November 2017

Where Do We Go From Here?

2017 Risk Management Maturity Benchmark Survey

Sponsored by:

RiskLens RSA

TABLE of CONTENTS

Overview

The cyber and technology risk profession continues to evolve many of its practices. That said, unanswered questions remain, such as:

- How mature is the profession today?
- Where are we weakest/strongest?
- Which improvements in maturity are likely to matter most?
- How do we rate against others in our industry?

This survey was undertaken to help gauge the current state of cyber and technology risk management maturity. The intent being, if we know our strengths and weaknesses — and their significance — then we can make informed choices about how to improve over time. But why this survey? Don't maturity models already exist for our profession and, if so, why not simply use them? The answer boils down to differences in what the models are measuring, and how the measurements are evaluated to arrive at a result.

Without getting into gory modeling details here, suffice it to say that many of the most commonly used maturity models within our profession infer maturity from what could be described as lagging indicators — e.g., whether certain policies exist, technologies are in place, or processes have been defined. This is a bit like inferring whether a teenager is mature by the clothes they wear and the grades they get in school. Might there be a correlation between these indicators and maturity? Certainly. That said, many of us know teenagers who dress reasonably well and get decent grades, but whom we would never entrust to care for something we value. Their ability to make good decisions and perform reliably simply isn't where it needs to be. Likewise, many of us also know organizations that score reasonably well on common maturity assessments, but have significant difficulty prioritizing well or executing reliably.

Defining Maturity and the Analysis Model

Most maturity models don't explicitly define what maturity represents. Instead, the data points being measured are simply averaged to arrive at an overall maturity score, which is usually ordinal in nature (e.g., an overall maturity of 3.62 out of 5). Although these scores can be useful for determining whether an organization is getting better or worse over time, the score itself doesn't have a clearly defined meaning. A higher score is simply better than a lower score. Furthermore, the relevance of each data point is often assumed to be the same as all the others (unweighted), and dependencies between data points are not accounted for.

In order to provide more explicit context for determining which factors should be measured, how they should be analyzed, and what the results mean, in this model we define a mature organization as one that can cost-effectively achieve and maintain an acceptable level of risk. Measuring maturity then becomes a matter of estimating the probability that an organization is operating in this state. In order to arrive at this estimate, we have to understand and evaluate the factors that drive it.

Within the model used here, the factors that drive maturity were arrived at through a combination of root cause analyses performed within various organizations, logical decomposition of factors into layers

of an ontology, and agent-based modeling[1]. The result was a Bayesian network of these factors, which enabled probabilistic modeling. (NOTE: The details of this model are beyond the scope of this document.)

The underlying premise of this model is that cost-effectively achieving and maintaining an acceptable level of risk is dependent upon two dimensions:

1. The degree to which decision-makers are able to make well-informed decisions (e.g., set appropriate policies and objectives, prioritize effectively, choose cost-effective solutions, and treat root causes). At a high level, well-informed decisions are analyzed within the model as a function of:
    1. Visibility into the risk landscape
    2. The quality of analysis and reporting
    3. Externally stipulated compliance requirements (which act as guard rails)
    4. Root cause analysis
    5. Resource availability
2. The degree to which the people who must execute against those decisions, do so reliably, which is a function of their:
    1. Awareness of what's expected of them
    2. Ability to perform what's expected of them (skills and resources)
    3. Motivation to meet their risk management responsibilities

Deficiencies that exist in these factors, or the factors below them in the ontology, drives the probability of cost-effectively achieving and maintaining an acceptable level of risk — i.e., the organization's maturity.

[1] https://en.wikipedia.org/wiki/Agent-based_model

Key Findings from the Survey

- Only 5% of respondents rated their organizations as “Strong” across ten or more of the fourteen factors.
- On average, risk management maturity levels were low, regardless of industry or organization size. Interestingly, the four highest-scoring organizations came from different industries, which suggests that maturity isn’t the exclusive domain of any one industry.
- The decision-making and execution dimensions of the model scored equally low for most respondents, which suggests that as a profession we struggle to both prioritize/choose wisely or execute reliably. An argument can be made (and anecdotal evidence supports this) that execution improves as decision-making improves, the hypothesis being that when stakeholders have greater faith in the decisions they make, they provide greater support and incentives for those who have to execute.
- The factor *Motivation* (incentivizing reliable execution of risk management responsibilities) scored lower than any other factor (44% reported this element as “Weak”). Not surprisingly, sensitivity analysis suggests that, out of all of the individual factors, strengthening this factor should provide the most significant overall lift in program efficacy. Note, however, that getting executive management to strongly motivate personnel generally requires that they understand and believe in the risk-relevance of the issues and their choices (as alluded to in the previous bullet point). Consequently, being well-informed regarding the risk landscape is often a prerequisite to effective incentives.
- The factor *Model Quality* scored second lowest, with 43% of respondents reporting this as “Weak” — i.e., their organizations rely heavily on the intuition and mental models of risk practitioners to make sense of the risk landscape. Unlike the Motivation factor above, improving the Model Quality factor would not by itself generate significant improvement in decision-making because it would be constrained by other factors (specifically Asset, Control, and Threat data, as well as Analyst Skills) that also did not tend to score well in the survey.

Analysis and Overall Results

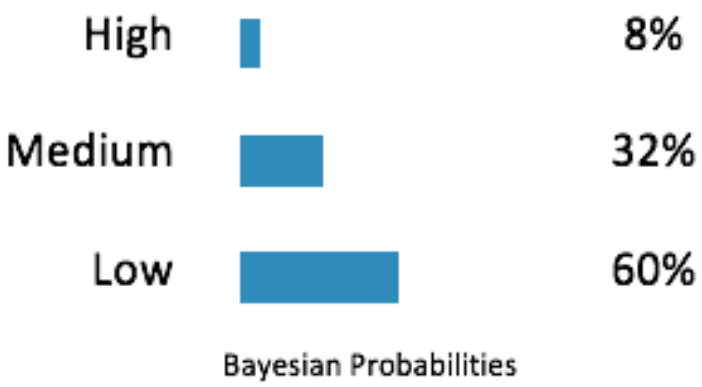
Because insufficient data currently exist to empirically or precisely define quantitative levels of maturity, we defined three qualitative levels of maturity:

- High Maturity — An organization will reliably and cost-effectively achieve and maintain an acceptable level of risk, even within a dynamic risk landscape
- Moderate Maturity — An organization may periodically achieve an acceptable level of risk, but not cost-effectively, and it will not be able to maintain it over time
- Low Maturity — An organization will not be able to achieve or maintain an acceptable level of risk.

This simple ordinal scale provides sufficient granularity for an analysis of this nature that is intended to generate insights regarding the industry and provide ballpark accuracy rather than high levels of precision. Additionally, Bayesian networks are uniquely capable of leveraging subject matter expert estimation and qualitative scales to represent probabilities for scales of this nature.

Overall Summary Analysis

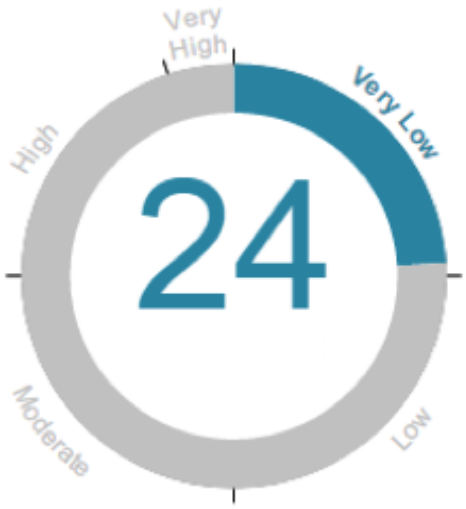
The weighted average of survey responses were fed into the model, which generated the following results:

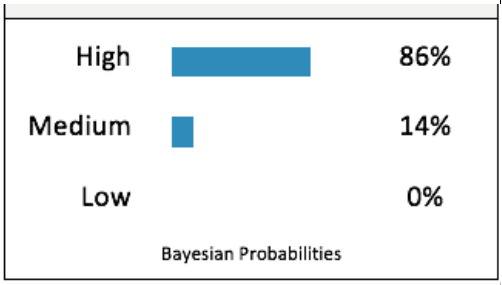
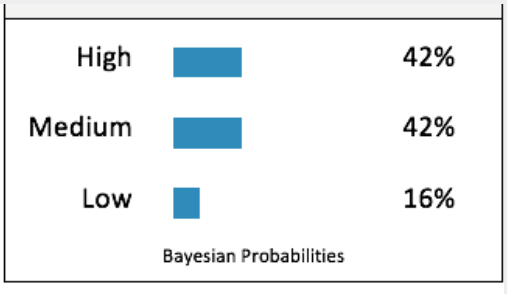


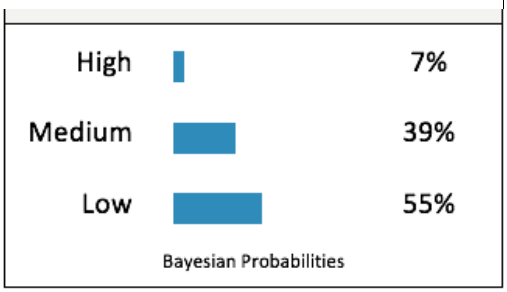
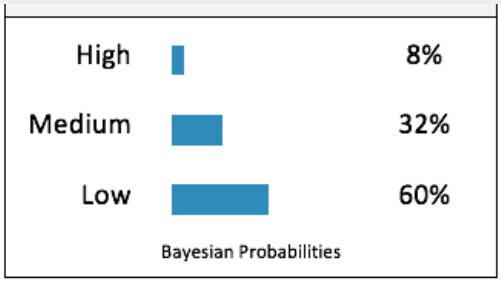
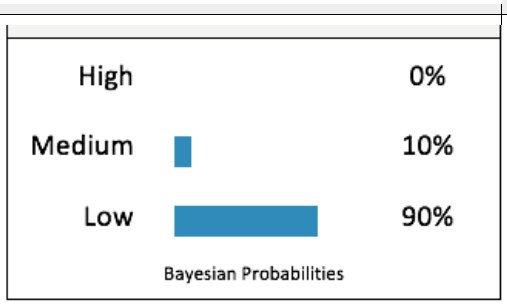
These results suggest there is an 8% probability that an average organization within the survey population would operate at a High level of maturity, a 32% probability that it would operate at a Medium level of maturity, and a 60% probability that it would operate at Low maturity.

An index value was then generated from these values, which makes comparisons between organizations, and trend analysis, easier. The index value generated for the average organization was 24 (out of 100). In other words, an average organization would be leaning strongly toward the bottom of the maturity scale.

Although an average value can useful in characterizing a population, it is just one data point out of several that help to shed light on what's being measured. The following table provides additional insight into the maturity of organizations that responded to this survey:



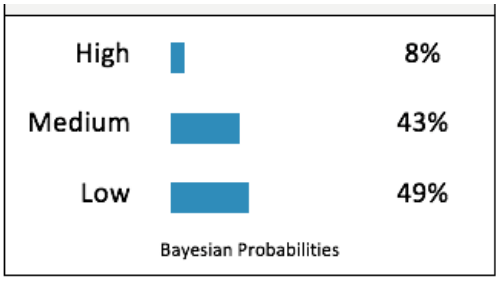
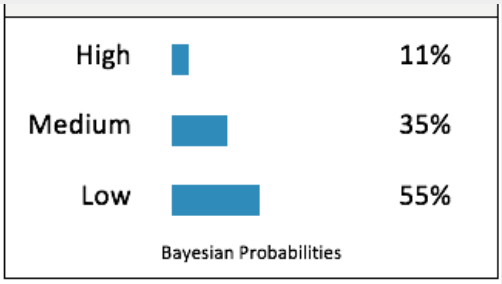
	Bayesian Probabilities	Index Score
Highest score		92
90th percentile		62

	Bayesian Probabilities	Index Score
75th percentile		26
Average		24
Lowest score		5

These results suggest that even those organizations in the 90th percentile aren't mature in any real sense. They may be better than most of their contemporaries, but they appear to still have a long way to go. Most organizations represented within this survey fell well within the Low level of maturity.

Industry-versus-Industry Analysis

Although many industries were represented within the survey, only the Financial Services (27%) and Technology (23%) industries had enough participation to allow for meaningful comparisons. As illustrated in the table below, the differences in maturity between these two industries was not substantial.

	Bayesian Probabilities	Index Score
Financial Services		30
Technology		28

As you can see, the averages for both of these industries scored in the top quartile relative to all respondents.

From an individual factor perspective, the only meaningful difference between these two industries was in Compliance Requirements. The stronger compliance requirements within Financial Services are suspected to act as decision-making guardrails, which can result in a somewhat more mature approach to risk management, overall, than exists in less-strongly regulated industries.

Differences by Organization Size

Comparing results based on organization size did not generate profound insights — unless, of course, the insight is that organizations of all sizes appear to be equally immature. That said, there were two factors in the model where meaningful differences did appear to exist:

- Organizational Resources, and
- Threat Visibility

Specifically, (and not surprisingly) organizations below $500M in annual revenue scored significantly lower in Organizational Resources than did more “wealthy” organizations. Similarly, organizations below $1B in annual revenue scored substantially lower in Threat Visibility. It seems logical to assume that, due to the costs involved in maintaining good threat visibility, there would be a correlation between these two factors.

Interestingly, lower scores in these dimensions did not result in a meaningful difference in overall risk management maturity for smaller organizations. The reason is that the model’s results reflect the aggregate effect of many risk management dimensions. In other words, the fact that larger organizations have more resources is offset by deficiencies in other dimensions.

Conclusions

The Trappings of Risk Management

These results suggest that cyber and technology risk management programs may be focusing on the trappings of risk management (putting policies, processes, and technologies in place) rather than the fundamentals of well-informed decision-making and reliable execution. As a result, these programs are more likely to:

- Struggle with identifying and maintaining a focus on their most significant priorities, therefore wasting limited resources on lower risk concerns and potentially delaying remediation of truly high risk concerns.
- Implement risk mitigations that are less cost-effective, thereby missing the opportunity to apply the mis-spent resources on other risk concerns or business opportunities.
- Experience control failures due to unreliable execution, which introduces avoidable levels of risk.
- Experience "risk management groundhog day" — i.e., repeatedly experiencing the same failures by not recognizing and treating root causes.

Implementing the Fundamentals of Effective Risk Management

To be clear, the outcome of well-informed decisions within a mature organization would include some of the same policies, processes, and technologies (lagging indicators) commonly found in risk management programs that aren't mature. The practical difference is expected to boil down to being able to reduce noise and focus more effectively on truly high risk concerns, choose cost-effective solutions to the risk management measures that are implemented, and more effectively align with organization leadership's risk appetite. This better alignment also should improve the organization's ability to execute reliably by reducing political friction and resource contention and by increasing the odds that management will incentivize risk management responsibilities at all levels appropriately.

Improved execution also should be expected to occur from more rapid recognition and treatment of root causes, particularly when they're systemic. This not only reduces the frequency and duration of exposure windows that result from deficient controls, but it also reduces the waste associated with "fixing" the same problems over and over.

Lastly, more mature organizations should be able to more confidently and effectively take advantage of business/mission opportunities that introduce additional risk. Combined with fewer wasted resources, this will help the risk management function more directly contribute to the organization's bottom line.

Although the common approach of measuring lagging maturity indicators (the existence of policies, processes, and technology) provide some utility, we believe the risk management industry (including regulators) should focus more strongly on leading indicators. Until that happens, forward-thinking organizations have the opportunity to take the lead by recognizing and improving on those factors that reflect greater maturity. Meaningful business advantages should result for these organizations.

What's Next?

We undertook this survey and analysis with three objectives, to:

- Establish a current state metric of risk management maturity using a model and methods that provide fresh insights into what's working, and what's not. These insights should help organizations focus on specific weak points, and can help industry stakeholders (e.g., regulators) refine how they evaluate risk management programs.
- Given an understanding of the current state, begin the process of measuring and reporting on how risk management is evolving over time. With this in mind, this survey and report will be repeated annually.
- Provide a means for organizations to meaningfully gauge themselves against an industry benchmark.

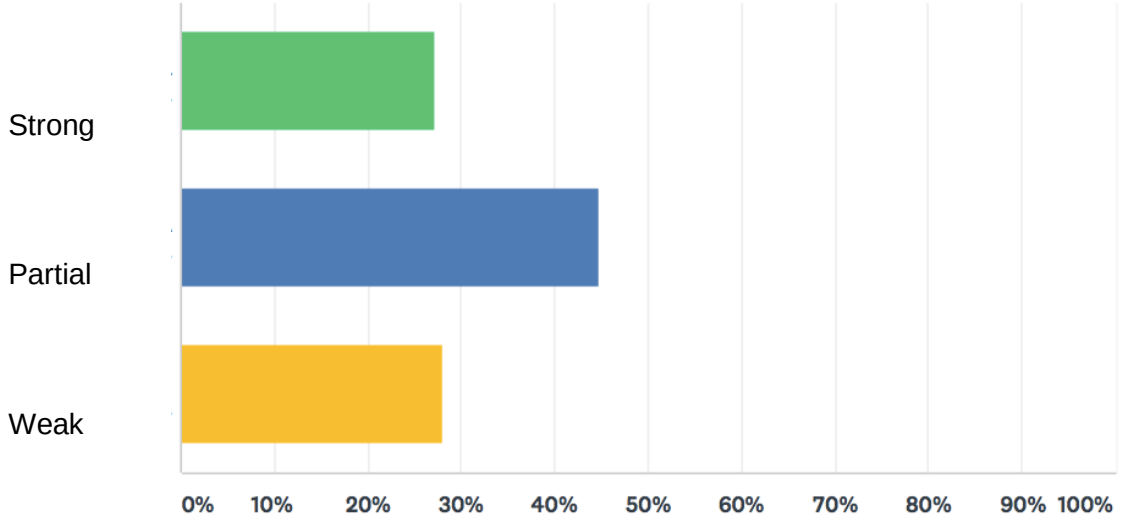
Given what we learned in this study, we also now recognize that these results can be used to generate focused resources and guidance on each element in the model. For example, because most organizations scored so poorly on the Motivation factor in the model, the FAIR Institute will develop guidance in the form of white papers and/or blog posts that help organizations mature in that dimension. Stay tuned for updates on these resources.

The FAIR Institute also will continue to refine the model, the survey, and its analysis methods to provide even greater intelligence from each year's study. To maximize our improvement efforts, feedback is a necessary and welcome element. Please direct your ideas and suggestions to Luke Bader, Director of Membership and Programs, at lbader@fairinstitute.org.

Summary Data

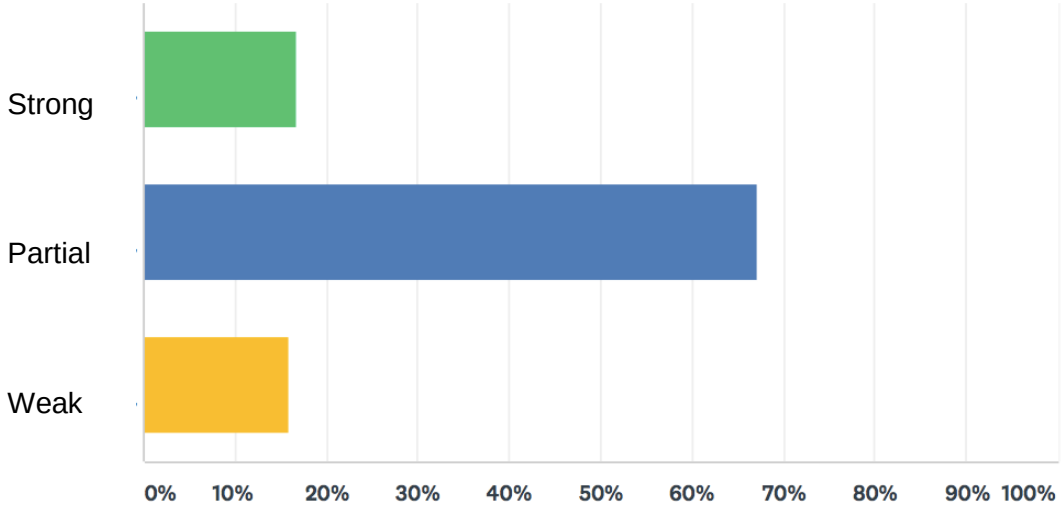
NOTE: The first six questions of the survey primarily focused on understanding the respondents, the organizations they represented, and the overall approach to risk management being used in those organizations. As a result, they did not play a role in the actual maturity analysis. These more demographically-focused data points are covered in the "About the Survey Respondents" section at the end of this report.

Question 7 — Risk Terminology: Select which description best fits your organization's current usage of risk terminology: strong, partial or weak. Do personnel involved in risk management operate from consistent and/or clear risk-related terminology?



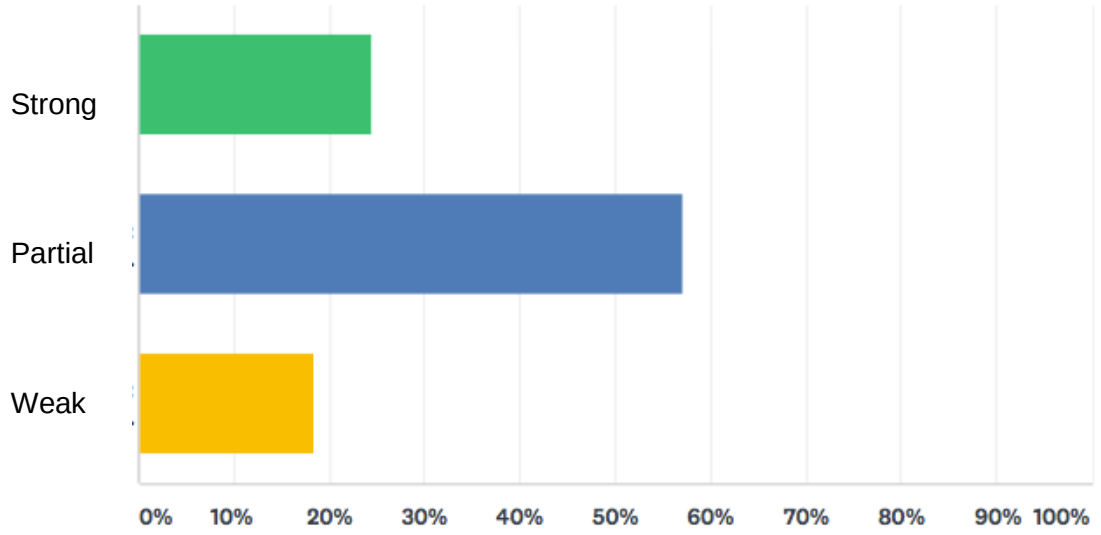
Answer Choices	Responses	
Strong: A standard set of risk-related terms has been formally defined or adopted. Personnel within the risk management organization (including cyber risk, audit, privacy, compliance, technology, operational risk, etc.) understand and consistently apply these terms. Inconsistent usage is corrected.	27.19%	31
Partial: A standard set of risk-related terms has been formally defined or adopted, but usage is inconsistent.	44.74%	51
Weak: No standard set of risk-related terms has been defined or adopted. If you ask six people in the risk management organization to define foundational risk-related terms or provide examples of what those terms represent, you will likely receive different answers.	28.07%	32

Question 8 — Asset Visibility: Which of the following best describes your organization's visibility into its system and information assets? The purpose is to gauge the organization's ability to know where its assets are and what their value is.



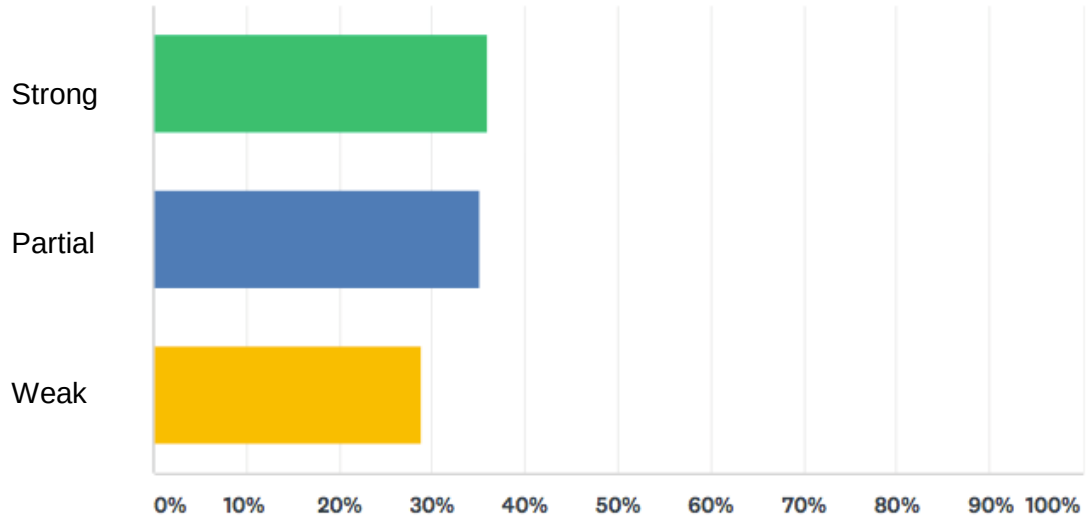
Answer Choices	Responses	
Strong: An inventory of systems, applications, and significant information repositories exists and is kept up-to-date through well-defined and consistently practiced procedures. An audit of the inventory would be unlikely to find that more than 5% of the entries are inaccurate. Also, the value/liability characteristics of assets (e.g., classification) is included in the inventory.	16.81%	19
Partial: An inventory of systems, applications, and significant information repositories exists but is not consistently maintained. Processes for maintaining the inventory are immature or are exercised unreliably. Audits of the inventory regularly find more than 5% of the entries are inaccurate.	67.26%	76
Weak: An inventory of systems, applications, and significant information repositories does not exist or is severely out of date (i.e., cannot be relied on to support decision-making). Processes for maintaining the inventory either do not exist or are not practiced.	15.93%	18

Question 9 — 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, patching)?



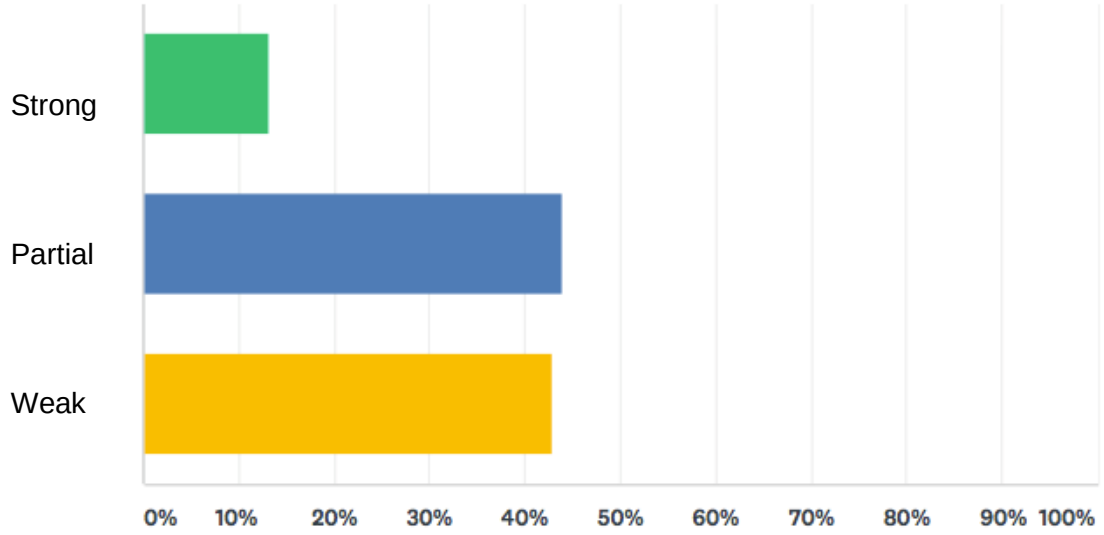
Answer Choices	Responses	
Strong: The frequency of controls testing (e.g., authentication, access privilege, configuration, and patch conditions, etc.,) is driven by the value/liability characteristics of the assets, the level of threat they face, and the anticipated degree of change surrounding those assets. In other words, controls testing is more frequent for assets that are of higher value, face a more active threat landscape, and that undergo more frequent changes.	24.56%	28
Partial: Authentication, access privilege, configuration and patch conditions, etc., are tested on a regular basis but the testing regimen is not risk-based. As a result, some key systems, applications, or points of attack may not get tested at all or testing occurs infrequently.	57.02%	65
Weak: Authentication, access privilege, configuration, and patch conditions, etc., are infrequently tested and not well known.	18.42%	21

Question 10 — Threat Visibility: Which of the following best describes your organization's visibility into the threat landscape?



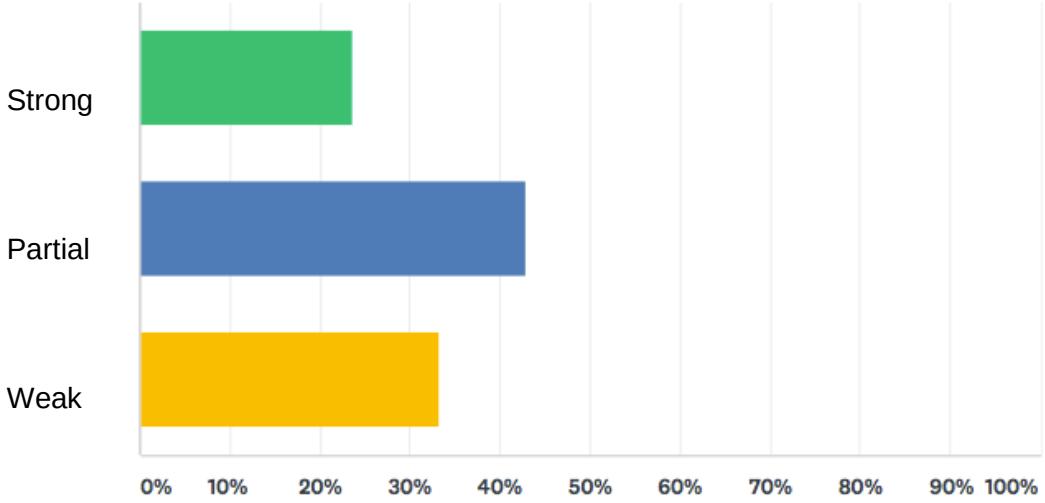
Answer Choices	Responses	
Strong: Threat intelligence is a specialization within the information security group (or has been outsourced) and is capable of providing organization-specific information regarding changes in the threat landscape (e.g., increases in the frequency or sophistication of attacks experienced by the organization). Threat data for key assets and points of attack are closely monitored.	35.96	41
Partial: Threat intelligence is received from internal resources and/or external sources (e.g., ISAC organizations) that provide information regarding changes and trends in the general threat landscape (e.g., the existence of a new zero-day exploit) as well as the organization's industry.	35.09	40
Weak: Threat intelligence is acquired in an informal or ad hoc manner (e.g., blogs, mailing lists, etc.) and is highly generalized in nature (i.e., the data is not specific to the organization's industry or the organization itself).	28.95	33

Question 11 — Model Quality: Which of the following best describes the models used to evaluate and measure risk? The purpose is to understand how well the organization is able to apply asset, control, and threat information to prioritize risk management efforts.



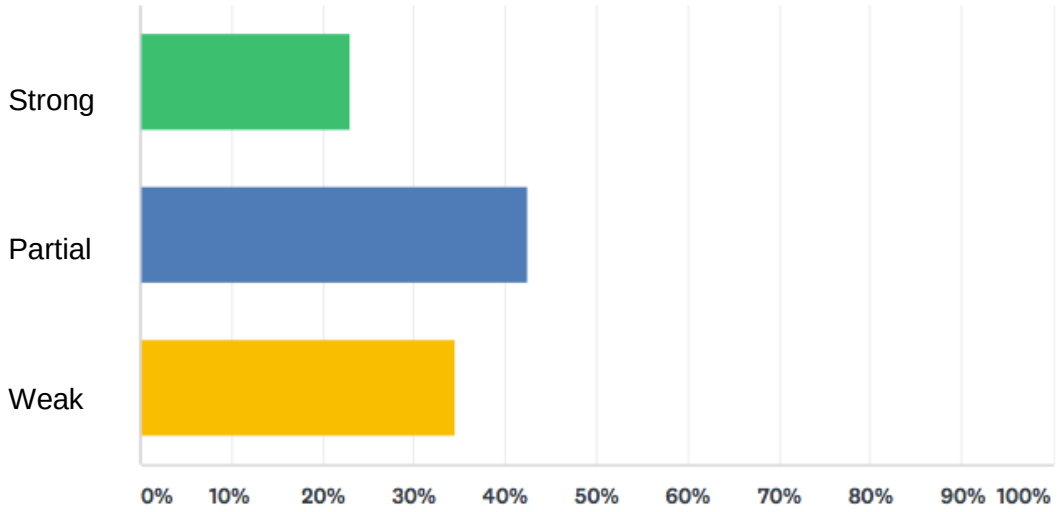
Answer Choices	Responses	
Strong: Risk analyses consistently leverage a well-defined and publicly vetted analytic framework (i.e., is not checklist- based). An example would be the Open FAIR model.	13.15%	15
Partial: Risk analyses rely on models that have been developed internally or by a third party, and that have not undergone independent validation.	43.86%	50
Weak: Analysis relies primarily on the intuition (mental models) of subject matter experts. Little or no documentation or validation of the underlying assumptions takes place.	42.98%	49

Question 12 — Analyst Skills: Which of the following best describes the training and skill sets of personnel who analyze and measure risk? The purpose is to understand the organization's ability to properly scope, analyze, and measure risk factors.



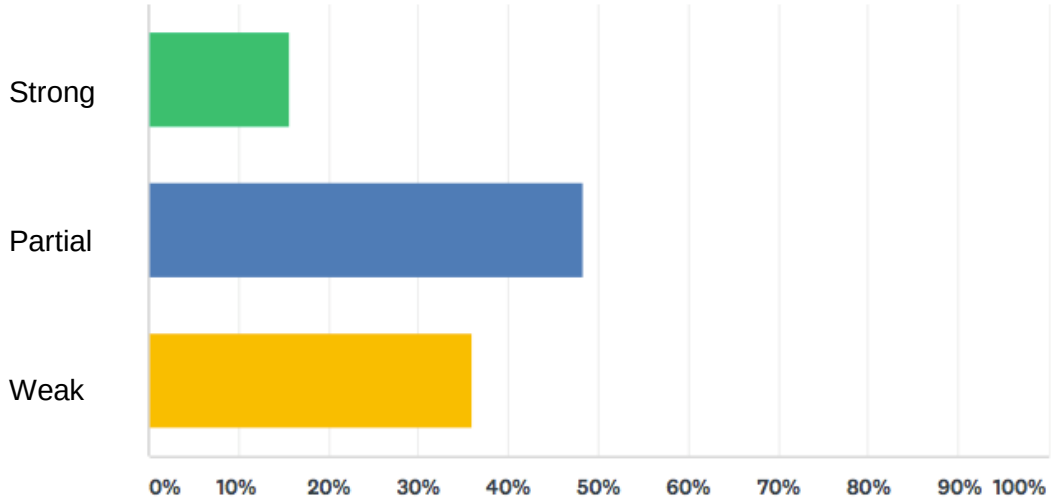
Answer Choices	Responses	
Strong: The organization has (or contracts to) personnel who are dedicated to performing risk analysis. Analysts have expertise in quantitative risk measurement concepts and principles and have been specifically trained in the process of scoping scenarios and making calibrated estimates.	23.68%	27
Partial: Analysts are not dedicated specifically to performing risk analysis. They have experience in performing qualitative information security risk analyses, but may have limited expertise in formal analysis methods, probability principles, etc.	42.98%	49
Weak: Analysts are experienced in information security and/or technology but are inexperienced in formal risk analysis methods.	33.33%	38

Question 13 — Execution Visibility: Which of the following best describes your organization's visibility into why conditions exist that are not compliant with organization policy? The purpose is to understand the organization's ability to identify why non-compliant conditions occur so that root causes can be treated.



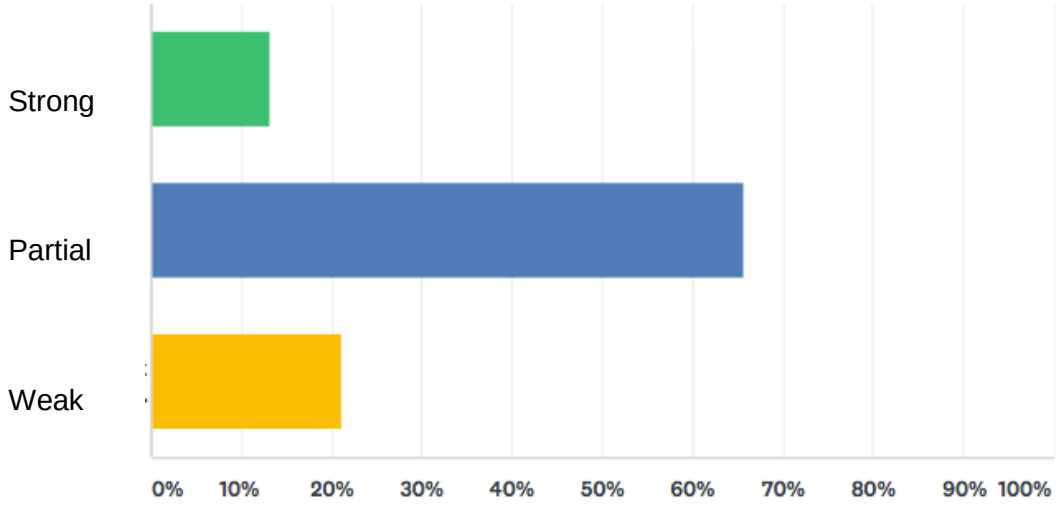
Answer Choices	Responses	
Strong: Root cause analysis of non-compliant conditions is performed at least 75% of the time when non-compliant conditions are discovered. The population of root-cause analyses are evaluated as a portfolio to discover systemic sources of non-compliance.	23.01%	26
Partial: Root cause analysis is periodically performed (at least half the time) when non-compliant conditions are discovered, but no attempt is made to perform a portfolio review of these analyses in an attempt to discover systemic problems within the organization.	42.48%	48
Weak: Root cause analysis is not performed (or is performed less than half the time) when noncompliant conditions are discovered.	34.51%	39

Question 14 — Decision-making Visibility: Which of the following best describes your organization's visibility into risk decision-making? The purpose is to understand an organization's ability to ensure that risk decisions are being made by at the appropriate level of authority and that risk ratings/values are accurate.



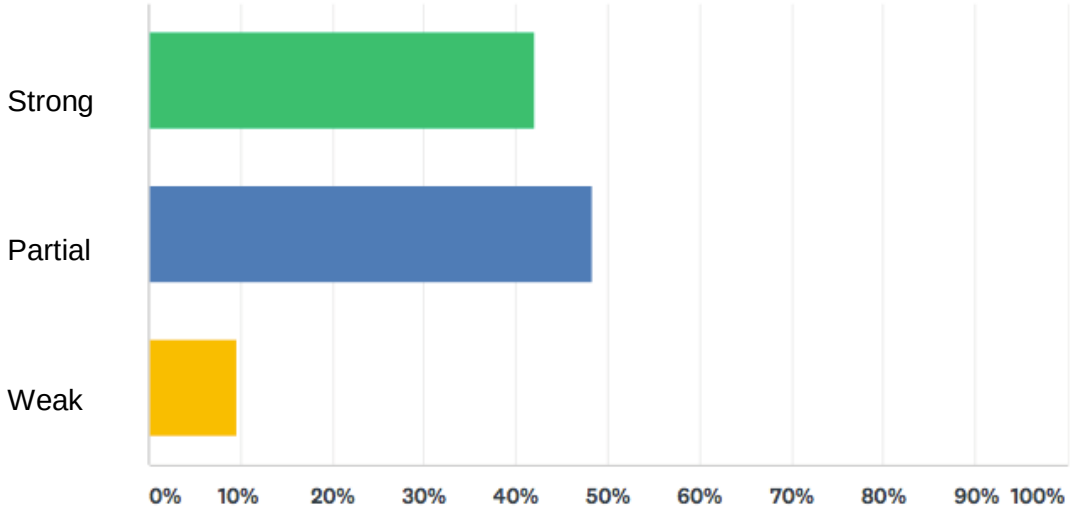
Answer Choices	Responses	
Strong: At least once per year the organization performs both of the following: 1) reviews risk management decisions to ensure that they are being made at the appropriate level of leadership, and 2) has an independent review performed of risk ratings/values to validate that the risk information being provided to decision-makers is accurate.	15.79%	18
Partial: At least once per year the organization performs one of the following: 1) reviews decisions (e.g., policy exception requests, policy/standards development, etc.) to ensure they are being made by the appropriate personnel, or 2) has an independent review performed of risk ratings/values that were used to validate that the risk information being provided to decision-makers is accurate.	48.25%	55
Weak: The organization does not review risk management decision-making to ensure that decisions are being made by the appropriate personnel or that risk measurements were accurate.	35.96%	41

Question 15 — Risk Reporting Quality: Which of the following best describes your organization's risk reporting? The purpose is to understand how easily decision-makers are able to understand and apply risk information when making risk decisions.



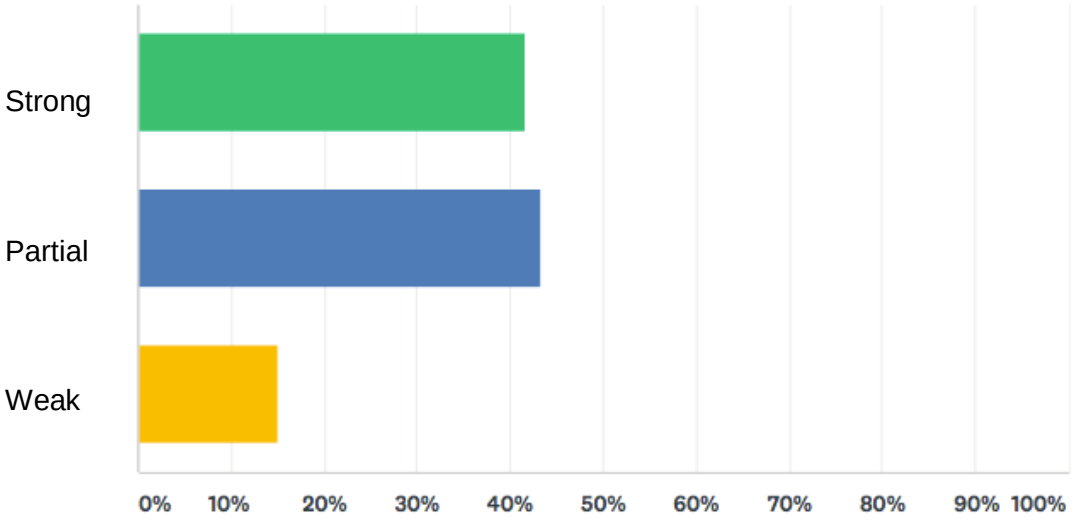
Answer Choices	Responses	
Strong: Risk reporting includes quantitative statements of risk so that decision-makers can effectively compare and prioritize information security concerns against other organization concerns (e.g., operational needs, growth opportunities, and other forms of risk).	13.16%	15
Partial: Risk reporting is worded for the intended audience but is primarily qualitative in nature.	65.79%	75
Weak: Risk reporting to operational and executive management contains a significant amount of technical information and jargon.	21.05%	24

Question 16 — 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.)? The purpose is to understand the degree to which the organization's risk management decisions (e.g., policies, etc.) are influenced by external requirements.



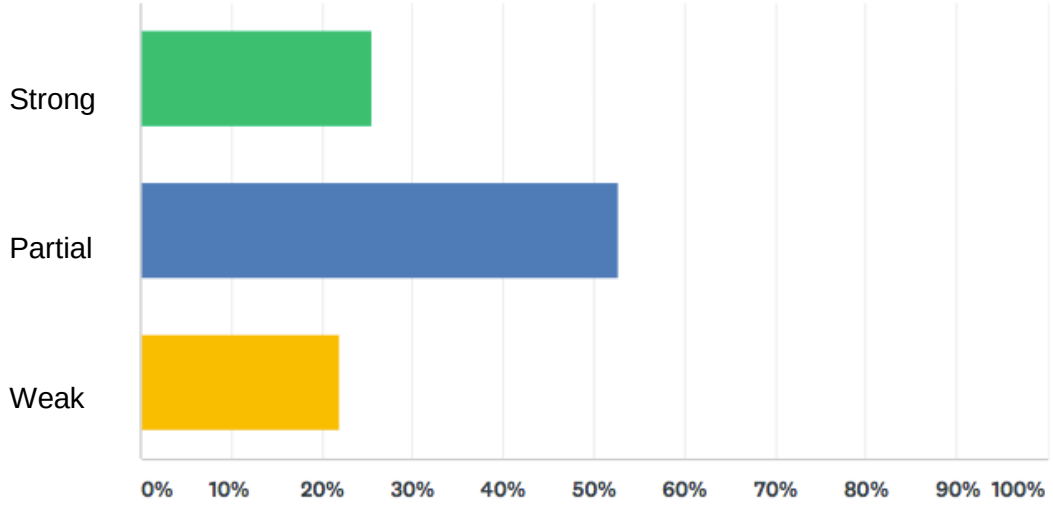
Answer Choices	Responses	
Strong: The organization is subject to external expectations regarding information security, and enforcement is consistent and potentially impactful.	42.11%	48
Partial: The organization is subject to external expectations regarding information security, but enforcement is either inconsistent or not significantly impactful.	48.25%	55
Weak: The organization is not subject to external expectations regarding information security, or external expectations are not enforced.	9.65%	11

Question 17 — Organizational Resources: Which of the following best describes the organization's capacity for funding information security? The purpose is to understand whether the organization's risk management efforts are constrained by the availability of financial resources. Note that this question is focused on the availability of business resources (e.g., capital) rather than resources within the information security team.



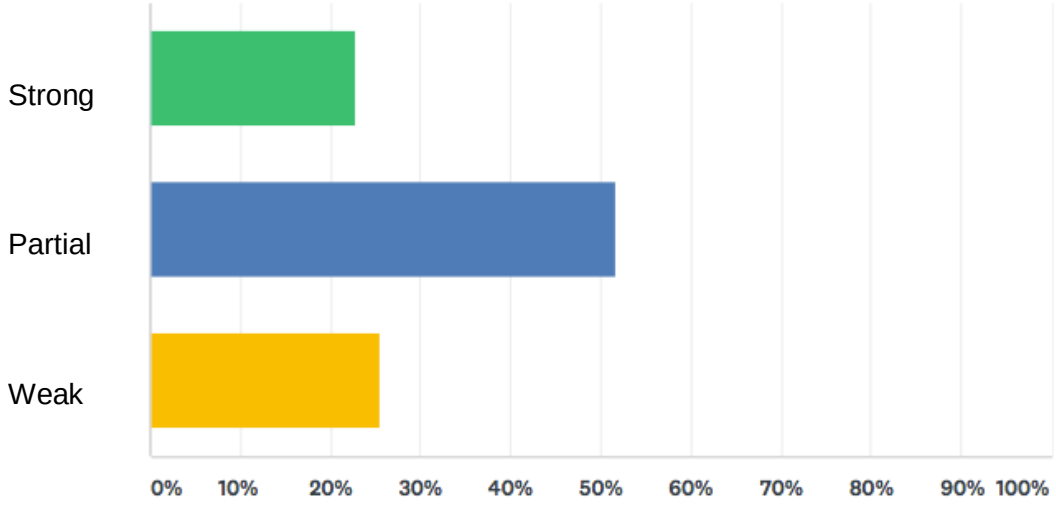
Answer Choices	Responses	
Strong: The organization has sufficient resources to support more advanced information security capabilities (as evidenced by the existence of advanced technologies and/or more advanced capabilities like in-house forensics staff, a dedicated threat intelligence team, dedicated red-team personnel, etc.)	41.59%	47
Partial: The organization has limited resources but is able to provide sufficient resources to meet its basic information security needs.	43.36%	49
Weak: The organization has severely limited resources which affect its ability to fund basic information security needs	15.04%	17

Question 18 — Awareness: Which of the following best describes how aware personnel is of the organization's expectations (e.g., policies and standards) regarding their information security related responsibilities?



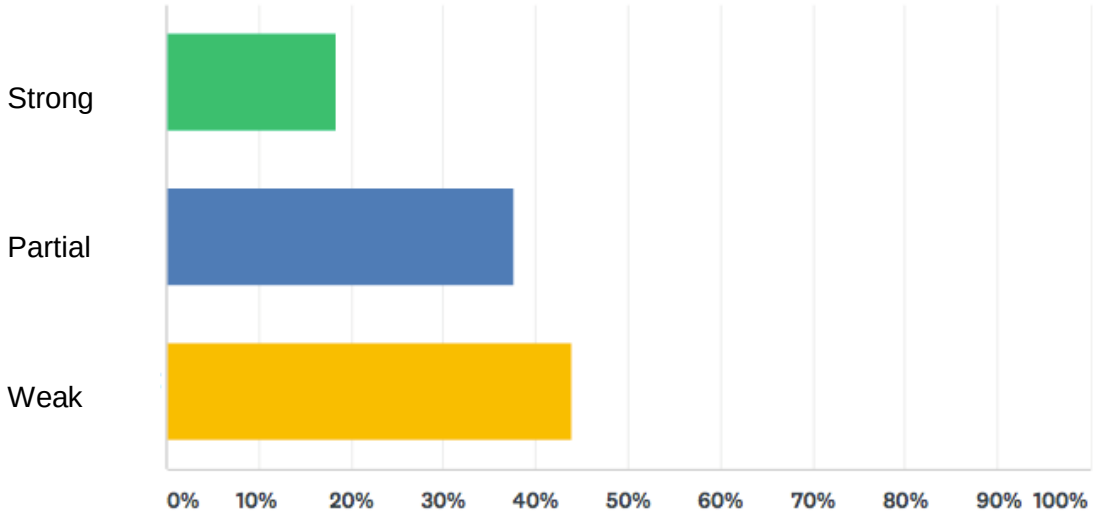
Answer Choices	Responses	
Strong: The organization has documented and published policies, standards and processes and these documents are kept up-to-date. Personnel are required to understand the specific risk management expectations for their job responsibilities (e.g., developers understand secure software standards, system, and network administrators understand configuration, change management, and architecture standards, etc.) and their understanding of these expectations is evaluated once per year.	25.44%	29
Partial: The organization has documented and published policies, standards and processes and these documents are mostly kept up-to-date. Personnel are required to read and acknowledge their understanding of the organization's general risk management expectations.	52.63%	60
Weak: The organization has little or no documented and published policies, standards, and processes, or these documents are out-of-date. There are no active processes in place to make personnel aware of these expectations. Most personnel have little or no understanding of the organization's risk management expectations.	21.93%	25

Question 19 — Capabilities: Which of the following best describes personnel skills and capabilities? The purpose is to understand whether personnel have the training and experience necessary to carry out their risk management responsibilities?



Answer Choices	Responses	
Strong: Updated training in relevant risk management areas of expertise is required on an annual basis to help ensure that personnel keep abreast of changes in the risk landscape, technology, and/or processes. Funding for this effort is not subject to budget cuts.	22.81%	26
Partial: Updated risk-related training is typically provided but not required. Funding for training is subject to budget cuts.	51.75%	59
Weak: Updated training is not provided or is inconsistently funded.	25.44%	29

Question 20 — Motivation: Which of the following best describes how personnel are incentivized to meet the organization's risk management expectations (e.g., policies and standards)? The purpose is to understand the degree to which information security objectives or requirements may be treated as a lower priority than other business imperatives (e.g., budget objectives, deadlines, etc.)?



Answer Choices	Responses	
Strong: Key cyber risk objectives are formally defined within the performance expectations and compensation/bonus plans for senior business leadership. Failing to meet cyber risk objectives consistently results in the same (or more severe) consequences as failing to meet revenue goals, exceeding deadlines, exceeding budget limits, etc.	18.42%	21
Partial: Cyber risk objectives are included in the performance expectations/reviews for key personnel with risk management responsibilities (e.g., system admins, software developers, etc.). Failing to meet cyber risk objectives can result in the same (or more severe) consequences as failing to meet deadlines, exceeding budget limits, etc.	37.72%	43
Weak: Failing to meet cyber risk expectations/objectives rarely results in meaningful consequences.	43.86%	50

Important Considerations

Despite the 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.

About the Survey Respondents

The survey was completed by 114 respondents. Respondents identified themselves as being a CISO (24%), Cyber Security Specialist (20%), Risk Officer (16%), Risk Analyst (11%), and C-Level Executive (6%). Another 22% chose "Other" to describe their role.

A wide variety of industries and organization types were represented. Banking/Finance led the pack (27%), followed closely by Technology (23%), Healthcare (8%), Insurance (7%), Manufacturing (5%), Retail (4%), Telecommunication (3%), and Transport/Logistics (3%). Another 19% of respondents chose "Other" to describe their industry.

Organizations of various sizes responded to the survey. Organizations at the smaller and larger end of the scale made up over half of total responses: less than $500M in annual revenue (31%), or greater than $20B in revenue (25%). In between were organizations having annual revenue between $500M and $1 (11%), $1B to $5B (16%), and $5B to $20B (18%).

Risk Management Frameworks currently being used by respondent organizations were: NIST/CSF (41%), ISO27001 (41%), and COSO (24%).

Risk Analysis Models currently being used by respondents were: FAIR (15%) and NIST 800-30 (27%). Another 54% reported that their organizations were discussing adopting FAIR, versus 25% that were considering adopting NIST 800-30.

Contributors

Jack Jones, Chairman, The FAIR Institute, is one of the foremost authorities in the field of information risk management. He has worked in technology for over 30 years, the past 28 years in information security and risk management. He has a decade of experience as a Chief Information Security Officer (CISO) with three different companies, including a Fortune 100 financial services company. He is the author and creator of the Factor Analysis of Information Risk (FAIR) framework. He writes about that system in his book Measuring and Managing Information Risk: A FAIR Approach, which was inducted into the Cyber Security Canon in 2016, as a must-read in the profession.

Luke Bader, Director of Membership and Programs, The FAIR Institute, manages member relations, events, and strategic initiatives for the Institute. For any inquires about the survey, membership, or partnership opportunities, please contact Luke at lbader@fairinstitute.org.

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 www.fairinstitute.org.