccurate understanding of their organization's condition.

- Respondents were asked to choose which of three responses for each question most closely represented their organization. This introduces at least two challenges:

    1. Limiting responses to three choices inherently constrains the ability to capture nuances that may exist in an organization, and

    2. The meaning and intent of survey questions and response choices may be interpreted differently by different people, which introduces the potential for inconsistency across respondents.

- The probabilities underlying the Bayesian network should be considered "Bayesian priors" — i.e., they are calibrated subject matter expert estimates and are not yet supported by statistically significant empirical data. As a result, analysis results should be thought of as "directionally correct".

- Lastly, no models are (or ever will be) perfect representations of the complex factors that drive something like risk management efficacy. The quality of this model will undoubtedly improve over time as we receive feedback, as more empirical data surfaces, and as additional analysis on the subject occurs.

Jack Freund, PhD, Co-Author, Measuring and Managing Information Risk: A FAIR Approach & FAIR Institute Fellow

Dr. Jack Freund is a leading voice in cyber risk measurement and management. He is an expert at using risk quantification to implement, mature, and sell information risk and security programs. Jack is currently serving as Director, Risk Science at RiskLens and previously worked for TIAA as Director, Cyber Risk. The book Jack co-authored on quantifying risk (Measuring and Managing Information Risk: A FAIR Approach) was inducted into the Cybersecurity Canon in 2016. Jack's writings have appeared in the ISSA Journal, Homeland Security Today, and the @ ISACA newsletter.

Read Jack's book:
Measuring and Managing Information Risk: A FAIR Approach.

The FAIR Institute is an expert, non-profit organization led by information risk officers, CISOs and business executives, created to develop and share standard information risk management practices based on FAIR. Factor Analysis of Information Risk (FAIR) is the only international standard quantitative model for information security and operational risk. FAIR helps organizations quantify and manage risk from the business perspective and enables cost-effective decision-making. To learn more and get involved visit **FAIR Institute.**