Risk Assessment & Mitigation for Core Security Capabilities

Marc Dupuis
School of Science, Technology, Engineering & Mathematics, University of Washington
Bothell, USA
https://orcid.org/0000-0002-5303-2511

Karen Renaud
Computer and Information Science, University of Strathclyde Glasgow, UK
University of South Africa, South Africa
https://orcid.org/0000-0002-7187-6531

***Abstract*—Efforts to assure the cybersecurity of an organization's information and systems rely on industry metrics to monitor their current state of play. These, when monitored over time, could also help organizations to determine whether they are improving their stance or lagging behind. We reviewed the literature on metrics and consulted 12 cybersecurity professionals, working in industry, to take a snapshot of the status quo of metric and framework usage. We report on what our respondents told us and conclude by explaining that, although they were aware of metrics, many only used minimal metrics, and few used any existing frameworks. This was primarily due to resource and other business constraints. It seems that we have to encourage and engender more metric usage, and that an automated approach, with an associated dashboard to support reporting, would be the best way to help organizations to benefit from this helpful mechanism.**

***Index Terms*—risk metrics, cybersecurity, management, mitigation, assessment**

I. Introduction

Organizations are highly inter-connected socio-technical systems, which require the formulation and implementation of effective cybersecurity strategies to ensure that everything is properly secured. Cyber attacks or employee errors might deter an organization's work processes and cause data to be leaked. Organizations have to acticipate and prepare for such eventualities. To do this, they might employ risk mitigation strategies to enhance resilience in the face of probable attacks. However, it is not always easy to determine whether said risk mitigation strategies are indeed effective.

Cybersecurity metrics are commonly used to quantify organizational risk mitigation strategies to assess the organization's state of play with respect to resistance and resilience. According to National Institute of Standards and Technology (NIST), security is measured to assess overall system security, to avoid subjectivity, to provide a systematic and speedy means to obtain meaningful measurements, provide understanding and gain insights into the composition of security mechanisms.

The purpose of this investigation was to assist organizations in determining their level of security readiness and resilience via security metrics. Identifying the most applicable security metrics for an organization is important in the successful implementation of an information security governance program [1]. The more effectively an organization can measure what it is attempting to manage from a cybersecurity standpoint, the more successful it will be in achieving its objectives [2]. We reviewed research articles, industry and standards bodies' proposals in this respect, in order to provide some actionable suggestions for developing and using metrics. Here, we present a synopsis of our research findings, followed by recommendations and suggestions for businesses in this respect.

II. Risk Assessment & Mitigation

A. Stakeholders

The NIST special report 800-55 [3] identifies main organizational executive cybersecurity stakeholders that each have particular roles and responsibilities within a security program, with the three most relevant being: agency head (chief executive officer - CEO), chief information officer (CIO), and chief information security officer (CISO) [3]. Of these stakeholders, the two primarily involved in the implementation and development of a security measurement program are the CIO and CISO, where the CIO focuses on using measures in reporting and communication and the CISO focuses on leading development and integrating measurement into policies, procedures, and practices [3]. Muiyuro aligns each of these roles with a guiding question when considering organizational cybersecurity measurement programs [4]:

CEO: "*Is the cybersecurity strategy aligned with our business strategy?*"

CIO: Chief Information Officer: "*How efficient have our tools been in protecting against cyber-attacks?*"

CISO: Chief Information Security Officer: "*Do we have real-time insights into critical incidents, threats, and vulnerabilities impacting our environment?*"

B. Risk Assessment

NIST defines risk as, "*a measure of the extent to which an entity is threatened by a potential circumstance or event*," and it is typically a function of adverse impacts that would arise if the circumstance or event occurs, as well as the likelihood of occurrence [5]. Such risk assessments facilitate decision-making at three tiers of risk management hierarchy:

2159-1245/24/$31.00 ©2024 IEEE
DOI 10.1109/eCrime66200.2024.00010

(1) organizational level, (2) mission/business process level, and (3) information system level. This includes framing, responding to, and monitoring risk. These processes inform decision-makers and support risk responses by identifying relevant threats, vulnerabilities, and impacts that may occur given potential for threats exploiting vulnerabilities [5]. A typical assessment methodology includes an explicit risk model (defining key terms and assessable risk factors/relationships), an assessment approach (specifying the range of values risk factors can assume), and an analysis approach (describing how combinations of risk factors are identified to ensure adequate coverage of problem space) [5].

NIST special report 800-37 outlines a generalized Risk Management Framework (RMF) and guidelines for establishing a repeatable risk management process in 7-steps (prepare, categorize, select, implement, assess, authorize, and monitor). The purpose this process serves in relation to an organization's metrics is to establish accountability for the controls implemented within and inherited by information systems, while connecting risk management processes at the organizational process levels to the information system level [6].

Breier and Hudec propose a formal risk analysis model that aims to provide an objective discrete-scale evaluation of implemented security controls. This is accomplished by mapping metrics to control objectives, assessing security clauses to security attributes and designing relevant mappings between them, and supporting the model with security statistics to make a detailed analysis [7].

C. Risk Mitigation

Human behavior can be split into three categories: (1) business process and environment, (2) cognitive factors, and (3) personal factors — each with corresponding opportunities for human-caused vulnerabilities [8]. These vulnerabilities caused by a human factor can be identified as human decision points (HDP), which Noureddine defines as, "certain tasks performed by human participants" [8]. Hueca asserts that truly effective security solutions require an embedded culture of cybersecurity awareness, as users are the first line of defense for an organization's cybersecurity posture. As such, Hueca recommends that organizations establish an awareness program/campaign that focuses on informing users of cyber risks in an effort to influence user behavior, and assisting the user in making the right decisions when interacting with computers and the internet. A well-designed awareness program should foster organizational learning and support the overall organizational mission from a security perspective [9]. NIST special report 800-50 provides guidelines for building and maintaining a comprehensive awareness and training program. Users are the largest audience in any organization and have the largest impact on reducing unintentional errors and IT vulnerabilities, meaning that by establishing an effective program that produces relevant security skills and competencies, vulnerabilities caused by human error can be greatly reduced [10].

III. Background Literature on Security Metrics

We have reviewed existing documents relating to cybersecurity metrics. In this section, we present our findings and highlight the key concepts.

A. Terminology

In the information assurance and cybersecurity space, it is imperative that we are able to determine our risk posture at any point in time. Effective decision-making requires as complete of an understanding of risk and how it is managed as is possible given various constraints an organization faces (e.g., budgetary, legal). This is the essence of risk management—making effective decisions with the information available.

Generally speaking, we use metrics to measure something. If we are interested in understanding a measure of cybersecurity awareness within an organization, we would identify appropriate metrics for that measure [11], [12].

The challenge for an organization lies is identifying the measures that best characterize their cybersecurity posture and the metrics that identify where they are at with respect to those measures. Identifying the threats an organization faces is relatively easy in comparison [12], whereas effectively detailing a given state for specific measures is incredibly challenging.

Thus, a *metric* may be viewed as data that informs a *measure*. A *measure* is a specific information assurance and cybersecurity concept identified as important to the risk management priorities of a particular organization. Effective risk management requires careful selection of measures appropriate for the organization.

Conceptually, this is similar to how data may become information when appropriate context is provided [13]. To take this analogy one step further, knowledge may emerge from this information if its use is thoughtful, analytical, and deliberate. The same is true for effective risk management. We must identify appropriate measures and the metrics that determine the state of those measures.

In Figure 1, the relationship between these concepts is delineated. In particular, we see that the risk management goals and objectives of the organization are derived to support the organizational mission. These derivations continue down the pyramid, while the results of these concepts feed into the higher order concept noted above it. Similar to a physical pyramid, if the foundation that is developed is weak or poorly constructed, the ability to maintain structural integrity becomes flawed and subject to destruction. Thus, in order for the organization to achieve its mission, it is critical that careful consideration is given for each subsequent level of the risk metric hierarchy as one moves down from top to bottom.

B. Characteristics of Effective Metrics

After determining metric categories, the next step is to assess the characteristics of effective metrics. There are specific characteristics identified to be consistent among effective metrics, and any new metric should satisfy these characteristics.

Fig. 1. Risk Metric Hierarchy

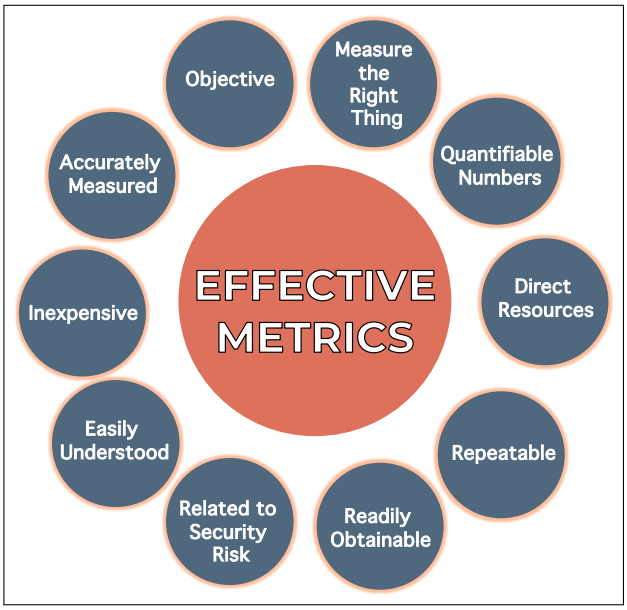

Fig. 2. Characteristics of Effective Metrics

Tagarev [14] states that metrics should be expressed as a cardinal number or percentage, cheap to collect, consecutively measured, expressed with at least one unit of measurement, and contextually specific. These characteristics allow metrics to be quantifiably compared and usable in different contexts. In addition to characteristics of effective metrics, Tagarev also includes characteristics of poor metrics that should be avoided. Poor metrics are subjectively and inconsistently measured, meaning the individual who measures the metric will affect the value, difficult to collect, not actual indicators, and not designed for stakeholders. Poor metrics may also be easy to collect but difficult to apply [14]. An example of this would be the number of spam emails blocked; you could easily count the number of spam emails received but the value of this action is hard to apply. Would an increase in spam emails mean you are better at tracking them or that you are getting increasingly being targeted? No one knows what the normal number of spam emails to be expected is, so this particular metric could well be misleading and needlessly reassuring.

NIST SP 800-55 provides criteria for effective cybersecurity metrics (see Figure 2). NIST states metrics should yield quantifiable numbers, metrics should indicate where to direct resources, processes should be repeatable, and the data supporting metrics needs to be readily obtainable [15]. Saydjari echoes the same information about what makes effective metrics. Saydjari claims good metrics should measure the right thing, be quantifiably measured, capable of being measured accurately, repeatable so the results are independent of the analyst, inexpensive to execute, validated against the truth, and refereed independently [16]. Effective metrics should also be easy to understand, measurable, and objective. Metrics should directly relate to a security risk [17].

C. Categorizing Metrics

Categorizing metrics is one of the first steps in identifying which metrics to use. Many researchers have attempted to create a taxonomy for cybersecurity metrics, but none have succeeded in creating an industry-accepted vocabulary [18]. This section will list four attempts at defining cybersecurity metric categories.

The first set of categories is from NIST SP 800-55 Revision 1, which splits metrics up into three categories: (1) implementation, (2) effectiveness/efficiency, and (3) impact. Implementation metrics show the progress in implementing information security programs; these may be metrics that track the percentage of systems in compliance with a new cybersecurity measure [3], for example. Metrics in this category should strive for 100% compliance. Effectiveness/efficiency metrics are used to track the implementation, operating efficiency, and the result of program-level processes and system-level security controls [3]. Effectiveness/efficiency metrics track the robustness and timeliness of updates and results. These metrics are useful for leading decisions within an organization and monitoring which security controls are working as intended. Impact metrics describe how an organization's information security is affecting the mission goals. These metrics are inherently organization-specific because they relate to the mission goals. Impact metrics may be used to quantify cost savings, public image and public trust, and other information security impacts [3].

The second set of categories is from Bhol, who set out to create a taxonomy for security metrics by creating five metric categories: (1) vulnerabilities, (2) protection mechanism, (3) threats, (4) users, and (5) encounter outcomes. The first category, vulnerabilities, includes the metrics which measure how vulnerable, susceptible, or weak the security is [19]. This category is further broken up into the attack surface, which is the exposure to the outside world; malware infection, which is attacks from malicious programs; wrongly configured SSL certificates; which certifies the owner and authenticates transactions, and patching cadence, which is related to the

security patches pushed and the time taken to update. The protection mechanism category includes the metrics which determine how protected resources are [19]. This section is characterized further by four parameters: preparedness level, penetration resistance, blacklisting, and intrusion attempts. The preparedness level tracks the number of fully patched and updated network devices. Penetration resistance metrics include those related to tracking the difficulty to penetrate a system [19]. Blacklisting tracks the number of entities blocked and the time taken to ban them. Intrusion attempts track the number and severity of intrusion attempts. Measurement metrics relate to the risk the current landscape poses [19]. This category is further split up into four subcategories: attack power, botnets, malware spreading, and risk scenario. Users relate to the individuals who interact with the system and the metrics that track their level of awareness [19]. Possible user metrics include the strength of passwords, phishing susceptibility, and the number of super users. Finally, encounter metrics record the results of an attack and the protection after it occurred. An example of an encounter metric would be the mean time to detect and the mean time to respond [19].

The third set of categories is from Savola, who introduces another three levels for metrics: business level; information security management; and ITC products, systems, and services. Business level metrics are determined by the business goals and provide a direction for security [20]. These metrics can be created by defining the business goals and extrapolating measurements from there. Information security management helps assist decision-making and provides values to prove security measures are working [20]. Lastly, metrics for ITC products, systems, and services show the dependability and trust of these systems [20].

The last set of categories is from Saydjari, who introduces four more security metric categories. The first is criteria-compliance, which is one of the oldest types of metrics. Criteria compliance verifies that their systems follow the set limitations [16].

The next category is intrusion-detection-based metrics, which evaluate the performance of intrusion detection systems [16]. These metrics are usually easily accessible from the detection systems and may be harder to apply in some cases because it may not be clear what the data means. The next category is policy-based metrics, which are similar to intrusion detection but instead, look at numbers like unauthorized login attempts and files accessed [16]. The last category is incident-based metrics, which evaluate the actual attacks and the damage they induce [16]. These metrics are limited by the organization's ability to see the attacks.

D. Existing Frameworks

Existing frameworks can provide guidance needed to fine-tune your security practices. This section presents four existing frameworks and covers areas from creating metrics for the first time or amalgamating existing metrics for more nuanced measurement.

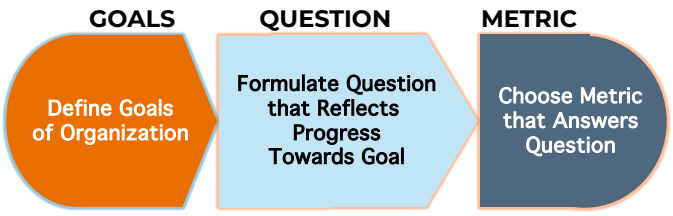

Fig. 3. Goal—Question—Metric framework

Papazov presents three common frameworks for selecting metrics, the first framework presented being the GQM (Goal-Question-Metric) framework [21] (see Figure 3). This framework is good for choosing metrics to drive management decisions and is often closely related to the organization's goals [22]. The basic structure of the GQM framework is to describe the goals of the organization based on questions related to each of the organization's goals, and then choose metrics that answer the questions posed. The benefit of this framework is that the metrics created are immediately applicable and answer an organizational question. One downside of GQM is that the metrics are often project-related, so the big picture of the organization is often lost in the metrics [22].

The second framework Papazov presents is the PRAGMATIC framework [23], which stands for: **P**redictive, **R**elevant, **A**ctionable, **G**enuine, **M**eaningful, **A**ccurate, **T**imely, **I**ndependent, and **C**ostly (see Figure 4, Table I). A predictive metric should reflect the future as well as the current state so that preventative measures can be taken. A relevant metric has relevance to the security posture of the organization. For a metric to be actionable, it should help decision-makers take corrective action. A genuine metric should return the same values no matter who conducts the measurement. A meaningful metric should be usable by any individual, not only those with cybersecurity knowledge. Accurate metrics should be precise in their measurements. For a metric to be timely it should have a rapid feedback loop allowing action to be taken quickly. Independent metrics should be resistant to manipulation, meaning people cannot change the values to be more favorable or lean a certain way. Finally, metrics should be cheap enough to collect to make the data worthwhile. This framework works to answer more general organizational questions [22].

The third framework presented by Papazov is Educause [24],
which uses the acronym, SMART. SMART stands for: specific, measurable, attainable, repeatable, and time-dependent. These characteristics ensure that metrics can be compared and collected in a way that the measures are independent of the individual collecting the values. The metrics will also be narrow enough that the measures will be easily defined and collection will be easier. The SMART and PRAGMATIC frameworks are closely related. However, the PRAGMATIC framework is much more rigid, as compared to the SMART framework. Any metric that is PRAGMATIC should also be

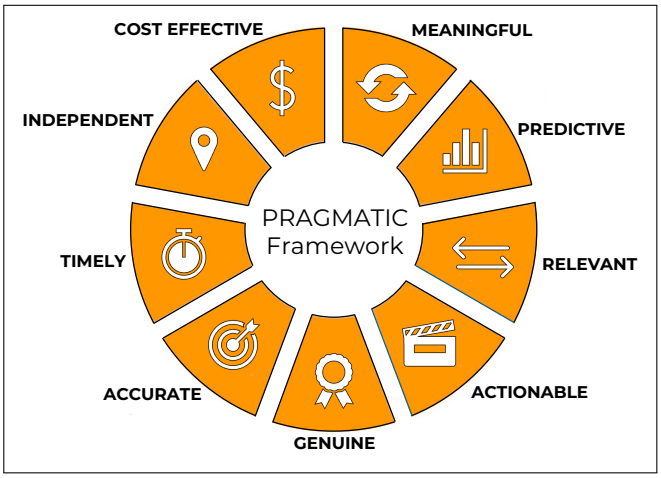

Fig. 4. PRAGMATIC Framework Diagram

TABLE I
PRAGMATIC FRAMEWORK

Predictive	Repeatable Results; Sufficient for a Metric to be Objective
Relevant	Directly Associated with Security Posture
Actionable	Allows or Action Compels Management to Act
Genuine	Conveys Useful Information to Management
Meaningful	Repeatable Results Sufficient for a Metric to be Objective
Accurate	Reflect Reality Sufficiently Accurate
Timely	Allows for a Quick Action Response
Independent	Resistant to Manipulation Reflects Current Status of Objectives
Cost Effective	Return on Investment

SMART, but the inverse is not always true [22].

Another framework often used is the Common Vulnerability Scoring System (CVSS) [25]. The CVSS is commonly used for assessing the severity of individual cybersecurity vulnerabilities. The CVSS has three metric groups: (1) Base, (2) Temporal, and (3) Environmental. The base metrics represent how critical the vulnerability is. The temporal metrics represent how urgent the vulnerability is. The environmental metrics represent how critical the vulnerability is for a specific environment [11]. Each provides a value from 0 to 10 rating the severity of the vulnerability. The downside to this framework is that it requires an in-depth analysis of processes and systems. The required data to calculate the base metric score is the attack vector, attack complexity, privileges required, user interaction, scope, confidentiality impact, integrity impact, and availability impact [26]. All of these require time and energy to produce.

The last is a NIST-developed framework for improving critical infrastructure cybersecurity. This framework outlines ways for organizations to approach cybersecurity including the effect on physical, cyber, and user regions [27]. As with many cybersecurity concepts, this framework will have to be adapted to each organization as they all have unique risks, tolerances, and infrastructures. This framework helps organizations describe their current cybersecurity posture, their target state, assess and prioritize areas for improvement, track progress to the goal state, and communicate to internal and external stakeholders about cybersecurity risk [27]. This framework is split up into 3 sections: a core, implementation tiers, and a profile. The framework core consists of a list of desired activities and outcomes and presents industry standards and guidelines [27]. The implementation tiers rank organizations based on their cybersecurity maturity and processes compared to the practices presented in the framework. Lastly, the framework profile walks organizations through assessing their business needs against selected framework categories to create a profile that enables them to better prioritize to reach their target profile [27].

E. "Usable" Metrics

Usability, in this context, refers to the ease with which a particular metric can be deployed. It is clear that no one set of metrics will perfectly match every organization's security needs. Each organization needs to determine what areas they need to monitor and protect. There are, however, general metrics that work in many situations for many organizations; these metrics constitute a good foundation for quantifying risk.

In the user susceptibility category, a couple of metrics reveal how much users might contribute to an unsecured system. Rating user password strength by time to crack provides insight into where improvement might be made. Users should have passwords that take longer than 30 days to crack. The organization should also keep track of how many users have root access [17]. A good rule is to give users the least amount of privilege needed for their job, the fewer individuals that are super users, the less opportunity for breaches there are.

Risk assessments and vulnerability scans are also essential in determining if an organization is prepared. These scans reveal which components and systems are the most susceptible and conducting these often means organizations know where their weak spots are. Research conducted by Christina Richmond found that the organizations with the highest level of security readiness conducted risk assessments and vulnerability scans almost continuously compared to the less-secure organizations. Richmond also found that higher security organizations were more likely to make changes based on their risk assessments [28]. The frequency of risk assessments and vulnerability scans appears to be a major factor in an organization's level of security.

A few recommended ways to convert risk assessments and vulnerability scans into more usable metrics were proposed by the participants in the cybersecurity shared research program. The proposed metrics are the coverage of vulnerability scanning and coverage of penetration testing. The coverage of vulnerability scanning is the percentage of IT assets covered by automated vulnerability scans and the coverage of penetration is the percent of IT assets subjected to penetration testing [29]. Converting risk assessments and vulnerability scans into a baseline of 0% to 100% makes the measure easy to understand with a clear path to improvement.

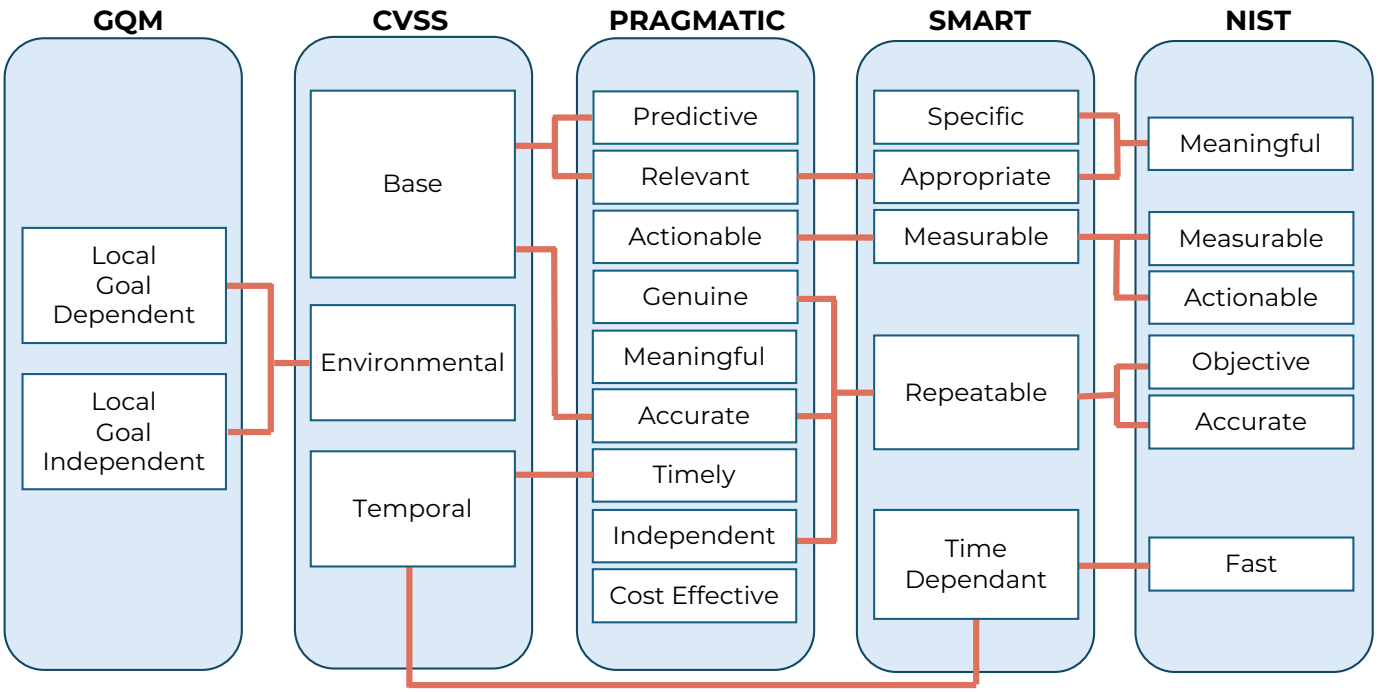

Fig. 5. Framework Metrics Visualised

The mean time to detect and mean time to respond are similar metrics that both provide good measures for revealing how well organizations can find an attack and respond to one. The mean time to detect is the average time taken for an organization to identify a cyber incident. The mean time to respond is the average time from detection to resolution [30]. The cybersecurity shared research program suggests tracking the average time between the start and detection of a cyber incident [29]. Kinser states a capable organization should detect an attack within minutes and be able to resolve an attack within hours or days, depending on the severity of the attack. The average breach to resolution time is 7 days [30].

Building on the mean time to detect and respond is a new metric proposed by Aziz called the "mean blind spot". The mean blind spot is the average amount of time between the recovery from a cyber incident and the occurrence of another incident [31]. This metric was designed to track the time when an organization is most vulnerable, the time when their resources are held up dealing with the previous incident.

Fig. 6. Usable Metrics

F. Current Issues

Current issues for cybersecurity measurement programs used by organizations today can be divided into two main problem areas: the metrics themselves and the reporting methods used to gain insight from them. Considering a definition where the accuracy of a metric is dependent on the accuracy of the measures it's comprised of, factors affecting the accuracy of a measure include imprecise definitions with vague terminology, inconsistent methods, lack of context, and a changing meaning of metrics/measures over time due to the dynamic nature of cyber technology [32]. There is also the question of determining how to combine particular measures into a metric because it can be difficult to quantify what weight each measure should be given. Measures are also often collected without a proper evaluation of their usefulness on the basis that more information is better than less, causing a waste of time/resources and generating misleading results if dependencies aren't clear [32]. From the viewpoint of those collecting these measures, collecting useless measures or ones that only reflect positive results can cause those involved in collection to feel ineffective [32].

Papazov highlights the benefits of automatic processes for metric collection: unscheduled calculations, reduced workload

for employees, and near-continuous feedback loops. However, heterogeneous devices making up networks increase the complexity of an automatic solution – making automation difficult [22]. Papazov also discusses an issue coined 'metrics gaps' by Brotby and Hinson, where the more mature any metric program is, the easier it is to assume the program is 'good enough' and to miss issues in the collection program [22]. Krautsevich identifies a lack of widely-accepted and unambiguous definition that defines what it means for one system to be more secure than another. There is no universal formal model for all metrics which can be used for rigorous analysis, and the diversity of metrics is caused by an inability to prove that a metric really measures security. Creators of security metrics define what 'more secure' is by means of metrics, but this does not prove that the metric really indicates a change in security [33].

For cybersecurity stakeholders, Muiyuro describes that telling the story of the state of their organization's security is complicated due to a lack of common language, difficulty in obtaining required data, organizational differences, lack of performance baselines, and legacy thinking that is focused on tracking what is being done instead of how well it is being done [4]. Many organizations struggle with fully understanding what they need to report and to whom and that existing reports lack actionable information, such as how the legacy approach does not provide the insight necessary to make risk-based decisions. Existing cybersecurity technologies don't have integrated dashboard/reporting capabilities, and many executive cyber reports are manually compiled, infrequent, and hard to produce [4]. For cybersecurity stakeholders, telling the story of the state of their organization's security is complicated due to a lack of common language, difficulty in obtaining required data, organizational differences, lack of performance baselines, and legacy thinking that is focused on tracking what is being done instead of how well it is being done [4]. Scala and Goethals define descriptive analytics as using data from the past and present to understand current and historical performance, and have identified a disconnect in semantics where the cybersecurity field is attempting to utilize descriptive analytics to make an assessment or prediction about future events, reflecting an attitude of legacy thinking [34].

IV. Consultation

To gain insights into industry use of metrics, frameworks and general risk mitigation strategies, we surveyed a number of respondents who were involved with cyber security in a range of capacities. The primary focus of our inquiry was directed toward those in management (e.g., Chief Information Security Officers, Chief Information Officers) or operations (e.g., cyber analysts, cyber ops). We posed the questions enumerated in Appendix A. The mapping of the questions to the aspects we have reviewed so far are shown in Table II.

A. Participants

Fifteen respondents completed the open-ended survey with follow-up interviews to seek clarification and elaboration, as appropriate. Each was given a $50 gift voucher from the online platform of their choice, in their own country. All respondents were directly involved in cyber operations and/or decision making. This study included participants from the United Kingdom (3) and the United States (12). The following roles were identified by these participants: Chief Information Security Officer (6); Cyber Operations (3); Chief Information Officer (3); Cyber Analyst (2), and VP of Engineering (1). Experience in their current positions ranged from less than one year to over 27 years. Organizational size varied from small (less than 100 employees), to medium (100 to 5,000 employees), and finally to large (50,001 to 100,000 employees). Participants represented both public and private sector organizations.

TABLE II
Question numbers (Appendix A) mapped to aspects being assessed

Survey Question(s)	Assesses
1-5	Participant Background
6, 7	Risk Management Measures
8,9,12	How Metrics are Chosen
10,11	Framework Usage
13	Difference between Metrics and Measures
14-17	How Metrics are Collected
18	Benchmarks Used
19	Categorization of Metrics
20,21	Changes in Metric Usage over Time
22	Influence of Business Context on Metrics
23-27	Reporting Systems

B. Ethics

This study was approved by the Institutional Review Board of the University of Washington. All participants participated in this study of their own free will and were notified that they would be able to cease their participation at any time and for any reason.

C. Analysis

The two authors went through the respondents' free text responses and consolidated them to provide a summary of answers to each question, as reported below.

V. Summary of Respondents' Responses

A. Risk Management Measures

We asked respondents which cybersecurity metrics and measures they thought were the best indicators of an organization's level of security and readiness. Table III shows how many people mentioned each of the metrics.

B. How Metrics are Chosen

A number of participants wanted metrics to be 'easy to read, easy to interpret (also for non-technical personnel), and give value to the business.' This respondent wanted the metrics to facilitate assessment of ongoing cyber risks to their business. More than one participant talked about the need for metrics to be strategic, actionable, accurate and correlated. Yet another refers to the need for metric measurement outcomes to be

TABLE III
NUMBER OF TIMES METRICS WERE MENTIONED BY RESPONDENTS

Metric	Number
Monitoring Attacks on Employees e.g., Phishing	3
Monitoring Employee Behaviors e.g., Password Choice	3
Monitoring Employee Awareness	7
Incident Response Planning	4
Incident Management	8
Patching Cadence	7
Technical Measures e.g., Firewall, Antivirus	9
Configuration	2
Compliance with Standards	8
Access Management	2
Penetration Testing	6
Monitoring Security Progress	25
Organizational Engagement e.g., budget and implementation of processes	6
Total:	90

reported to a metric monitoring group who are able to monitor the metrics in terms of efficacy and need for tailoring. Yet, as one participant points out, metrics should be proactive and not reactive. Otherwise, the organization could get trapped into a bullwhip cycle [35].

One participant highlights the 'unknown unknowns' which exacerbate the metric choice difficulty. Another points to the need for metrics to be chosen in collaboration with decision makers who hold the purse strings in organizations. Another also highlights the need for metrics to be chosen based on business priorities and risk.

C. Framework Usage

Eight of the respondents did not use a metrics framework. Those who did report using one mentioned: Cyber Care, NIST, ISO amd MITRE. When asked why they chose this framework, they provide a range of justifications. The Cyber Care user said: "*We are early adopters of this approach and testing new ideas. We do not want to implement something because everyone else does it. We chose this because the metrics are directly related to what we process during board and team meetings. Nothing in there should be something that only technical staff understand.*"

Of those who used NIST, the first said it had been chosen by their predecessor. Their own preference would have been to hire penetration testers rather than use a variety of metrics to assess their security. The other said that NIST was well known across the industry and its use allowed them to communicate with other companies about risk using the same language. The one who used ISO simply said "*business alignment*."

D. Difference Between Metrics and Measures

One respondent said: "*Metric = data; Measure = process in place to reduce or avoid risk*." Another said: "*Not sure I fully understand the definitions. Sounds like Metrics is numbers based and measure is qualitative*." Two said the two terms were used interchangeably in their organizations.

E. How Metrics are Collected

One participant said that the way metrics are collected is dependent on the budget that is available to facilitate this. Another said the collection might be linked to the outcome of a penetration test, while a third pointed to automate collection.

Three used Security Information and Event Management (SEIM) systems to collect all their metrics. Another two also referred to an automated tools but did not name any specific ones. Another did not say how to collect metrics, but rather pointed to the worst way i.e., spreadsheets.

Another said: "*I prefer good GRC tools from which I can record the individual metrics/measurements from control assurance work, assessments, audits and reviews and then get a good aggregate of how they look from multiple perspectives.*"

F. Benchmarks Used

Respondents referred to guidance from the UK's National Cyber Security Centre, ISO, and Microsoft Secure Score. Another used frequency of events, out of band events, failures and outages. Yet another did not see the need for any specific benchmark. Yet another admitted that this was challenging in their organization.

G. Categorization of Metrics

Here there were a variety of responses from four respondents:

- Mapping of metric to risk.
- Responsiveness of organization to particular kinds of incidents.
- The most impactful (show stopper or impacting revenue and/or customers).
- The CVSS/OWASP/CWE vulnerabilities are used to categorise metrics.

The rest of the participants did not respond to this question.

H. Changes in Metric Usage Over Time

One respondent points to "Project management, change advisory board, information governance board and Information management board." Other respondents also talk about the need for management to be involved in deciding on metric changes.

Another points to an ongoing monitoring which supports reviewing of metrics on a continuous basis, which suggests that changes are decided by those who are responsible for security in the organization. Another three also do things this way.

I. Influence of Business Context on Metrics

The respondents were asked whether the metrics currently being used by their organization includes relevant business context. Five agreed that this was the case. One of these said: "*Security is hard and VERY technical in nature and would be impossible for regulars MBA business folks to understand.*"

J. Reporting Systems

Half of the respondents used a security dashboard to aid reporting within the organization. When asked about the ways their organization's reporting processes enable accurate and timely decision-making, a number of responses were provided:

- "*There is a reporting button integrated into Outlook and a single point of contact, the Helpdesk.*"
- "*all the executives and main tech have an mobile application as part of the reporting.*"
- "*They ... are to interested in day to day operations to be bothered with what the security reporting is saying or lack of security reporting is saying.*"
- "*There are set quarterly meetings for discussion/decision-making on strategic and long-term stuff. Ad-hoc meetings are available with the risk governance committee for immediate issues.*"
- "*As it's all templated out in ServiceNow- it's very easy to see that the same results are being produced time over time and there's also audit records to ensure that nothing was changed or altered by say another admin.*"

VI. Dashboard Concept

Given these findings and the associated discussion, we developed a "Risk Metrics Dashboard" Concept. The goal was to clearly delineate between risk management goals, measures used to assess achievement of those goals, and the metrics that gauge success for each of these measures. Ultimately, risk management goals are developed to support the mission of the organization. Everything else that follows is either directly or indirectly in support of that mission. Thus, the risk management goals, associated measures for those goals, and the metrics that gauge the state of those measures will vary considerably. Flexibility in risk management focused dashboards is needed, including how they communicate risk and what should and should not be measured. The interactive version of the Risk Metric Dashboard Concept may be found at the following URL: https://tinyurl.com/dashboardconcept. A non-interactive version may be found in the Appendix.

VII. Lessons Learned

The final question we asked our respondents provide expert views into the use of metrics.

One points to the resourcing constraints, highlighting the difference between what is possible, and what is feasible in this domain: *"Consider the implications of resourcing in terms of time and budget, smaller organisations do not tend to have dedicated security teams or completely unified threat management systems. Consider also the level of assurance its possible to provide in light of the restricted resource in comparison to a large bank with a dedicated security team and large security budget."*

Another respondent expresses much the same sentiments: *"It takes a long time to build a system to provide answers. We have gone through many iterations, but we are not buying loads of systems based on features"*

A third argues for a revealed vulnerability approach: *"I think the best approach is to hire hackers to show you the unknown unknowns and then from there do what they recommend for mitigation/detection, and repeat at least yearly."*

A final perceptive comment from a respondent, which circles back to the first two respondents' responses: *"Cyber security needs to be addressed proactively and metrics and measure are largely lagging indicators. Focusing on where breeches most commonly come from first (email), will help keep companies secure."*

In conclusion, there is awareness of a range of metrics, although not of many frameworks, amongst the respondents. However, what does come through clearly is that the gold standard is often infeasible, either in terms of budgetary or other constraints. We have to be realistic in our endeavors, helping people to collect metrics but not expecting everyone to be able to cover all bases.

References

[1] V. Anu, "Information security governance metrics: a survey and taxonomy," *Information Security Journal: A Global Perspective*, vol. 31, p. 466–478, July 2022. 10.1080/19393555.2021.1922786.

[2] S. Gupta Bhol, J. Mohanty, and P. Kumar Pattnaik, "Taxonomy of cyber security metrics to measure strength of cyber security," *Materials Today: Proceedings*, vol. 80, p. 2274–2279, 2023. 10.1016/j.matpr.2021.06.228.

[3] E. Chew, M. Swanson, K. M. Stine, N. Bartol, A. Brown, and W. Robinson, "Performance measurement guide for information security," Tech. Rep. NIST SP 800-55r1, National Institute of Standards and Technology, 2008. 10.6028/NIST.SP.800-55r1.

[4] A. Muiyuro, "Cybersecurity metric: Supporting accurate and timely decision-making," Nov 2018. https://www.alliances.global/wp-content/uploads/2019/05/Cybersecurity-Metrics-Dashboard-CIO-Alliance-Copy.pdf.

[5] Joint Task Force Transformation Initiative, "Guide for conducting risk assessments," Tech. Rep. NIST SP 800-30r1, National Institute of Standards and Technology, 2012. 10.6028/NIST.SP.800-30r1.

[6] Joint Task Force Transformation Initiative, "Risk management framework for information systems and organizations:: a system life cycle approach for security and privacy," Tech. Rep. NIST SP 800-37r2, National Institute of Standards and Technology, Dec 2018. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf, 10.6028/NIST.SP.800-37r2.

[7] J. Breier and L. Hudec, "Towards a security evaluation model based on security metrics," in *Proceedings of the 13th International Conference on Computer Systems and Technologies - CompSysTech '12* (B. Rachev and A. Smrikarov, eds.), p. 87, ACM Press, 2012. 10.1145/2383276.2383291.

[8] M. Noureddine, K. Keefe, W. H. Sanders, and M. Bashir, "Quantitative security metrics with human in the loop," in *Proceedings of the 2015 Symposium and Bootcamp on the Science of Security* (D. Nicol, ed.), p. 1–2, ACM, Apr 2015. 10.1145/2746194.2746215.

[9] A. Hueca, B. Manley, and L. Rogers, "Building a cybersecurity awareness program," 2020. https://resources.sei.cmu.edu/asset_files/Handbook/2021_002_001_651800.pdf.

[10] M. Wilson and J. Hash, "Building an information technology security awareness and training program," Tech. Rep. NIST SP 800-50, National Institute of Standards and Technology, 2003. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf, note=10.6028/NIST.SP.800-50.

[11] Y. Cheng, J. Deng, J. Li, S. A. DeLoach, A. Singhal, and X. Ou, "Metrics of security," in *Cyber Defense and Situational Awareness* (A. Kott, C. Wang, and R. F. Erbacher, eds.), vol. 62, p. 263–295, Springer International Publishing, 2014. 10.1007/978-3-319-11391-3_13.

[12] M. Mateski, C. M. Trevino, C. K. Veitch, J. Michalski, J. M. Harris, S. Maruoka, and J. Frye, "Cyber threat metrics," *Sandia National Laboratories*, p. 30, 2012.

[13] C. Shannon, "The lattice theory of information," *Transactions of the IRE professional Group on Information Theory*, vol. 1, no. 1, p. 105–107, 1953. 10.1109/TIT.1953.1188572.

[14] N. Tagarev, "A critical look at the metrics for measuring the effectiveness of a cybersecurity system," in *Proceedings of International Conference on Application of Information and Communication Technology and Statistics in Economy and Education (ICAICTSEE); Sofia* (D. G. Velev, ed.), p. 9, 2019.

[15] M. Swanson, N. Bartol, J. Sabato, J. Hash, and L. Graffo, "Security metrics guide for information technology systems," Tech. Rep. NIST SP 800-55, National Institute of Standards and Technology, 2003. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55.pdf 10.6028/NIST.SP.800-55.

[16] O. S. Saydjari, "Is risk a good security metric?," in *Proceedings of the 2nd ACM workshop on Quality of protection - QoP '06* (G. Karjoth and F. Massacci, eds.), p. 59, ACM Press, 2006. 10.1145/1179494.1179508.

[17] W. Boyer and M. McQueen, "Ideal based cyber security technical metrics for control systems," in *Critical Information Infrastructures Security* (J. Lopez and B. M. Hämmerli, eds.), vol. 5141, p. 246–260, Springer Berlin Heidelberg, 2007. 10.1007/978-3-540-89173-4_21.

[18] National Institute of Standards and Technology, "Measurements for information security," Sep 2020. https://www.nist.gov/cybersecurity/measurements-information-security.

[19] S. Gupta Bhol, J. Mohanty, and P. Kumar Pattnaik, "Taxonomy of cyber security metrics to measure strength of cyber security," *Materials Today: Proceedings*, p. S2214785321046009, Jun 2021. 10.1016/j.matpr.2021.06.228.

[20] R. Savola, "Towards a security metrics taxonomy for the information and communication technology industry," in *International Conference on Software Engineering Advances (ICSEA 2007)* (B. Werner, ed.), p. 60–60, IEEE, 2007. 10.1109/ICSEA.2007.79.

[21] V. R. Caldiera, G. Basili, and H. D. Rombach, "The goal question metric approach," *Encyclopedia of Software Engineering*, pp. 528–532, 1994.

[22] Y. V. Papazov, "Cybersecurity metrics," Tech. Rep. STO-EN-IST-170, NATO, n.d.

[23] A. Jaquith, *Security metrics: replacing fear, uncertainty, and doubt*. Pearson Education, 2007.

[24] Educause, "Effective security metrics," 2017. https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/toolkits/effective-security-metrics.

[25] A. Kott and C. Arnold, "Towards approaches to continuous assessment of cyber risk in security of computer networks," 2015. 10.48550/arXiv.1512.07937.

[26] FiRST, "Common vulnerability scoring system version 3.1 specification document revision 1," n.d. https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf.

[27] National Institute of Standards and Technology, "Framework for improving critical infrastructure cybersecurity, version 1.1," Apr 2018. http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf, 10.6028/NIST.CSWP.04162018.

[28] C. Richmond, "Cybersecurity readiness: How "at risk" is your organization?," 2017. White Paper https://www.business.att.com/content/dam/attbusiness/reports/cs-cybersecurity-readiness-whitepaper.pdf.

[29] Participants in the Cybersecurity Shared Research Program, "Library of cyber resilience metrics," Nov 2017. https://www.betaalvereniging.nl/wp-content/uploads/Library-of-Cyber-Resilience-Metrics-Shared-Research-Program-Cybersecurity.pdf.

[30] S. Kinser, P. de Graaf, M. Stein, F. Hughey, R. Roller, D. Voss, and A. Salmoiraghi, "Scoring trust across hybrid-space: A quantitative framework designed to calculate cybersecurity ratings, measures, and metrics to inform a trust score," tech. rep., The MITRE Corporation Hanscom AFB United States, 2020.

[31] B. Aziz, A. Malik, and J. Jung, "Check your blind spots: A new cyber-security metric for measuring incident response readiness," in *RISK 2016: Risk Assessment and Risk-Driven Quality Assurance*, (Graz, Austria, October 18), pp. 19–33, 2016. 10.1007/978-3-319-57858-3_3.

[32] P. E. Black, K. Scarfone, and M. Souppaya, "Cyber security metrics and measures," in *Wiley Handbook of Science and Technology for Homeland Security*, p. hhs440, John Wiley & Sons, Inc., Nov 2008. 10.1002/9780470087923.hhs440.

[33] L. Krautsevich, F. Martinelli, and A. Yautsiukhin, "Formal approach to security metrics.: what does "more secure" mean for you?," in *Proceedings of the Fourth European Conference on Software Architecture Companion Volume - ECSA '10* (C. E. Cuesta, ed.), p. 162, ACM Press, 2010. 10.1145/1842752.1842787.

[34] N. M. Scala and P. L. Goethals, "A model for and inventory of cybersecurity values: Metrics and best practices," in *Handbook of Military and Defense Operations Research* (N. M. Scala and J. P. Howard, eds.), p. 305–330, Chapman and Hall/CRC, 1 ed., Feb 2020. 10.1201/9780429467219.

[35] J. Dejonckheere, S. M. Disney, M. R. Lambrecht, and D. R. Towill, "Measuring and avoiding the bullwhip effect: A control theoretic approach," *European Journal of Operational Research*, vol. 147, no. 3, pp. 567–590, 2003. 10.1016/S0377-2217(02)00369-7.

APPENDIX

A. Questions for Study Participants

1) In which country do you currently reside?
2) What job category best describes the type of work you do in cybersecurity?
3) How many years have you been involved in your current role?
4) What is the size of the organization you work for?
5) What industry classification best describes your organization?
6) What steps do you take to assess your organization's level of security and readiness?
7) What cybersecurity metrics and measures do you feel are the best indicator of an organization's level of security and readiness? (No ordering implied)
8) What factors led you to choose the metrics you previously mentioned?
9) What characteristics do you look for in metrics to make sure they are actionable and/or useful to the organization?
10) Does your organization utilize a cybersecurity metrics framework?
11) Why did you choose this framework over others?
12) Are there any cybersecurity metrics and measures you feel should NOT be measured? Please explain
13) Does your organization differentiate metrics from measures? How?
14) What is your preferred way of collecting cybersecurity metrics and/or measures?
15) Are these collection processes easily implemented and repeatable? Please explain.
16) What are the sources or types of sources your organization uses to collect cybersecurity metrics and/or measures?
17) Are cybersecurity metric and/or measure collection processes manual or automated? Please explain.
18) What benchmarks do you use to gauge your metrics?
19) Do you categorize your metrics in any particular way?
20) Have the metrics and measures you use changed over time? How so?
21) What processes are in place to support changes in used metrics over time?
22) Do the metrics currently being used by your organization include relevant business context?
23) What reporting systems do your organization have in place to provide insight on cybersecurity posture to decision makers?
24) Does your organization utilize a cybersecurity dashboard to aid reporting?
25) In what ways do your organization's reporting processes enable accurate and timely decision-making?
26) How do you present cybersecurity information to all your stakeholders?
27) Is the information communicated to stakeholders actionable? Please explain.
28) Is there anything you would like to add?

B. Risk Metric Dashboard Concept

(Starts on next page.)

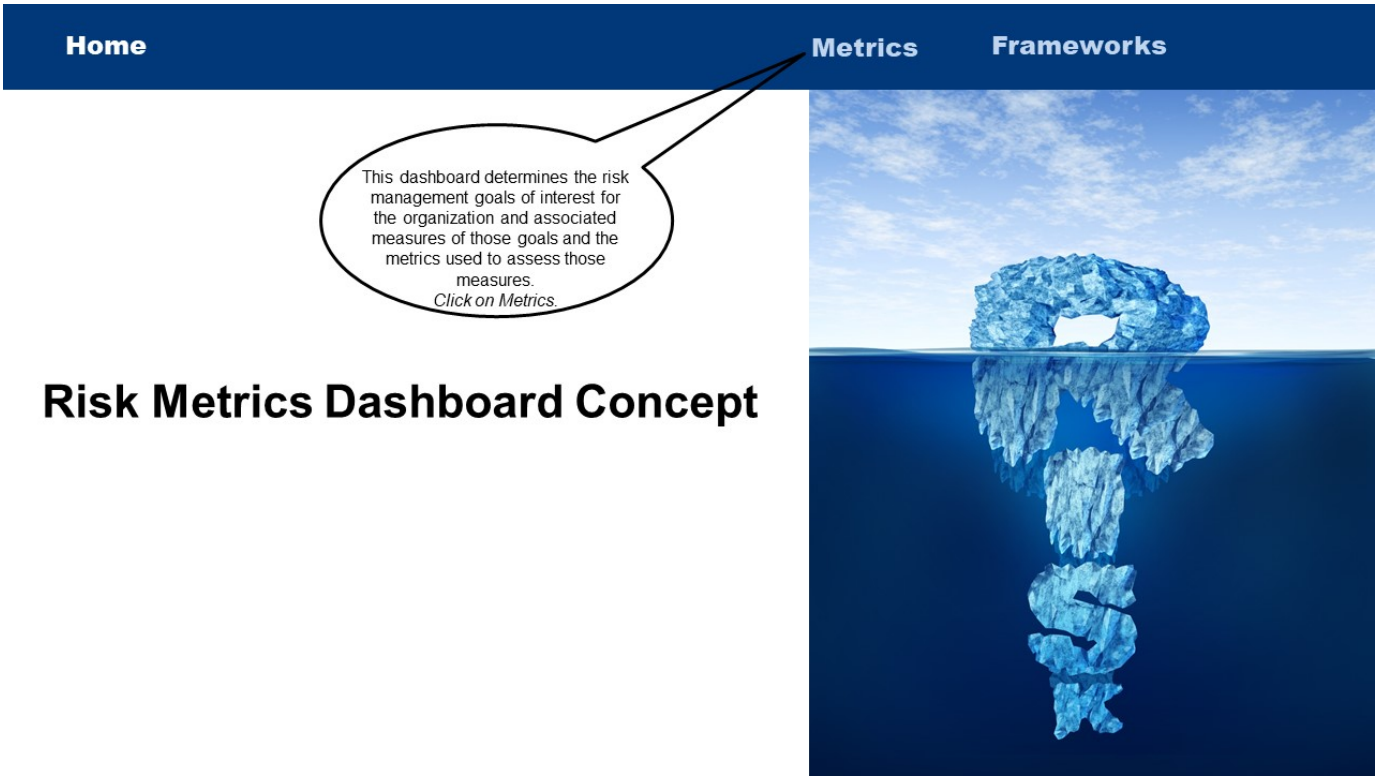

Fig. 7. Risk Metrics Dashboard Concept Landing Page

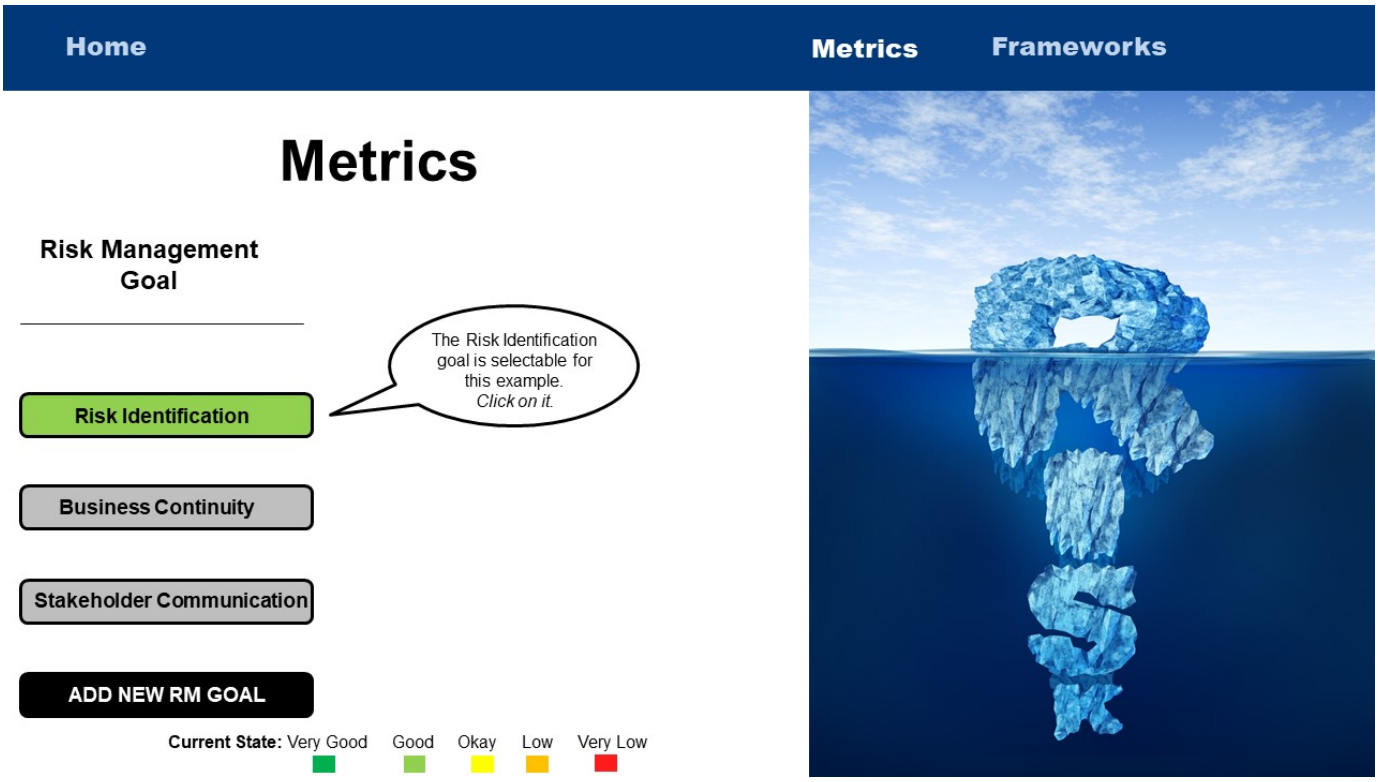

Fig. 8. Risk Identification Step

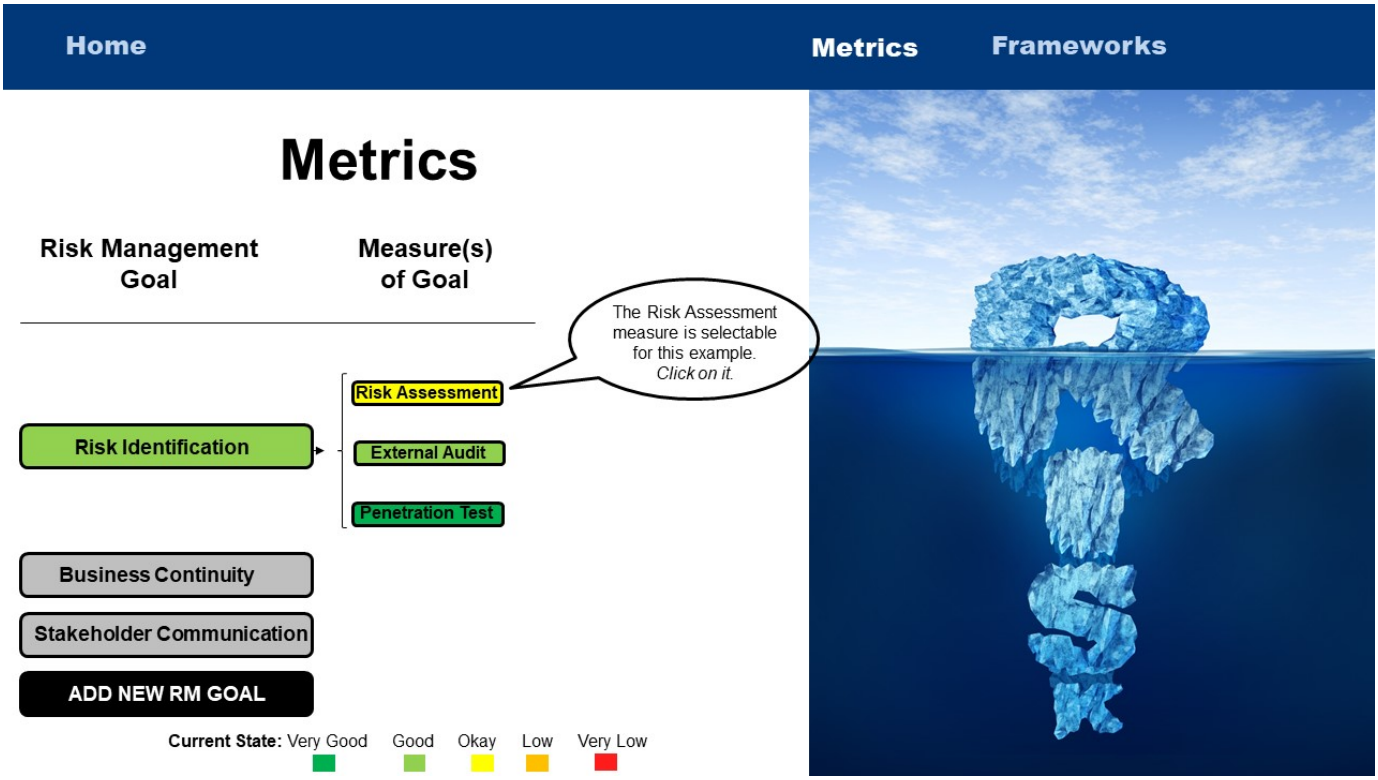

Fig. 9. Measure(s) of Goal

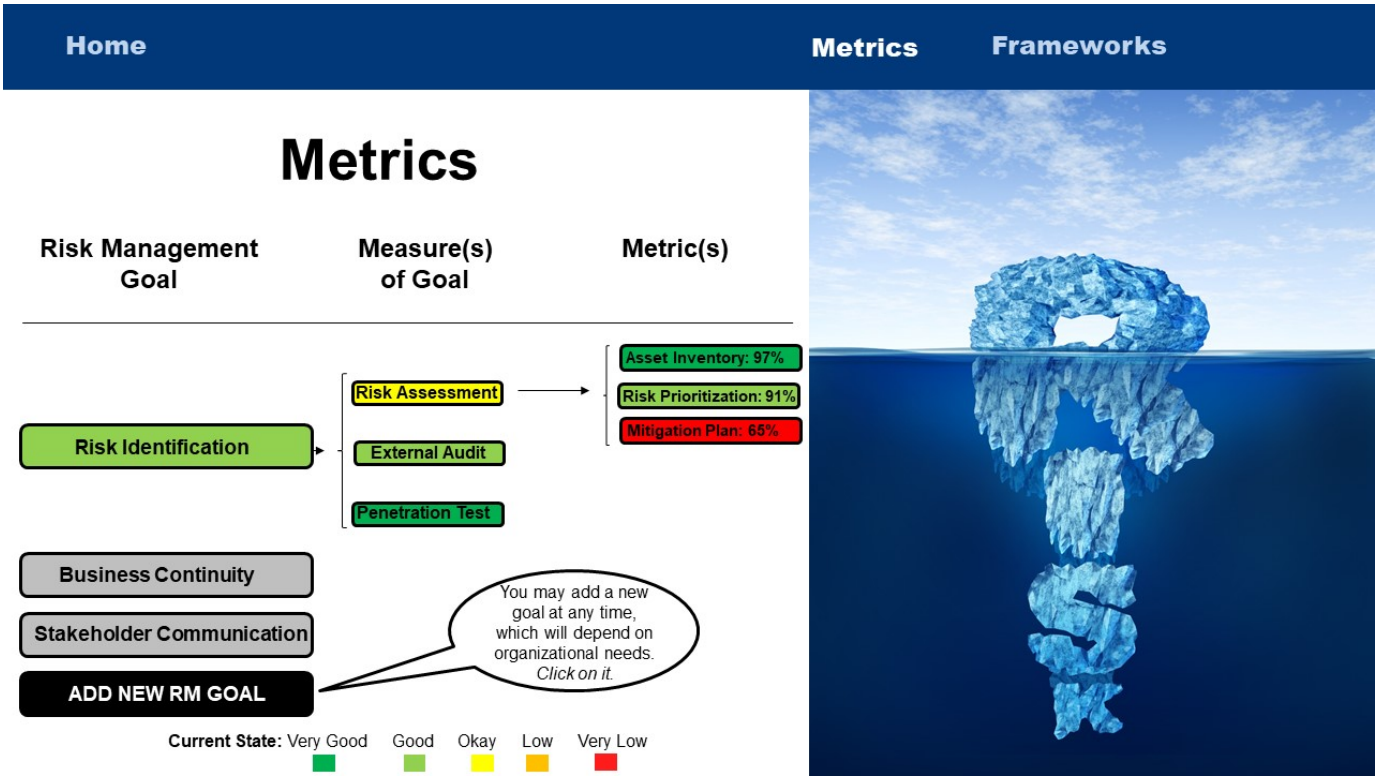

Fig. 10. Specific Metrics for Each Goal

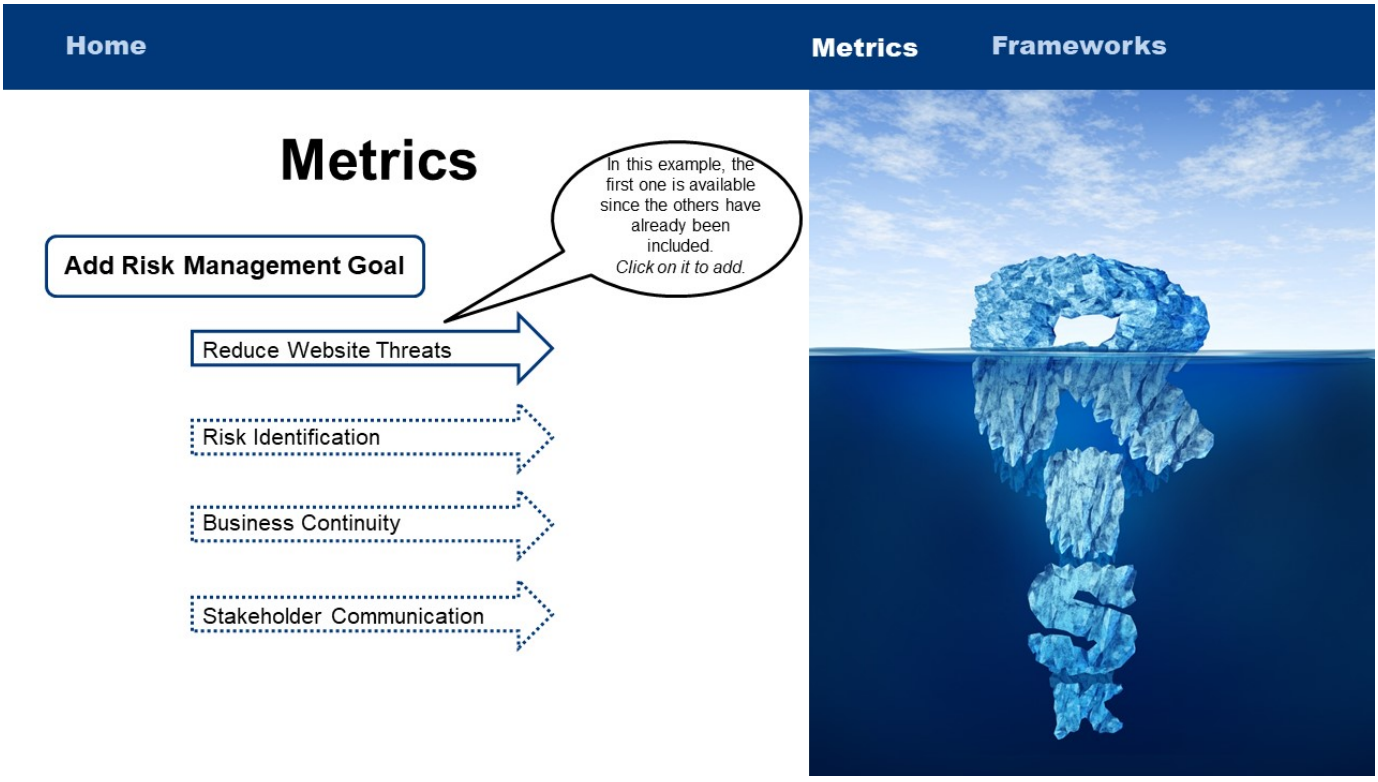

Fig. 11. New Risk Management Goal May be Added

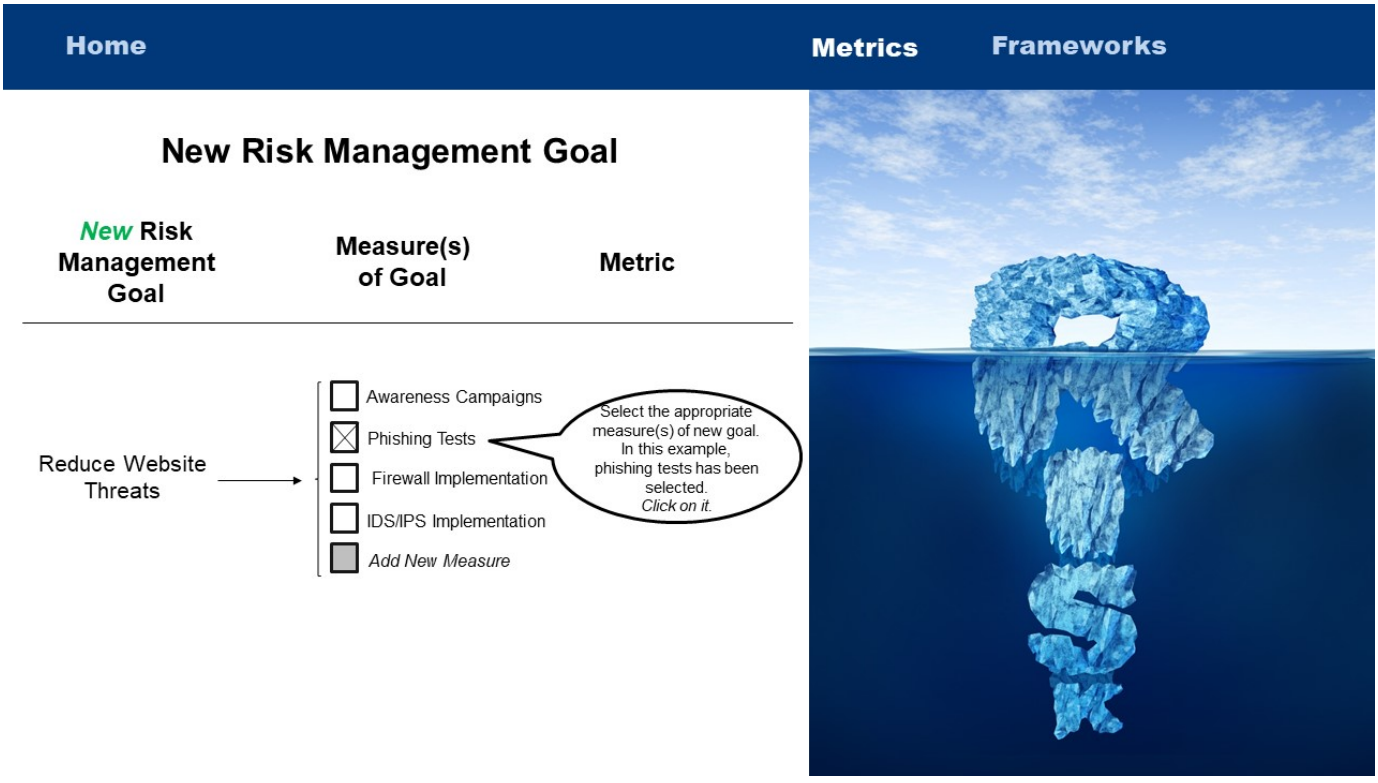

Fig. 12. Determine the Measure(s) of Goal

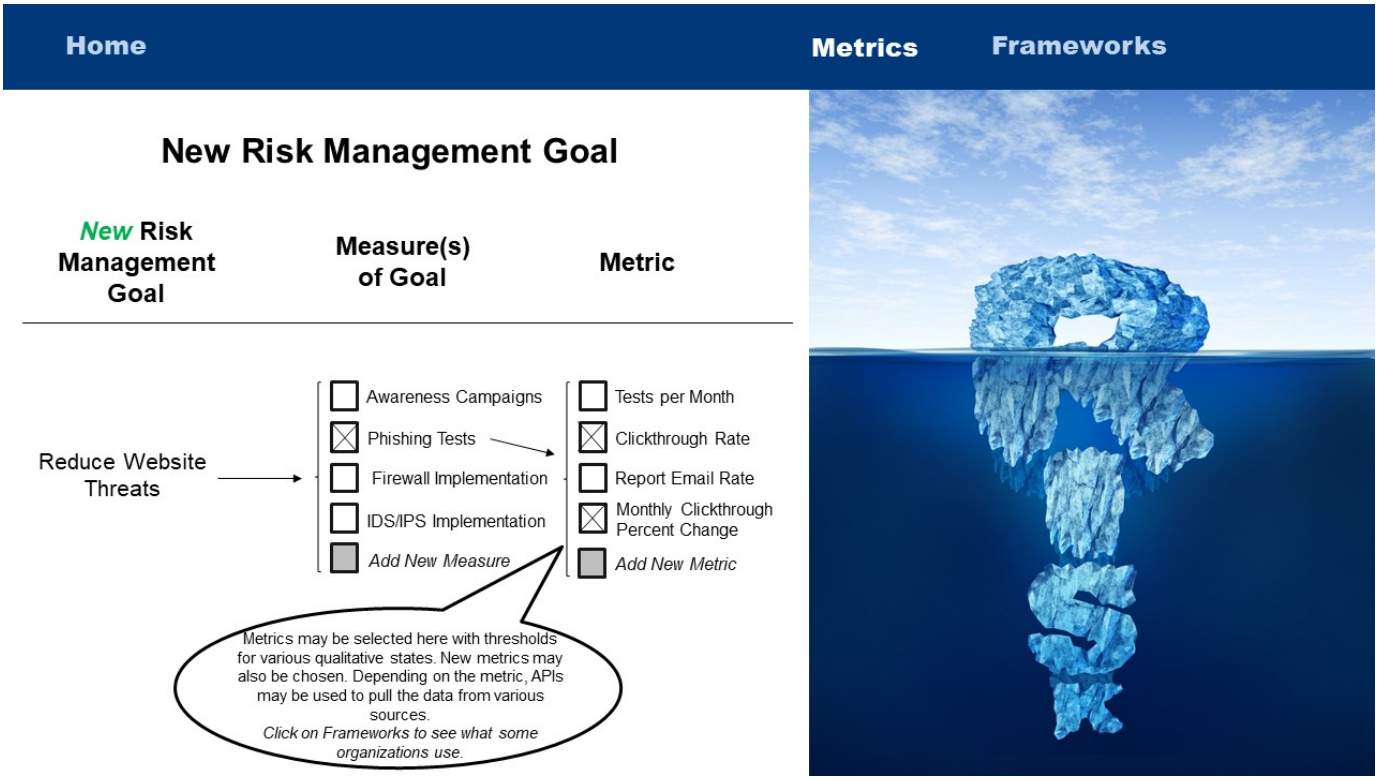

Fig. 13. Applicable Metrics for the Measure(s) May be Added

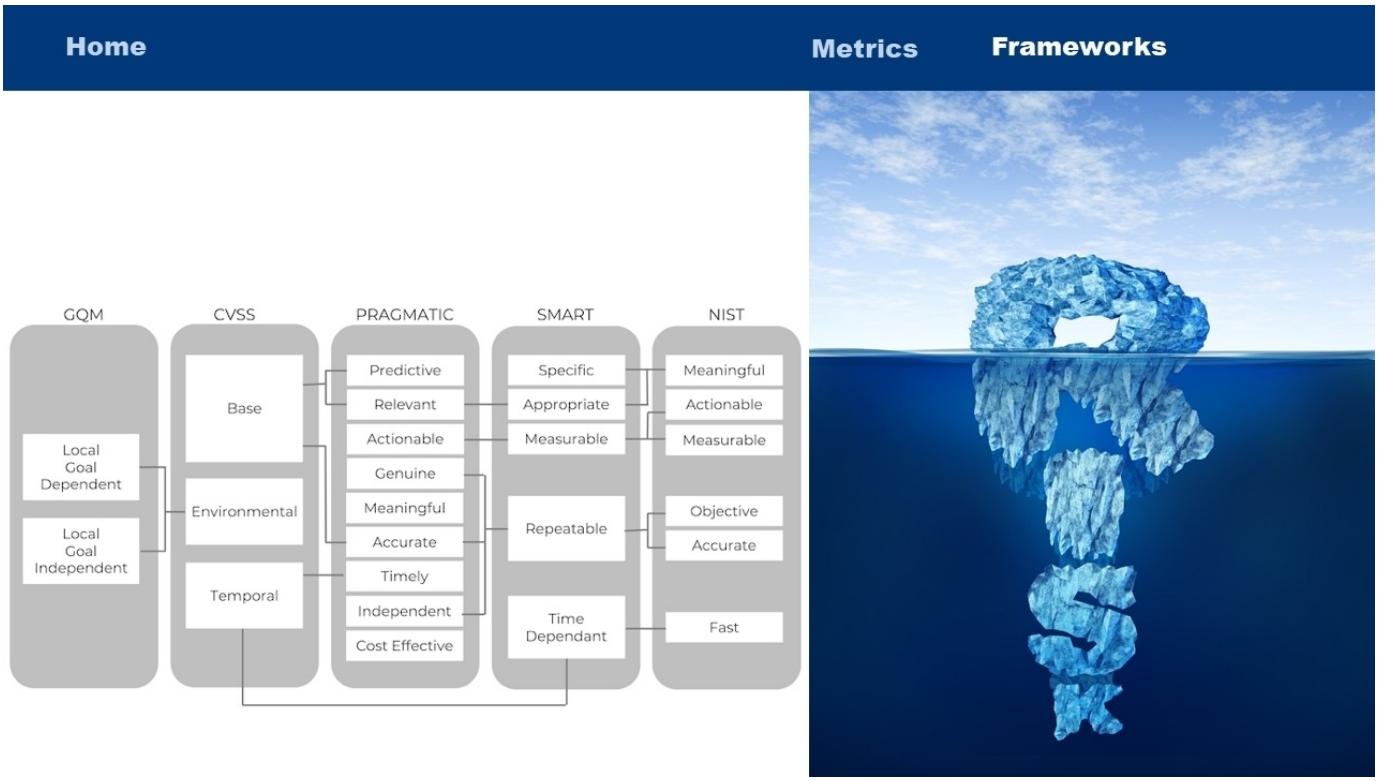

Fig. 14. A List of Specific Frameworks an Organization May Use