Massachusetts Institute of Technology
Cybersecurity at MIT Sloan
Working Paper

The Cyber Risk Cube: A New Tool for Cybersecurity Risk Management

Dr. Michael Siegel
msiegel@mit.edu

Kristin YiJie Chen
kristiny@mit.edu

Tara Kuruvila
tkuruvil@wellesley.edu

Working Paper
November 16, 2021

E94
245 First St
Cambridge, MA 02142

The Cyber Risk Cube: A New Tool for Cybersecurity Risk Management

By

Dr. Michael Siegel
msiegel@mit.edu

Kristin YiJie Chen
kristiny@mit.edu

Tara Kuruvila
tkuruvil@wellesley.edu

Table of Contents

Executive Summary

In the last few years, the concern over cybersecurity has grown dramatically. As threats become more prevalent, it is crucial for companies to have a practical and effective cyber risk strategy. With all the existing, and sometimes competing, guidelines and frameworks intended to inform cyber risk strategies, organizations face the problem of deciding which is right for them. To resolve the confusion, this research proposes a practical and useful tool that can be used by organizations of any size or in any industry for cyber risk management.

We propose a Cyber Risk Cube (CRC) designed to be practical for all parts of an organization. It can be used as a common language for sharing ideas and solutions to cyber risk management. Organizations can use it as an information-sharing tool to communicate about approaches to managing cyber risk. At the same time, the CRC provides details for implementing solutions to managing cyber risks. The CRC tool begins with the examination of three fundamental parings for examining cyber risk: Internal/External, Measurement/Management, and Qualitative/Quantitative:

- Internal/External has to do with what is being assessed and by whom
- Measurement/Management is the frequency and oversight of that risk assessment output
- Qualitative/Quantitative has to do with how risk is being measured during the assessment

These collectively make up the starting point and the common language for building a cyber risk management practice. We use these fundamentals to aid organizations in selecting the most effective cyber risk management strategies recommended for their organization by size, industry, and other defining characteristics. The approach provides for a database of tools, techniques and cases to assist organizations in design and development of cyber risk management solutions. Finally, this approach provides a means for working with regulators, auditors and dealing with issues related to governance and compliance.

I. Introduction

In recent years, there has been a dramatic increase in data breaches and other cyberattacks. Because these events result in the loss of customer information, trade secrets, and other confidential assets, this increase has seriously threatened corporate credibility, competitive advantage, and financial stability. During a typical meeting with the Board of Directors and C-level executives, there are several common cyber risk questions asked shown in ***Figure 1.1***:

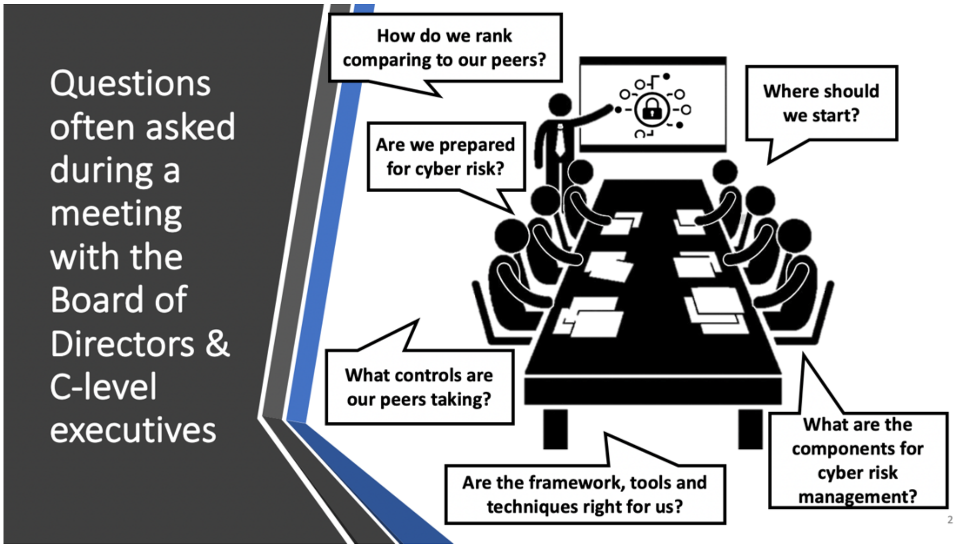

Questions often asked during a meeting with the Board of Directors & C-level executives
How do we rank comparing to our peers?
Where should we start?
Are we prepared for cyber risk?
What controls are our peers taking?
What are the components for cyber risk management?
Are the framework, tools and techniques right for us?
2

Figure 1.1 Common Cyber Risk Management Questions

When asked these questions, executives often lack concrete actionable answers. Organizations understand that as threats become more diverse and sophisticated, they have to respond to cybersecurity's dynamic nature. However, they are often unsure of exactly where to start or what to do when it comes to cyber risk. There are hundreds, if not thousands, of cyber risk publications, white papers, standards, frameworks, guidelines, tools, and academic articles. With the vast selection of frameworks, regulations, and resources, it is challenging for organizations to know, choose, and implement the right ones.

For larger firms the process might involve a wide range of consultants and approaches, while hard choices must be made to direct security spending for small and medium enterprises. Among all organizations, there is a need for a high-level strategy that allows organizations to build a holistic roadmap and compare themselves to their peers. Hence, we propose our new tool, the Cyber Risk Cube. Our tool seeks to guide organizations to a common understanding of cyber risk management. Using case studies and literature reviews, we consolidate data on current cybersecurity practices and their relative effectiveness. We evaluate which approaches are most favorably reviewed and most commonly undertaken and filter these by size, industry, rationale, budget, and other characteristics to create a database of these approaches. Thus, we can effectively make personalized recommendations to organizations.

II. Literature Review, Related Research and Practice

Given the plethora of existing frameworks and guides for managing cyber risk, choosing the best approach can be challenging. Although there exist some blog posts and journal-published papers (as well as many blog posts), which compare well-known and commonly used frameworks by listing the merits and shortcomings of each, these are targeted for a point in decision making rather than the beginning of the process and there does not appear to be a standardized model. For example, blog posts on TechRepublic[1], Security Boulevard[2], Edureka[3], and CIO[4] explain the basics of the common frameworks and considerations when starting to think about cybersecurity. However, there is an apparent lack of simplified models for starting the process and comparing across and inside organizations with a holistic view, leaving a gap to be filled both in research and practical tools. Therefore, we propose an information-sharing tool for best cybersecurity practices with the aim of filling this gap.

There is a large literature in cybersecurity that studies information-sharing tools. Choucri, Madnick, and Koepke (2017)[5] categorize and summarize institutions propelling data-sharing initiatives. They report over sixty CERTs, ISACs, International Entities, US national entities, Non-US national entities, Non-profits, and private sector companies and the types of information they share. It is evident that a large institutional landscape is dedicated to information sharing of cyber threats and vulnerabilities.

In a technical report for Microsoft, Goodwin et al. (2015)[6] present a guide for the development of information sharing tools related to cyber threats. Their framework identifies methods and mechanisms of exchange, including person-to-person and machine-to-machine sharing, and models of exchange, which includes voluntary exchange models and mandatory disclosure models. The CRC tool fits nicely into the authors' identified framework as a voluntary exchange model of information from machine-to-machine.

In addition, the CRC tool employs many of the suggestions to reduce barriers to information sharing outlined in Lewis et al. (2015)[7] which focuses on the supply-chain level. They suggest anonymizing data in order to prevent misuse of sensitive information and other organizations gaining competitive advantages. Our tool provides the option for organizations to be anonymous.

[1] https://www.techrepublic.com/article/how-to-choose-the-right-cybersecurity-framework/
[2] https://securityboulevard.com/2019/02/which-cybersecurity-framework-is-right-for-you/
[3] https://www.edureka.co/blog/cybersecurity-framework/
[4] https://www.cio.com/article/3295578/how-to-implement-a-successful-security-plan.html
[5] https://cams.mit.edu/wp-content/uploads/2017-06.pdf
[6] C. Goodwin, J. P. Nicholas, J. Bryant, K. Ciglic, A. Kleiner, C. Kutterer, A. Massagli, A. Mckay, P. Mckitrick, J. Neutze, T. Storch, and K. Sullivan. A framework for cybersecurity information sharing and risk reduction. Technical report, Microsoft Corporation, 2015. https://download.microsoft.com/download/8/0/1/801358EC-2A0A-4675-A2E7-96C2E7B93E73/Framework_for_Cybersecurity_Info_Sharing.pdf
[7] R. Lewis, P. Louvieris, P. Abbott, N. Clewley, and K Jones. "Cybersecurity information sharing: a framework for sustainable information security management in uk sme supply chains". Proceedings of the European Conference on Information Systems (ECIS) 2014, Tel Aviv, Israel, June 9-11, 2014, ISBN 978-0-9915567-0-0 http://bura.brunel.ac.uk/handle/2438/9977

Crucially, none of the above-mentioned models focus on information-sharing related to frameworks and related decision making. Choucri, Madnick, and Koepke, target threats and vulnerabilities. Goodwin et al. target cyber threat information sharing and Lewis et al. targets supply chain information sharing. We contribute to the literature by reviewing and selecting the foundations of information sharing for other types of information and applying them to decision making regarding frameworks.

We reviewed articles and papers that address approaches to the six components of the cyber risk cube – Internal, External, Qualitative, Quantitative, Measurement and Management. Some reports and papers have addressed approaches to gain internal and external views of cyber risk such as conducting periodic internal audits, self-assessments, and assessments by third parties. For example, Deloitte[8], Crowe Horwath[9], Debra Cope[10] and Jacob Olcott[11] stated the importance and potential of managing cyber risk and gaining an internal view of it by performing internal audits and self-assessments periodically. However, these approaches only present the organization with a partial view of their cyber risk. Bozkus Kahyaoglu, S. and Caliyurt, K[12] determined key issues and weaknesses within the internal audit and the risk management perspective which further proved that these previous approaches do not consider other aspects of cyber risk management.

In the Gartner Security and Risk Management Summit of 2019[13], a session addressed quantitative versus qualitative cyber risk assessments and covered the pros and cons of each. They discussed the state of risk assessments and whether the industry was ready for reporting cyber risk analytics quantitatively. In the end, participants agreed that while there is still a place for qualitative assessments as a communication tool, the quantitative approach to cyber risk is the rising trend.

Other papers and several blogposts attempt to compare across qualitative and quantitative approaches. A few attempts to compare across frameworks. Roldán-Molina et al (2016)[14] contribute to the literature on aiding cyber risk related decision making. They propose a model "addressing the perception, comprehension, projection and decision/action layers" allowing one to identify which framework/approach is most suitable to support each of the layers. Another useful resource are the websites of companies that have created these frameworks and guides, both quantitative and qualitative. They often compare various frameworks on a number of characteristics declaring one as most effective. A RiskLens blog[15] compares the qualitative and quantitative approach and describes the strengths and weaknesses of each, based on a Gartner

[8] https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-cyber-ia-urgent-call-to-action.pdf

[9] http://contentz.mkt5790.com/lp/2842/240669/Foundation%20The%20Future%20of%20Cybersecurity%20in%20IA%20March%202018_1.pdf

[10] https://search.proquest.com/docview/1731524213?pq-origsite=gscholar

[11] https://www.nist.gov/system/files/documents/2016/09/15/bitsight_rfi_response.pdf

[12] https://www.emerald.com/insight/content/doi/10.1108/MAJ-02-2018-1804/full/html

[13] https://www.risklens.com/blog/gartner-2019-debate-quantitative-vs-qualitative-cyber-risk-analysis/

[14] https://dora.dmu.ac.uk/bitstream/handle/2086/15670/Paper_CISTI_2017_04_04_En.pdf?sequence=1&isAllowed=y

[15] https://www.risklens.com/blog/gartner-2019-debate-quantitative-vs-qualitative-cyber-risk-analysis/

debate. The article focuses on the FAIR model that powers RiskLens. In a post[16], UpGuard compares BitSight, SecurityScorecard and UpGuard. However, these blog posts, although insightful, are often biased towards the hoster's framework.

As for the measurement and management component of the CRC, Filippo Curti (2019)[17] contributed to the literature on Cyber Risk Definition and Classification for Financial Risk Management. In their Appendix A, they proposed to conduct a "aggregated monthly level" schedule that would track both the cyberattacks that resulted in financial losses (incidents), and the ones that did not result in financial losses. According to the Guide for Conducting Risk Assessments published by NIST[18], the frequency of cyber risk assessment and risk factor monitoring should be determined by the organization. Organizations that follow this guidance can use the CRC to understand cyber risk management and measurement approaches taken by peers.

Gartner PeerInsights[19] [20] examines what frameworks competitors and peers are using and their relative effectiveness. Here, reviewers can rate various kinds of software and tools, comment on their experiences with it, and compare them to other competing software and tools. Reviewers identified by company size, industry and region. This is an extremely useful tool but one that lends itself to considerable selection bias. The subset of people and organizations that write reviews are likely not representative of all users and customers are likely to post reviews if they are either extremely satisfied or dissatisfied with the particular risk management tool. In addition, although Gartner PeerInsights focuses on various categories including Blockchain Platforms, Data Intergration, and IT Risk Management, outside of a SIEM tools category, there is no broader category dedicated to cybersecurity risk management tools which the CRC tool specifically focuses on along with cyber risk strategies. The CRC tool utilizes the same principle of collecting and presenting peer reviews but concentrates on a more focused category allowing for more detail and relevance for users.

These are helpful but have some drawbacks that the CRC address. First, these only focus on the most well-known, largely quantitative frameworks so they do not allow for a combination of quantitative and qualitative approaches which are often the best way forward. Moreover, these guides are general and not tailored to an organization's size, industry, budget, or other defining characteristics all of which impact the optimal cyber security strategy an organization should seek to implement. These papers and blogposts also do not lend any insight into what competitors might be doing or how to compare an organization's level of cybersecurity with its peers. Moreover, these papers and articles only consider and present a partial view of the organization's cyber risk.

III. The Cyber Risk Cube Tool

[16] https://www.upguard.com/articles/bitsight-vs-securityscorecard

[17] https://www.richmondfed.org/-/media/richmondfedorg/conferences_and_events/banking/2019/cyber_risk_classification_white_paper.pdf

[18] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[19] https://www.gartner.com/reviews/market/it-vendor-risk-management/vendor/upguard

[20] https://www.gartner.com/reviews/market/it-vendor-risk-management/compare/securityscorecard-vs-upguard

In this section we introduce the Cyber Risk Cube. For purposes of illustration, we will consider Acme Corporation a fictitious medium-sized technology company. Senior management at Acme Corporation has examined a lot of articles and online information about cybersecurity. They have determined that cyber risk management would be their priority this year and plan to implement a strategy to reduce cybersecurity risk. The executives learned about the Cyber Risk Cube and wanted to know more about how it works. They begin by understanding the six components that form the cyber risk cube in ***Figure 1.2***.

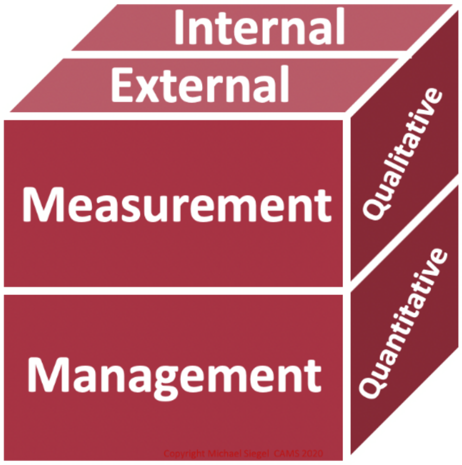


Figure 1.2 Cyber Risk Cube Tool

The Cyber Risk Cube with the six components (Internal, External, Quantitative, Qualitative, Measurement, and Management) impacts understanding, communicating, and building a risk management approach. The six components are in pairs: Internal and External, Quantitative and Qualitative, and Measurement and Management:

- Internal/External has to do with what is being assessed and by whom
- Measurement/Management is the frequency and oversight of that risk assessment output
- Qualitative/Quantitative has to do with how risk is being measured during the assessment

The cyber risk cube synthesizes the common tools, frameworks, methodology, and literature on cyber risk management from these six aspects.

Acme Corporation thinks this is a reasonable approach to dealing with cyber risk management based on their previous research. They decide to learn more about each pair's definitions and examples on the faces of the CRC.

Internal/External

This face of the cube makes the critical distinction between the organization's cybersecurity risk's internal and external views. An internal view comprises all risk factors that the organization itself can monitor and manage along with the security controls applied to mitigate the organization's internal cyber risk. An external view describes the facets of the risk that are detected externally about an organization, for example, the cyber risk associated with a third-party supplier. This includes assessing the organization’s risk level, as seen by third parties, and the organization’s assessment of third-party risks.

An organization needs to measure its security to determine whether they are taking the right steps to protect the business from cyber threat. Examples of approaches to internal or external cyber risk views will be included in the Tools and Techniques Database (see **Section IV***)*. For instance, yearly internal security audits, self-assessments, and managing security control for external assessment are effective ways to gain an internal view of the organization’s risk level. Management for the external evaluation refers to security controls that the organizations can adopt to reduce the organization’s risk level, as seen by external parties.

As for gaining an external view of third-party risk level, due diligence must be conducted before selecting and entering contracts or relationships with third parties. Organizations should not rely solely on experience with or prior knowledge of the third party as a proxy for cyber risk assessment. Approaches to the external component could be onsite or offsite vendor audits and specific third-party risk management guidelines such as OCC’s third-party relationships - a risk management guideline mostly for banking industries. Onsite visits may be useful to examine the third party's operations and capabilities. Finally, technical assessments are possible by incorporating technical measures (e.g., BitSight, Security Scorecard) of cyber risk.

Measurement/Management

This face of the cube represents a choice between static and dynamic management of cyber risk. For the most part, the choice will depend on the periodicity of managing and measuring their cyber risk. The Measurement component assumes that measuring cyber risk is always associated with some level of management. Therefore, the Measurement component means cyber risk measurement with infrequent management (e.g., set intervals such as monthly, yearly). The Management component is associated with cyber risk measurement and management that is more frequent (e.g., set intervals with shorter duration – daily, weekly and, in some cases approaching real-time). For the Management component, it refers to the dynamic management of cyber risk. Examples include organizations that perform audits to measure and manage cyber risk daily or weekly. The infrequent management of cyber risk the Measurement component is an example of organizations conducting annual or monthly security goal evaluations.

An interesting example of practicing either a Measurement or Management using the same measure is demonstrated by Key Performance Indicators (KPIs). KPIs are used to track the performance of the organization’s implemented controls periodically because using KPIs is an effective way to measure the success of a cybersecurity program and aid in decision-making. It provides a snapshot of how the security team functions over time and helps the organization understand better what is working and what is not and improve decision-making about future projects. KPIs can assess cyber risk at varying frequencies. Therefore, KPIs are a quantitative approach that can be used in either the Measurement component or the Management component based on the frequency that the organization is assessing. If the organization is tracking cyber risk through KPIs and manage cyber risk daily, for example, that is a relatively high frequency and it would be categorized in the Management component. Otherwise, it would fall into the Measurement component.

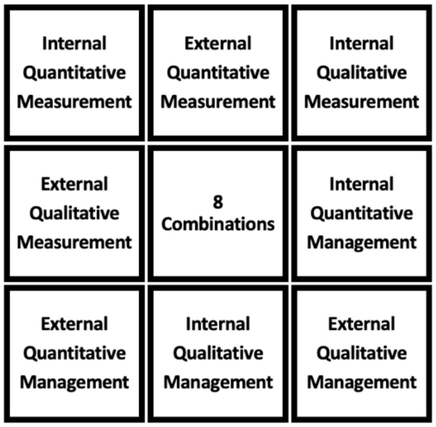
Qualitative/Quantitative

Qualitative risk assessments use ordinal rating scales to plot risk based on likelihood of occurrence and impact of loss. For instance, the FFIEC cybersecurity assessment tool[21] or NIST Cybersecurity Framework[22] which measures the use of cybersecurity controls is classified as a qualitative approach. Quantitative risk assessments use dollars, cents or scalar values such as Value-at-Risk (VaR) rather than an ordinal measure. Other examples of quantitative approaches include Factor Analysis of Information Risk (FAIR)[23], BCG Cyber Doppler[24], Security Assessment Framework for Enterprise (SAFE)[25], Cyber Security Evaluation Tool (CSET)[26], BitSight[27], SecurityScoreCard[28], and Cyber Resilience Assessment Framework Tool[29].

Acme Corporation is now even more convinced that they want to go ahead with using the CRC tool. After understanding the three pairs of components, they will select at least one component from each of the pairs on each cube's face. This means they choose either internal or external, measurement or management, and qualitative or quantitative.

IV. Methodology of the Cyber Risk Cube Tool

Organizations will choose one or more faces of the Cube as shown in ***Figure 1.3***. The selection will be based on their rationales, budget constraints, workforce, or organization posture.



Internal Quantitative Measurement	External Quantitative Measurement	Internal Qualitative Measurement
External Qualitative Measurement	8 Combinations	Internal Quantitative Management
External Quantitative Management	Internal Qualitative Management	External Qualitative Management

Figure 1.3 Combinations of the Cyber Risk Cube Tool

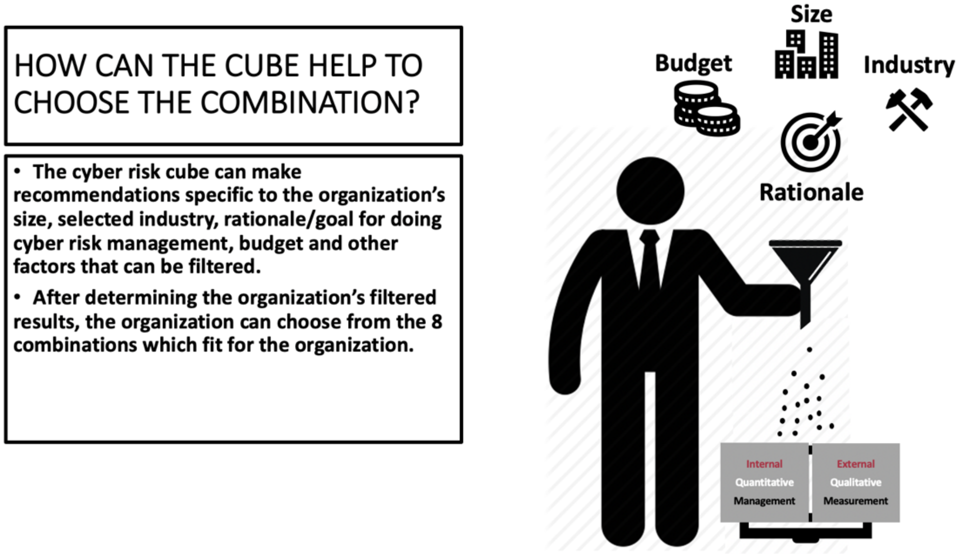
Filters

[21] https://www.ffiec.gov/cyberassessmenttool.htm
[22] https://www.nist.gov/cyberframework
[23] https://www.fairinstitute.org/
[24] https://www.bcg.com/capabilities/technology-digital/smarter-way-to-quantify-cybersecurity-risk.aspx
[25] https://www.lucideus.com/safe.html
[26] https://www.us-cert.gov/ics/Assessments
[27] https://www.bitsight.com/
[28] https://securityscorecard.com/
[29] https://www.hkma.gov.hk/media/eng/doc/key-information/speeches/s20160518e2.pdf

Not all organizations are going to handle cyber risk management in the same way. Organizations will vary their approach based on size, selected industry, rationale for doing cyber risk management, budget, compliance and other factors. We have included a filter function for organizations to more easily get appropriate combinations based on factors in ***Figure 1.4***. The CRC Tool applies to organizations of all sizes and industries.

The management team at Acme Corporation examined these components and they feel that they will analyze the cyber risk to gain an internal view of their cyber risk level. This year, the management approach will frequently measure and manage their cyber risk as cyber risk management is their priority. They decide to use a qualitative approach due to their time and budget constraints. These are their initial choices of components, but they will confirm the combination after looking at more detail provided in the Cyber Risk Cube Tool. Acme management has decided to use this combination as its first cyber risk project; it may consider other combinations later.

The Acme Corporation looked at this closely and classified themselves as a medium-size technology company. Their rationale for implementing cyber risk management is to comply with regulations and requirements requested from their customers. Acme Corporation has chosen the Internal – Qualitative – Management combination after going through the definitions and examples of the six components. They plan to use the *Tools and Techniques* and *Cases* databases described below to look at examples of how others have approached cyber risk management.



HOW CAN THE CUBE HELP TO CHOOSE THE COMBINATION?

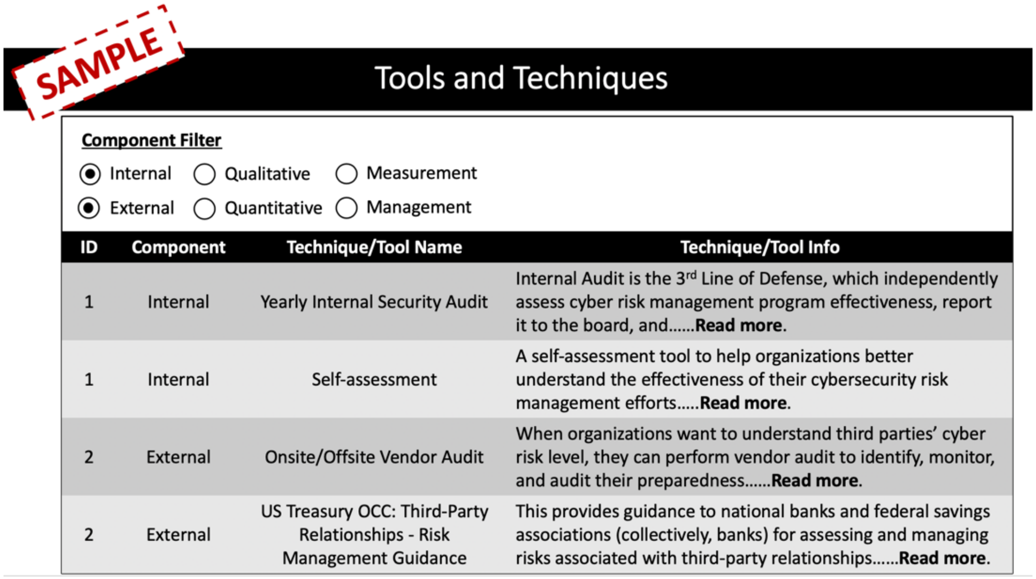
- **The cyber risk cube can make recommendations specific to the organization's size, selected industry, rationale/goal for doing cyber risk management, budget and other factors that can be filtered.**
- **After determining the organization's filtered results, the organization can choose from the 8 combinations which fit for the organization.**

Figure 1.4 Filtering feature of the Cyber Risk Cube

Tools and Techniques and Cases

After filtering, the CRC will help organizations make practical decisions by displaying two databases: Tools and Techniques and Cases. Possible tools and techniques used for each of the six components available in the Tools and Techniques Database, while collecting organizational implementations of the eight combinations of components will be included in the Cases Database. We have developed an initial set of records in both databases using existing case studies, literature, and online information sources.

A sample of possible tools and techniques is shown in ***Figure 1.5***. The initial schema of the Tools and Techniques database is shown in ***Figure 1.6***. Organizations can browse options for tools and techniques for each of the six components. Additional examples of tools and techniques can be found in Appendix B.



SAMPLE

Tools and Techniques

Component Filter

● Internal ○ Qualitative ○ Measurement

● External ○ Quantitative ○ Management

ID	Component	Technique/Tool Name	Technique/Tool Info
1	Internal	Yearly Internal Security Audit	Internal Audit is the 3rd Line of Defense, which independently assess cyber risk management program effectiveness, report it to the board, and……**Read more.**
1	Internal	Self-assessment	A self-assessment tool to help organizations better understand the effectiveness of their cybersecurity risk management efforts…..**Read more.**
2	External	Onsite/Offsite Vendor Audit	When organizations want to understand third parties' cyber risk level, they can perform vendor audit to identify, monitor, and audit their preparedness……**Read more.**
2	External	US Treasury OCC: Third-Party Relationships - Risk Management Guidance	This provides guidance to national banks and federal savings associations (collectively, banks) for assessing and managing risks associated with third-party relationships……**Read more.**

Figure 1.5 Sample of the Tools and Techniques Database[30]

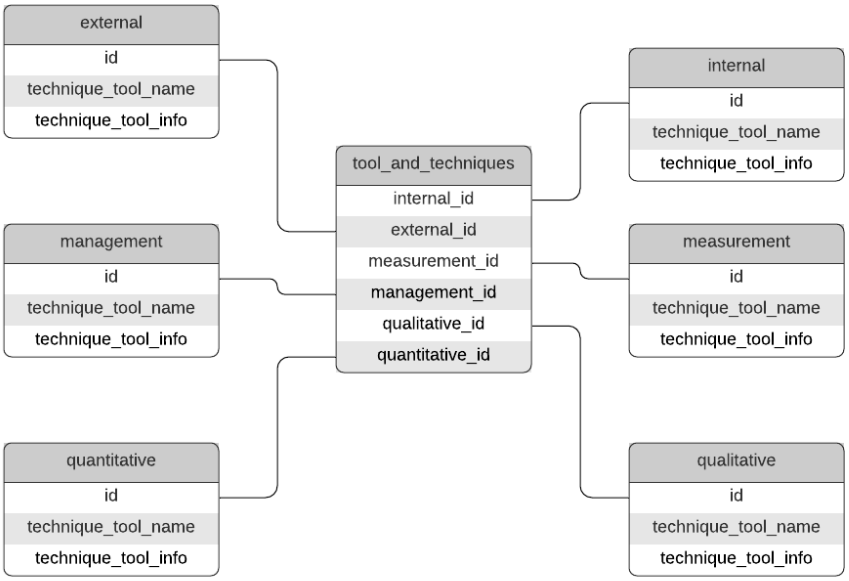
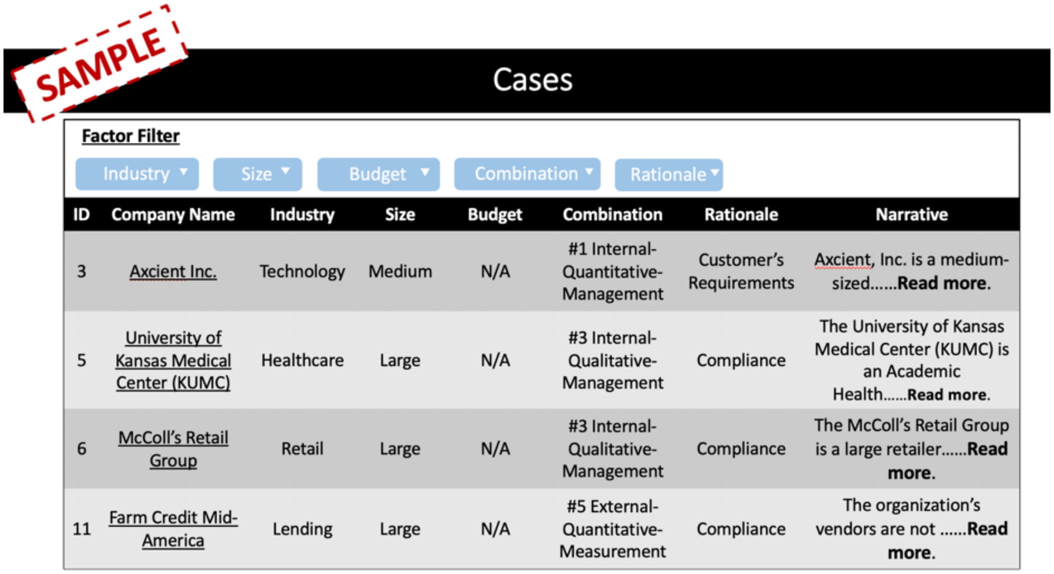


Figure 1.6 Schema of the Tools and Techniques Database

[30] Appendix B includes a limited set of examples which are used in the paper

A sample of the Cases that a user can access is shown in ***Figure 1.7*** and the initial database schema in ***Figure 1.8***. The sample case study is a Large Healthcare Organization with approximately 3,600 employees[31]. Cyber risk management is performed by the University of Kansas Medical Center (KUMC)'s Office of Information Security (OIS) which is a relatively new department that formerly existed as a subunit of the IT Department.

KUMC performs a self-assessment, which is identified as an Internal approach in the previous Tools and Techniques Database. As for the Qualitative component, the organization uses the Baldrige Cybersecurity Excellence Builder in conjunction with the NIST Cybersecurity Framework for self-assessment and program development. For the Management component, it implements management controls from the NIST Cybersecurity Framework and actively manages cyber risk by daily monitoring of risk. The narrative describes how this process helped the KUMC OIS team understand their roles and engage their customers in protecting the organization. Moreover, it helps them establish a better approach to intake, response, and follow-up, improving stakeholder relationships and getting the right solutions to their customers.



ID	Company Name	Industry	Size	Budget	Combination	Rationale	Narrative
3	Axcient Inc.	Technology	Medium	N/A	#1 Internal-Quantitative-Management	Customer's Requirements	Axcient, Inc. is a medium-sized......**Read more.**
5	University of Kansas Medical Center (KUMC)	Healthcare	Large	N/A	#3 Internal-Qualitative-Management	Compliance	The University of Kansas Medical Center (KUMC) is an Academic Health......**Read more.**
6	McColl's Retail Group	Retail	Large	N/A	#3 Internal-Qualitative-Management	Compliance	The McColl's Retail Group is a large retailer......**Read more.**
11	Farm Credit Mid-America	Lending	Large	N/A	#5 External-Quantitative-Measurement	Compliance	The organization's vendors are not ......**Read more.**

Figure 1.7 Sample of the Cases Database

[31] https://www.nist.gov/cyberframework/success-stories/university-kansas-medical-center

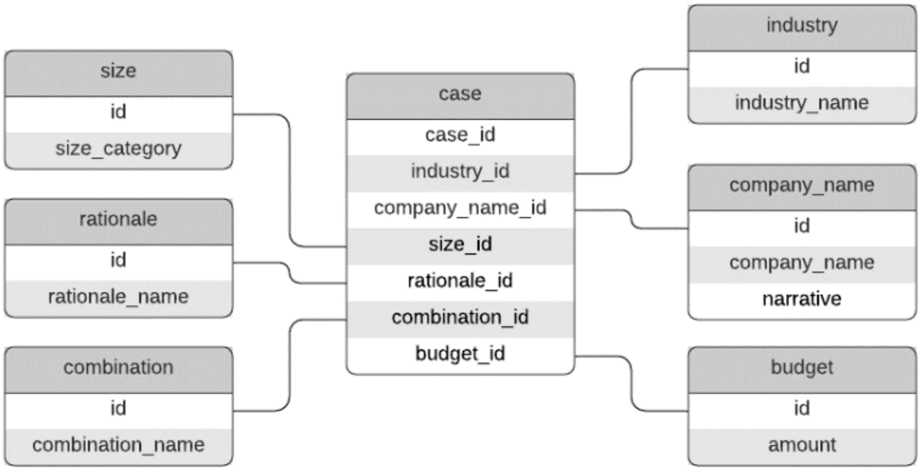
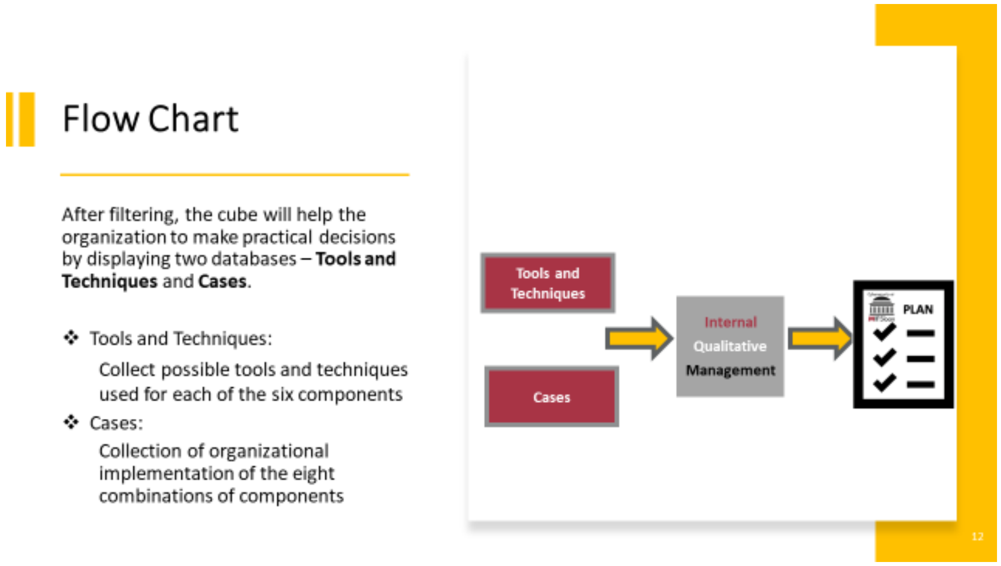


Figure 1.8 Schema of the Cases Database

After going through these two databases, organizations will decide what tools and techniques they would like to adopt in their organization. Organizations can finalize their decision of on which combination(s) to apply and develop an implementation plan for the organization. Additional examples of cases can be found in Appendix A.



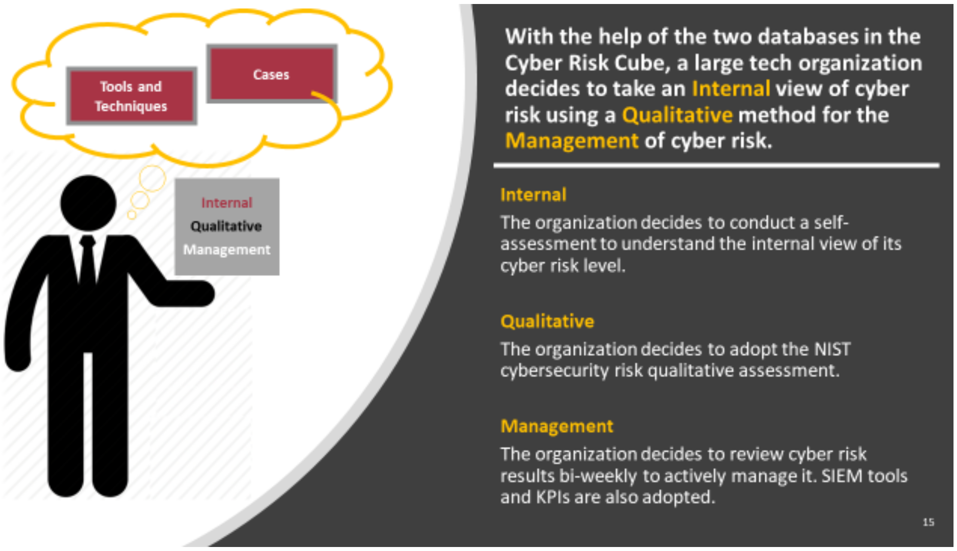
Flow Chart

After filtering, the cube will help the organization to make practical decisions by displaying two databases – **Tools and Techniques** and **Cases**.

- Tools and Techniques:
  Collect possible tools and techniques used for each of the six components
- Cases:
  Collection of organizational implementation of the eight combinations of components

Figure 1.9 Flow Chart of the Cyber Risk cube

After deciding the combination that they want to adopt, the Acme Corporation uses the CRC tool's filtering feature to help them make practical decisions by displaying two databases – Tools and Techniques, and Cases as shown in ***Figure 1.9***. The factors that they use to filter in the Cases database are Industry – Technology, Size – Medium, and Combination – #3 Internal/Qualitative/Management. For the Tools and Techniques database, the Acme Corporation filter the component – Internal, Qualitative, and Management. These two databases display the possible tools and techniques and case studies according to the filtering results.



With the help of the two databases in the Cyber Risk Cube, a large tech organization decides to take an Internal view of cyber risk using a Qualitative method for the Management of cyber risk.

Internal

The organization decides to conduct a self-assessment to understand the internal view of its cyber risk level.

Qualitative

The organization decides to adopt the NIST cybersecurity risk qualitative assessment.

Management

The organization decides to review cyber risk results bi-weekly to actively manage it. SIEM tools and KPIs are also adopted.

15

Figure 1.10 Decision made with the help of Cyber Risk Cube

The Acme Corporation has decided to take an *Internal* view of cyber risk using a *Qualitative* method for the *Management* of cyber risk after going through these two databases in the cyber risk cube as shown in ***Figure 1.10***. To obtain an internal view of their cyber risk, they decide to conduct a self-assessment just like what the other medium-sized organization is doing to understand the internal view of its cyber risk level. The Acme Corporation chooses to adopt the Qualitative component with the NIST cybersecurity risk assessment. For the Management component, they will be reviewing cyber risk results bi-weekly and making changes based on the reviews. SIEM tools and KPIs are also adopted to measure and mange cyber risk. Examples of these tools and techniques are described in Appendix B.

Acme also believes that this language and approach to cyber risk management will help deal with governance and compliance issues.

1. *Data Collection System*

A data collection system supports the Tools and Techniques and Cases databases. A schematic of the systems is shown in ***Figure 1.11***.

We start by conducting case studies, literature reviews, and collecting feedback from organizations to build database instances. We then apply filter variables to the cases. Filter variables include but are not limited to size (small, medium, large) or industry (banking, energy, industrial, technology, etc.). Organizations will use the same filter variables to find practices that might fit their needs. These same filter variables will allow them to compare with industry peers' cyber risk practice (or other groups inside a single organization).

The review process will contain both a peer review and self-review process to provide feedback on individual instances in the database. This is where reviewers can suggest how well a tool worked for their practice or how well a case worked as an implementation. This cycle ensures the CRC tool's information can continue to be improved and be more effective and reliable for companies to use.

Information in the databases will be enhanced by the continuous review of the literature and available case studies. Additionally, we will collect data from individual companies, industry groups, government and non-governmental organizations to create a rich set of tools, techniques, and cases for the CRC tool. An option for adding anonymous data will be available.

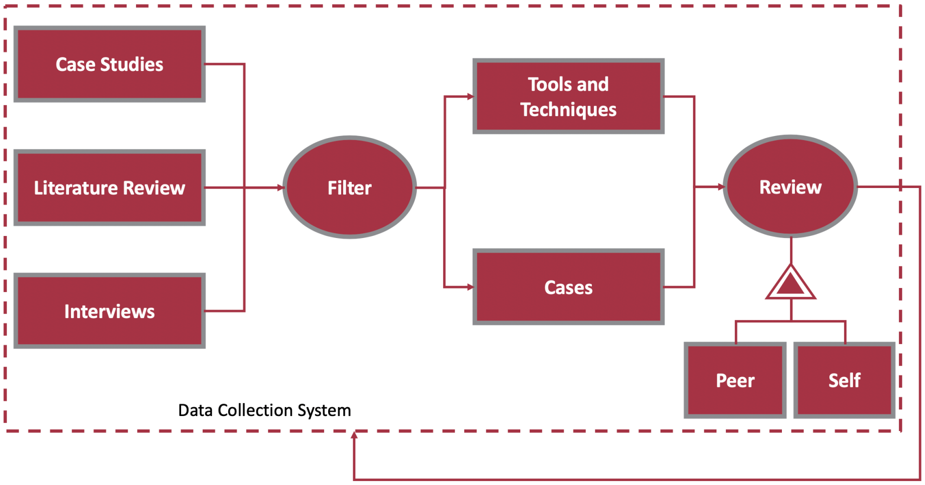


Figure 1.11 Flow Chart of the Data Collection System

2. ***Continuous Improvement of the Database***
   We are planning to improve the Cyber Risk Cube tool by adding features such as a scoring system. Cases will be graded in the selection process, making it easier for organizations to select possible implementations. Organizations can also study others' improvement in the industry by keeping up with new and changing tools and techniques, and cases. We do not advocate for the organization blindly copying security solutions without reflecting on how they fit their own organization. A lot can be learned from studying how other organizations (or other parts of your organization) have solved similar cyber risk management problems.

V. Cyber Risk Cube: Options for Implementation

We envision the CRC and associated toolset to be useful for all organizations with varying models for data collection and sharing. For example, a large company may have a private option where the Cube is used for internal knowledge collection and sharing. It may also take advantage of a semi-private implementation provided by an industry specific Information Sharing and Analysis Centers (ISACs). Alternatively, the company may look for a larger private platform for additional information on tools, techniques and applications of specific cases. On the other hand, a small to medium-size enterprise might turn to a sponsoring industry consortium to use the CRC in providing advice on cyber risk management approaches through data collected anonymously from consortium members.

Below are some **examples** of how different types of organizations might use the Cyber Risk Cube to support development of cyber risk management approaches:

1. ***Large Organizations***
   Large organizations can develop an internal database for the cyber risk cube and use it in your organization to share knowledge across departments.

2. ***Industry Organizations (ISACs, Foundations, Academic Organizations, etc.)***
   Industry organizations can develop data collection strategies and provide a version of the Cyber Risk Cube for members. The CRC databases will continue to collect information allowing for continuous learning and improvement, and new approaches and past experiences are evaluated by members.

3. ***Consulting Firms***
   Consulting firms can collect this information based on experience with clients and provide services that analyze approaches to new and developing cyber risk management implementations. An internal evaluation process will allow the firm to rate various tools and techniques, and cases. The Cube will help the firm provide advice to clients on their cyber risk maturity level and its practices compared to peers in the industry.

4. ***Governments and Non-Governmental Organization***
   Government and NGOs can use the Cube internally, similar to large organizations, and also provide services to its constituency that includes developing better approaches to cyber risk management. Governments and NGOs can analyze tools and techniques their stakeholders and vendors are using. They can also compare their vendors' cyber risk maturity level to vendors' peers when doing vendor risk assessments. Information from vendors and stakeholders can be collected to build the database to support the use of the Cube.

5. ***Small and Medium Enterprises (SMEs)***
   Small and medium-sized enterprises can leverage Government, NGO and Industry Organizations offering implementation of the Cyber Risk Cube to develop current and targeted approaches to cyber risk management. This can be extremely helpful as these organizations may have limited budgets for developing and implementing strategies. Simplifying the analysis phases and selecting a range of implementations can be a beneficial head start to SMEs, wanting to reduce their cyber risk exposure.

These are just a few of the many possible development approaches and uses of the Cyber Risk Cube.

VI. Conclusion

Cyber risk has become a significant challenge due to the growth of cybersecurity threats. All organizations must make advances in managing cyber risk. The Cyber Risk Cube tool presented in this paper decomposes cyber risk management into six components and provides companies with a guide to manage cyber risk. The tool also provides a platform for communicating about approaches to managing cyber risk. Moreover, it allows organizations to map to practical solutions in industry, including selecting tools and techniques and their implementation. It also allows for continuous improvement to keep up with the changes in the industry and regulations.

In order to facilitate its use, we provide a structure for the data needed to instantiate this tool. To demonstrate the applicability of the Cyber Risk Cube tool, we used existing case studies to contextualize this tool. Finally, we made suggestions about how different organizations may have varying approaches to developing and using the Cyber Risk Cube.

More research and systematic collection and evaluation of data can be valuable for identifying other factors that should be considered during the filtering process. At this stage, the factors we placed are the size and industry of an organization, rationale for performing cyber risk management, and budget constraints. A review system (scoring) is suggested to better select and evaluate approaches to cyber risk management. As we work with more organizations in developing implementations of the Cyber Risk Cube, we expect to gain additional insights and provide continuous improvement in cyber risk management.

Appendix A - Cases Narrative

1. Internal - Quantitative – Management

1.1 Large Financial Organization[32]

ID: 1

Company Name: LPL Financial

Filter Variables

Industry = Financial;
Size = Large;
Budget = N/A;
Rationale = Compliance;
Combination = #1 Internal-Quantitative-Management

Narrative

LPL Financial is a platform for independent financial analysts, with $615 billion in assets. Teams for enterprise and technology risk and audit had no consistent definitions, often interchanging terms for risk, threat, vulnerability and impact, so there was a need for consistent language.

LPL is using the RiskLens to make internal audits more effective and better communicate their results by merging the FAIR framework – Quantitative method – with Enterprise Risk Management. Every internal audit finding is run through RiskLens. FAIR prioritizes investments in risk management by measuring how much residual risk is reduced.

1.2 Large Bank[33]

ID: 2

Company Name: Investors Bank

Filter Variables

Industry = Banking;
Size = Large;
Budget = N/A;
Rationale = Compliance;
Combination = #1 Internal-Quantitative-Management

Narrative

The Investors Bank is a publicly traded, full-service bank that operates over 150 branches across New Jersey and New York. The Investors Bank decided to take compliance one-step further. It focuses on creating a culture of not only compliance but also resilient security to protect their customers, employees and partners. Hence, managing cyber risk efficiently and effectively is one of their challenges.

The bank uses Frontline VM, a vulnerability management software to perform the work of running scans, analyzing the results, generating reports, and providing

[32] https://www.fairinstitute.org/blog/fair-breakfast-case-study-lpl-financial-realigns-risk-management-around-fair-video

[33] https://w2k5c134qwx2vutib80kg2a7-wpengine.netdna-ssl.com/wp-content/uploads/2019/02/DigitalDefense-Investors-Bank-Case-Study-122818F.pdf

direct remediation planning guidance. The bank also establishes Key Risk Indicators (KRIs) and metrics to measure and manage risk.

1.3 Medium Technology Organization[34]

ID: 3
Company Name: Axcient, Inc.
Filter Variables
Industry = Technology;
Size = Medium;
Budget = N/A;
Rationale = Customer's requirements;
Combination = #1 Internal-Quantitative-Management
Narrative

Axcient, Inc. is a medium-sized United States-based data service organization with around 300 employees. Managed Service Providers (MSPs) use data backup and recovery solutions, like Axcient, to provide their customers with continuous access to business-critical services and information. If the cloud service provider experiences a data breach or leakage, the MSP is responsible for any of their customers' information impacted. Axcient manages cyber risk in order to fulfill their customer's requirement.

Axcient uses SecurityScorecard's security rating system to review performance and ensure that their continuous monitoring also leads to ongoing compliance for a strong security posture. To strengthen their cybersecurity culture, Axcient posts their daily security rating in the office, leading to staff taking greater care of cybersecurity.

2. *Internal - Quantitative – Measurement*

2.1 Large Technology Organization[35]

ID: 4
Company Name: Anonymous
Filter Variables
Industry = Technology;
Size = Large;
Budget = N/A;
Rationale = Compliance;
Combination = #2 Internal-Quantitative-Measurement
Narrative

A large technology organization turned to the RiskLens platform to address cyber risk assessment. The tech organization is subject to reporting to the Securities and Exchange Commission (SEC). In 2018, the SEC announced a guide to assist public companies in preparing disclosures about cybersecurity risks and incidents.

[34] https://securityscorecard.com/resources/case-study-axcient
[35] https://www.risklens.com/blog/case-study-tech-company-quickly-identifies-top-cyber-risks-with-quantitative-analysis/

The tech organization was only using qualitative heat maps before turning to the RiskLens platform when they quickly noticed that the qualitative approach wasn't enough to meet the SEC's requirement.

3. *Internal - Qualitative – Management*

3.1 Large Medical Center[36]

ID: 5

Company Name: University of Kansas Medical Center (KUMC)

Filter Variables

Industry = Healthcare;
Size = Large;
Budget = N/A;
Rationale = Compliance;
Combination = #3 Internal-Qualitative-Management

Narrative

The University of Kansas Medical Center (KUMC) is an Academic Health Center in Kansas City, Kansas with approximately 3,600 employees and 3,500 students. KUMC's Office of Information Security (OIS) is a relatively new department that formerly existed as a subunit of the IT Department.

The Information Security team at KUMC is using the Baldrige Cybersecurity Excellence Builder in conjunction with the NIST Cybersecurity Framework for self-assessment and program development. This process helped the team to better understand their own roles and to engage their customers in protecting the organization. This process has helped the Information Security Team establish a better approach to intake, response, and follow-up, improving stakeholder relationships and getting the right solutions to their customers.

3.2 Large Retail Organization[37]

ID: 6

Company Name: McColl's Retail Group

Filter Variables

Industry = Retail;
Size = Large;
Budget = N/A;
Rationale = Compliance;
Combination = #3 Internal-Qualitative-Management

Narrative

The McColl's Retail Group is a large retailer with over 18,652 employees and 1500 convenience stores and news agents across England, Scotland and Wales. Convenience retailer McColl needs to stay compliant with the Payment Cards Industry (PCI) regulations and thus, decided to find a suitable security solution to address cyber risk.

[36] https://www.nist.gov/cyberframework/success-stories/university-kansas-medical-center
[37] https://logrhythm.com/case-studies/uk-mccolls/

McColl’s Retail Group chooses to use this combination of the cyber risk cube by implementing the LogRhythm NextGen SIEM Platform. To ensure they stay compliant, the SIEM Platform can create personalized security alerts, helping McColl keep its high volumes of transactions safe.

3.3 Large Technology Organization[38]

ID: 7
Company Name: Alibaba Cloud
Filter Variables
Industry = Technology;
Size = Large;
Budget = N/A;
Rationale = Compliance;
Combination = #3 Internal-Qualitative-Management
Narrative

Alibaba Cloud is one of the world’s leading cloud computing service providers, and the leading cloud computing service provider in China, providing services for innovative enterprises and organizations around the world.Alibaba Cloud is committed to providing reliable, secure, and compliant cloud computing products and services. They need to stay compliant with more than 30 regulations, standards, framework, etc.

Alibaba Cloud has established a risk management framework to identify, analyze and manage risks within the organization and those related to services provided. The risk management framework involves management and various teams, and covers strategic and operational risks, such as security and availability. The comprehensive risk management system is created in accordance with the ISO27001:2013 Standard, which requires an information security risk assessment to be carried out annually.

The organization uses a qualitative risk assessment method that calculates risk rating for changes based on potential impact. Likelihood of occurrence is also computed to ensure more additional resources and control measures are dedicated to higher risks.

3.4 Large Bank[39]

ID: 8
Company Name: Standard Chartered PLC
Filter Variables
Industry = Banking;
Size = Large;
Budget = N/A;
Rationale = Compliance;

[38] http://alicloud-common.oss-ap-southeast-1.aliyuncs.com/Alibaba%20Cloud%20Security%20Whitepaper_v2_012017.pdf
[39] https://av.sc.com/corp-en/content/docs/risk-review-and-capital-review-2018.pdf

Combination = #3 Internal-Qualitative-Management
Narrative
Standard Chartered PLC is a large banking and financial services organization headquartered in London with more than 1,200 branches and outlets (including subsidiaries, associates and joint ventures) across over 70 countries, employing around 87,000 people. It is a universal bank with operations in consumer, corporate and institutional banking, and treasury services.

The Standard Chartered bank defines Information and Cyber Security (ICS) Risk as the potential for loss from a breach of confidentiality, integrity or availability of the bank's information systems and assets through cyber-attack, insider activity, error or control failure. Hence, they have been managing cyber risk.
In 2018, the bank approved a Risk Type Framework (RTF) to formally set out the Group-wide strategy for managing cyber risk. ICS Risk is managed through a structured ICS Policy Framework comprised of a risk assessment methodology and supporting policies, procedures and standards that are aligned to industry best practice models. The bank also monitors and reports on the risk appetite profile to ensure that performance which falls outside the approved risk appetite is highlighted and reviewed at the appropriate levels.

4. *Internal - Qualitative – Measurement*

4.1 Small Healthcare Clinic[40]

ID: 9
Company Name: Anonymous
Filter Variables
Industry = Healthcare;
Size = Small;
Budget = N/A;
Rationale = Compliance;
Combination = #4 Internal-Qualitative-Measurement
Narrative
This small healthcare clinic employs five people and uses eight stationary computing devices. A cloud service provider (CSP) is used as the primary method to handle roughly 1,600 patient ePHI records. The clinic has no dedicated IT personnel and so the owner took on all IT and security-related responsibilities. Since that information security risk assessments in the healthcare industry are legally required and demand an ongoing investment of time and resources, the small dental clinic decided to use the assessment tool recommended by the federal government(the SRA tool).

The clinic chooses to use measurement due to limited staff number by implementing an internal security system that included motion alarms and locks. The system was periodically tested to confirm it was in working order.

[40] http://www.micsymposium.org/mics_2017_proceedings/docs/MICS_2017_paper_7.pdf
https://repository.stcloudstate.edu/cgi/viewcontent.cgi?article=1084&context=msia_etds

The small dental clinic is using the Security Risk Assessment (SRA) Tool provided by HealthIT.gov to cover the main benchmarks required by law. This tool was chosen because it is recommended by the federal government for the healthcare industry.

5. *External – Quantitative – Measurement*

5.1 Large Financial Organization[41]

ID: 10
Company Name: Anonymous
Filter Variables
Industry = Financial;
Size = Large;
Budget = N/A;
Rationale = Compliance;
Combination = #5 External-Quantitative-Measurement
Narrative
This global financial firm is a leader in commercial banking with thousands of business partners around the world.

The firm shares sensitive data with thousands of partners around the world. They were assessing the security risk of their third-party business relationships with annual questionnaires and audits, but this was not enough to enable the level of risk-based decision making the organization made in other areas of their business.

Using BitSight Security Ratings for Third Party Risk Management, the firm receives timely, data-driven analysis of a partner's security effectiveness. New ratings are generated on a daily basis, giving organizations continuous visibility into the security of their assets so the firm doesn't have to rely on subjective responses in questionnaires.

5.2 Large Lending Cooperative[42]

ID: 11
Company Name: Farm Credit Mid-America
Filter Variables
Industry = Lending;
Size = Large;
Budget = N/A;
Rationale = Compliance;
Combination = #5 External-Quantitative-Measurement
Narrative

[41] https://info.bitsight.com/bitsight-case-study-global-financial-firm
http://cdn2.hubspot.net/hub/277648/file-2506331389-pdf/case_studies/BitSight_Financial_Services_Case_Study_3.pdf?hsCtaTracking=28d8494d-3a18-45bc-ad40-8e4a921bc0a7%7Ca059669e-8940-4cb8-abd2-65e1e869b061
[42] https://securityscorecard.com/resources/farm-credit

Farm Credit Mid-America is one of the largest agricultural lending cooperatives in the U.S. Farm Credit System, employing more than 1,100 people and serving more than 100,000 customers across Indiana, Ohio, Kentucky, and Tennessee The organization's vendors are not required to adhere to the same regulatory oversight so may have lower security standards. Farm Credit was relying on point in time assessments and questionnaires to review vendor risk, but that lead to ineffective resource allocation, inaccurate security data and limited visibility into security risks

Farm Credit now uses SecurityScorecard to monitor, and report on the cyber health of its own IT infrastructure via an outside-in view This enables Farm Credit to proactively assess all connected third-party vendor environments and gain visibility into the organization's ecosystem risk.

6. *External – Quantitative – Management*

6.1 Large Healthcare Non-profit Organization[43]

ID: 12
Company Name: Children's Hospital of Minnesota
Filter Variables
Industry = Healthcare;
Size = Large;
Budget = N/A;
Rationale = Compliance;
Combination = #6 External-Quantitative-Management
Narrative
Children's Hospital of Minnesota is a largest healthcare non-profit in the United States, with two hospitals.

The organization was looking into selecting a security benchmark and policy that is meaningful and then sourcing the information to measure against that benchmark. Using the SecurityScoreCard platform, the CISO could frequently pull information on hospital systems in Boston, Seattle, Texas, and Colorado and see how their scores compared to Children's Minnesota in one comprehensive view.

6.2 Large institutional investment network [44]

ID: 13
Company Name: Liquidnet
Filter Variables
Industry = Financial;
Size = Large;
Budget = N/A;
Rationale = Compliance;

[43] https://s3.amazonaws.com/ssc-corporate-website-production/documents/resources/ChildrensMN-Case-Study-c04-1.pdf
[44] https://s3.amazonaws.com/ssc-corporate-website-production/documents/resources/Liquidnet-Case-Study-c03.pdf

Combination = #6 External-Quantitative-Management

Narrative

Liquidnet is the global institutional trading network where the world's top asset managers, managing over 15 trillion dollars in assets, come to execute their large equity trades. Liquidnet was relying on self-reported information provided by the vendors but needed to insure they were complying with third-party review requirements of customers and regulators. With SecurityScorecard Liquidnet could quantify the security performance of their vendors and provide continuous monitoring. The alternative to using SecurityScorecard for Liquidnet would have been to hire more employees in an attempt to make vendor assessments more frequent and more accurate, an expensive investment that could not come close to the capabilities of using a continuous monitoring platform.

7. *External – Qualitative – Management*

7.1 Blackstone[45]

ID: 14

Company Name: Blackstone

Filter Variables

Industry = Financial;
Size = Large;
Budget = N/A;
Rationale = Efficiency;
Combination = #7 External-Qualitative-Management

Narrative

Blackstone is an alternative investment management and financial services firm. It specializes in private equity, credit, and hedge fund investment strategies. Blackstone's third-party risk management programs relied on phone calls and spreadsheets, but this caused problems as the number of vendors grew and the number of different methodologies each used. Using CyberGRX's platform, Blackstone could develop a more efficient risk management program that helps them prioritize risk. Realizing the quantitative aspect of ranking vendors by risk is not enough, they also engage in risk-based discussions with vendors and business partners to gather qualitative data and assess how to mitigate risk.

8. *External – Qualitative – Measurement*

8.1 Large Technology Organization[46]

ID: 15

Company Name: Alibaba Cloud

Filter Variables

Industry = Technology;
Size = Large;
Budget = N/A;
Rationale = Compliance;

[45] https://www.cybergrx.com/blackstone-case-study/

[46] http://alicloud-common.oss-ap-southeast-1.aliyuncs.com/Alibaba%20Cloud%20Security%20Whitepaper_v2_012017.pdf

Combination = #7 External-Qualitative-Measurement

Narrative

Alibaba Cloud is one of the world’s leading cloud computing service providers, and the leading cloud computing service provider in China, providing services for innovative enterprises and organizations around the world.

Alibaba Cloud is committed to providing reliable, secure, and compliant cloud computing products and services. They need to stay compliant with more than 30 regulations, standards, framework, etc. For external view of the third parties’ risk level, they regularly complete third-party audits. The organization uses a qualitative risk assessment method which calculates risk rating for changes based on potential impact. Likelihood of occurrence is also computed to ensure more additional resources and control measures are dedicated to higher risks.

Appendix B - Tools and Techniques[47]

1. **Internal**

1.1 Yearly Internal Security Audit

ID: 1
Component: Internal
Technique/Tool name: Yearly Internal Security Audit
Technique/Tool info: Internal Audit is the 3rd Line of Defense, which independently assess cyber risk management program effectiveness, report it to the board.

1.2 Self-assessment

ID: 1
Component: Internal
Technique/Tool name: Self-assessment
Technique/Tool info: A self-assessment tool to help organizations better understand the effectiveness of their cybersecurity risk management efforts.

1.3 Control for external assessment

ID: 1
Component: Internal
Technique/Tool name: Control for external assessment
Technique/Tool info: It can be used to reduce the internal view of the organization's cyber risk.

2. **External**

2.1 Onsite/Offsite Vendor Audit

ID: 2
Component: External
Technique/Tool name: Onsite/Offsite Vendor Audit
Technique/Tool info: When organizations want to understand third parties' cyber risk level, they can perform vendor audit to identify, monitor, and audit their preparedness.

2.2 US Treasury OCC: Third-Party Relationships – Risk Management Guidance

ID: 2
Component: External
Technique/Tool name: US Treasury OCC: Third-Party Relationships – Risk Management Guidance
Technique/Tool info: This provides guidance to national banks and federal savings associations (collectively, banks) for assessing and managing risks associated with third-party relationships.

2.3 Due Diligence

ID: 2
Component: External
Technique/Tool name: Due Diligence
Technique/Tool info: An organization should have a process to evaluate the current threat landscape and identify the bad actors – external and internal – that might target the parties in the transaction. This landscape can vary by industry or

[47] This is a very limited set of examples which are used in the paper.

region, and higher risk transactions – such as organizations in certain countries or in sectors that have suffered recent attacks – require greater diligence.

3. **Qualitative**

3.1 FFIEC Cybersecurity Assessment Tool (CAT)[48]

ID: 3
Component: Qualitative
Technique/Tool name: FFIEC Cybersecurity Assessment Tool (CAT)
Technique/Tool info: The Assessment provides a repeatable and measurable process for institutions to measure their cybersecurity preparedness over time.

3.2 OSFI Cyber Security Self-Assessment[49]

ID: 3
Component: Qualitative
Technique/Tool name: OSFI Cyber Security Self-Assessment
Technique/Tool info: This self-assessment template sets out desirable properties and characteristics of cyber security practices that could be considered by a FRFI when assessing the adequacy of its cyber security framework and when planning enhancements to its framework.

3.3 FSSCC Cybersecurity Profile[50]

ID: 3
Component: Qualitative
Technique/Tool name: FSSCC Cybersecurity Profile
Technique/Tool info: The Profile is a scalable and extensible assessment that financial institutions of all types can use for internal and external (i.e., third party) cyber risk management assessment and as a mechanism to evidence compliance with various regulatory frameworks (a "common college application for regulatory compliance") both within the United States and globally.

3.4 ICSCERT – Cyber Security Evaluation Tool (CSET)[51]

ID: 3
Component: Qualitative
Technique/Tool name: ICSCERT – Cyber Security Evaluation Tool (CSET)
Technique/Tool info: CISA assessment products improve situational awareness and provide insight, data, and identification of control systems threats and vulnerabilities. Core assessment products and services include self-assessments using the Cybersecurity Evaluation Tool (CSET®), onsite field assessments, network design architecture reviews, and network traffic analysis and verification. The information gained from assessments also provides stakeholders with the understanding and context necessary to build effective defense-in-depth processes for enhancing cybersecurity.

3.5 HKMA – Cyber Resilience Assessment Framework Tool (CRAF)[52]

ID: 3
Component: Qualitative

[48] https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017_All_Documents_Combined.pdf

[49] http://www.osfi-bsif.gc.ca/eng/fi-if/in-ai/pages/cbrsk.aspx

[50] https://fsscc.org/Financial-Sector-Cybersecurity-Profile

[51] https://www.us-cert.gov/ics/Assessments

[52] https://www.hkma.gov.hk/media/eng/doc/key-information/speeches/s20160518e2.pdf

Technique/Tool name: HKMA – Cyber Resilience Assessment Framework Tool (CRAF)
Technique/Tool info: It can be used to determine the inherent riskiness of an institution.

3.6 Building Security in Maturity Model (BSIMM)[53]
ID: 3
Component: Qualitative
Technique/Tool name: Building Security in Maturity Model (BSIMM)
Technique/Tool info: An effective tool for understanding how organizations of all shapes and sizes, including some of the most advanced security teams in the world, are executing their software security strategies.

4. **Quantitative**

4.1 Factor Analysis of Information Risk (FAIR)
ID: 4
Component: Quantitative
Technique/Tool name: Factor Analysis of Information Risk (FAIR)
Technique/Tool info: It provides information risk, cybersecurity and business executives with the standards and best practices to help organizations measure, manage and report on information risk from the business perspective.

4.2 BCG Cyber Doppler
ID: 4
Component: Quantitative
Technique/Tool name: BCG Cyber Doppler
Technique/Tool info: BCG's Cyber Doppler tool builds on this insight, enabling companies to better understand their cyber risks and controls. It quantifies the likelihood of a cyber-attack occurring as well as the impact of a successful attack.

4.3 Aggregate reporting using risk appetite and Loss Exceedance Curves (LEC)
ID: 4
Component: Quantitative
Technique/Tool name: Aggregate reporting using risk appetite and Loss Exceedance Curves (LEC)
Technique/Tool info: It can be used to assess and report on existing risk visibility and operations metrics.

4.4 Cybersecurity Argument Graph Evaluation (CyberSAGE)
ID: 4
Component: Quantitative
Technique/Tool name: Cybersecurity Argument Graph Evaluation (CyberSAGE)
Technique/Tool info: CyberSAGE can combine numerical information to compute quantitative security assessment results.

4.5 Lucideus – Security Assessment Framework for Enterprise (SAFE)
ID: 4
Component: Quantitative
Technique/Tool name: Lucideus – Security Assessment Framework for Enterprise (SAFE)

[53] https://www.bsimm.com

Technique/Tool info: An Enterprise Wide, Objective, Unified, Real Time Cyber Risk Quantification (CRQ) platform which incorporates both technical & business aspects with an output for prioritized decision making.

4.6 BitSight's Security Ratings Platform[54]

ID: 4
Component: Quantitative
Technique/Tool name: BitSight's Security Ratings Platform
Technique/Tool info: It can be used to make data-driven decisions to reduce cyber risk.

4.7 UpGuard[55]

ID: 4
Component: Quantitative
Technique/Tool name: UpGuard
Technique/Tool info: It can continuously improve the organization's cybersecurity rating, detect data exposures, and control third-party risk.

4.8 SecurityScoreCard[56]

ID: 4
Component: Quantitative
Technique/Tool name: SecurityScoreCard
Technique/Tool info: Enable security and risk management teams to reduce vulnerabilities before attackers can exploit them.

5. **Measurement**

5.1 KPI conducted yearly/quarterly to track and manage cyber risk

ID: 5
Component: Measurement
Technique/Tool name: KPI
Technique/Tool info: Key performance indicators (KPIs) are an effective way to measure the success of the organization's cybersecurity program and aid in decision-making.

5.2 Periodic security goal evaluation

ID: 5
Component: Measurement
Technique/Tool name: Periodic security goal evaluation
Technique/Tool info: Organization can conduct security goal evaluation periodically to measure cyber risk.

6. **Management**

6.1 KPI conducted monthly/weekly to track and manage cyber risk

[54] https://www.bitsight.com

[55] https://www.upguard.com/?utm_campaign=Brand&utm_term=upguard&utm_source=adwords&utm_medium=ppc&hsa_mt=e&hsa_net=adwords&hsa_grp=61484095426&hsa_cam=1627240041&hsa_acc=1646746353&hsa_src=g&hsa_ver=3&hsa_ad=355114848909&hsa_tgt=kwd-552012141597&hsa_kw=upguard&gclid=CjwKCAjw8pH3BRAXEiwA1pvMsWeJ4SBWYMkWipq0tD0VCIB2ndwxf1W7aNmxuAGXBCQ6puM2gqk6xxoCT4AQAvD_BwE

[56] https://securityscorecard.com/request-a-securityscorecard-demo?utm_source=google&utm_medium=cpc&ad_id=412034285187&campaign_id=8675572763&utm_campaign=Branded&utm_content=Core&utm_term=Demo

ID: 6
Component: Management
Technique/Tool name: KPI
Technique/Tool info: Key performance indicators (KPIs) are an effective way to measure the success of the organization’s cybersecurity program and aid in decision-making.

6.2 Security Information and Event Management (SIEM) tools used daily for cyber risk management
ID: 6
Component: Management
Technique/Tool name: SIEM tools
Technique/Tool info: It can be used to review log and event data from a business' networks, systems and other IT environments, understand cyber threats, cyber risk and prepare accordingly.