We declare that we have completed this assignment in accordance with the UAB Academic Integrity Code and the UAB CS Honor Code. We have read the UAB Academic Integrity Code and understand that any breach of the Code may result in severe penalties. We also declare that the following percentage distribution faithfully represents individual group members' contributions to the completion of the assignment.

Name	Overall Contribution(%)	Major work items completed by me	Signature/Initials	Date
Shruti Azhagu Mani	16.5	4. Framework Components	shruti	03/24/2024
Swetha Julakanti	16.5	5.Steps(5.1,5.2,5.3,5.4) and 7.Disadvantages	swetha	03/24/2024
Harika Neelam	16.5	6. Advantages 8. Summary and 9.Conclusion	harika	03/24/2024
Rohit Panaganti	16.5	8. Summary	Rohit	03/24/2024
Chandana Chennayagunta	16.5	5. Steps (5.5, 5.6, 5.7)	chandana	03/24/2024
Shouzab Khan	16.5	1. Introduction, 2. Background, 3. Previous Work, 10.References	Shouzab	03/24/2024

FAIR Cybersecurity Framework

1 Introduction:

MSPs, or managed services providers, face a significant challenge in the modern business world. The data that MSPs' clients depend on to run their businesses is always being targeted by malicious actors. Most of the time, these clients are unaware of these risks and believe their MSP is taking care of everything. However, the client and the MSP are equally accountable for maintaining security. MSPs must put a lot of effort into educating people about cybersecurity and integrating it deeply into their operations to address this. They must ensure that their policies, procedures, resources, and plans for handling cybersecurity-related issues are all clear. According to the SecurityMagazine website, using a framework can simplify planning and make it easier for MSPs to instruct others in cybersecurity. It can also help them determine exactly what they need to do. Using a framework entails adhering to a set of guidelines and procedures that are accepted by all. Businesses may increase revenue due to improved organization and efficiency. It's like having a universal language that everyone speaks when interacting with clients and within the organization. By using a framework, you can ensure that both you and your clients have the same definition of "good," which will facilitate collaboration and help you meet everyone's expectations. Organizations can examine and manage information risk more thoroughly with the help of the FAIR framework, which emphasizes consistency, integration with other frameworks, loss exposure estimation, factor breakdown, quantitative analysis, scenario-based assessment, and continuous improvement.

A cybersecurity framework functions similarly to a set of guidelines and best practices for maintaining the online safety of your company. Its purpose is to control the hazards associated with digital technology use. You can affordably, intelligently, and adaptably safeguard your company by adhering to this framework. But cybersecurity is more than just being safe. It might also support the expansion of your company. For instance, you can ensure that your company can continue operating even in the event of an attack or hardware malfunction by utilizing the framework to set up local, offline, and cloud backups. Setting up these safeguards for your clients may require more work on your part as an MSP. According to the SecurityMagazine website, the FAIR framework, which stands for Factor Analysis of Information Risk, assists organizations in assessing and evaluating cybersecurity risk. Like a tool, it lets businesses determine the likelihood and severity of potential cyberattacks. This assists them in making well-informed decisions regarding the prevention or remediation of these attacks. A business using FAIR begins by enumerating and classifying everything that is significant and subject to risk, such as computer systems or data. The unique feature of FAIR is that it assigns a monetary value to these risks. As a result, companies can see exactly how much

money they stand to lose in the event of a problem. It helps them decide what actions to take to protect themselves in a way that makes sense financially. FAIR gives organizations a more sophisticated understanding of risk factors and helps them to efficiently prioritize mitigation efforts by putting risk into monetary terms and analyzing specified risk scenarios. By integrating it with other frameworks, organizations can align with industry best practices, and its standardized approach guarantees consistency and comparability across assessments.

2 Background:

FAIR is a method for managing cybersecurity threats. Early in the new millennium, Jack Freund and Jack Jones created it. Jack Jones has extensive experience in information security and has worked for a long time with risk management. He created FAIR in response to the need for an improved approach to quantifying and managing cybersecurity risks. Risks and their financial impact are examined in FAIR. It aids in the comprehension, assessment, and quantification of the financial risks that organizations encounter. This aids in their decision-making about how best to allocate their resources to mitigate these risks. According to the RSIsecurity website, FAIR is a popular risk management tool used by a wide range of industries and businesses. As more people gain knowledge about cybersecurity threats and how to counter them, it always gets better. Jones wanted to give organizations a better knowledge of their information risks by introducing a standardized and structured approach called FAIR. Organizations can allocate resources for risk mitigation and management more intelligently when they use FAIR, as it provides a financial measure of these risks. Over time, FAIR has become more widely accepted and recognised in a variety of sectors and industries. It is a useful tool for businesses looking to strengthen their cybersecurity posture because of its methodical approach and emphasis on quantification. With constant updates and improvements, FAIR keeps changing to reflect new discoveries about cybersecurity threats and difficulties.

The FAIR framework is a tool for calculating and interpreting financial risk. FAIR provides an accurate estimate of the amount of money you could lose, in contrast to other approaches that only indicate whether a risk is high, medium, or low. In summary, FAIR's main function is to estimate the probability of a negative event occurring and its potential severity. It does this by analyzing two variables: the likelihood of a negative event occurring (such as a cyberattack) and the potential financial loss. To make these easier to understand, FAIR breaks them down into smaller components. For instance, it examines the likelihood of success and the frequency with which someone might attempt to attack your company. It also considers how something going wrong could result in financial loss, such as reduced productivity or fines. According to the CiseSecurity website, risks can be effectively quantified using FAIR, using

monetary values as examples. Knowing exactly how much money you could lose in the event of an adverse event allows you to make more informed decisions. You may make long-term financial plans and decisions with the help of these figures. You can assess risks and determine which are most serious by comparing them using FAIR. This implies that you can concentrate your resources on repairing the issues that have the greatest potential to cause harm. Financial instruments facilitate the explanation of risk to individuals who may lack extensive knowledge of technology. It makes things safer for everyone and explains why fixing them is crucial. In order to ensure strong and proactive risk management strategies, FAIR's emphasis on continuous improvement encourages organizations to modify and evolve their risk management practices in response to shifting threats and business requirements.

3 Previous Work:

Businesses are becoming more and more flexible in how they address operational risk and cybersecurity. They need more than just following the rules to be safe. They understand that to truly protect themselves, they must concentrate more on risk management. Nowadays, companies view cyber risk as a serious issue, not just something to worry about for techies. This is because a lot of what businesses do now depends on digital systems. Risk and security professionals must strike the right balance between ensuring the company's continued operational viability and safety. They must assist all parties in comprehending how to control risk while maintaining the efficiency of the company. There has been a lot of previous work done in the form of methodologies, theories and relevant studies for the FAIR risk framework. According to the FAIR Institute website, authors David Sheronas and Micheal Radigan have explained that organizations can use the FAIR model as a framework to measure and consistently systematically manage information risk. Sheronas and Radigan talk about how businesses can evaluate the different elements that contribute to information risk by efficiently using the FAIR model. This entails assessing the probability that various threats will materialize as well as calculating the possible financial impact or repercussions of these threats. The writers offer directions on how entities can collect pertinent data and information to incorporate into the FAIR model, along with the methods for carrying out the essential examinations to extract significant understanding from the outcomes. They go over the difficulties and practical issues that organizations might run into when implementing the plan, as well as solutions to these problems. Sheronas and Radigan draw attention to the advantages of applying the FAIR model to information risk management, including the ability to better inform decision-making, give a common vocabulary and framework for discussing and ranking risks, and match risk management initiatives with corporate goals.

The FAIR framework can be applied to cloud services for risk management and security as well. In the paper “FAIR: A Framework for Risk Management for Cloud Service Providers" written by Edgar Weippl and Christoph Wegener, the authors discuss that the FAIR framework can be used by cloud service providers to assess and manage the risks associated with their offerings. They could go over the various issues they have with controlling risk in cloud computing, such as protecting data, adhering to regulations, and determining who oversees what. The authors offer suggestions on how cloud service providers should modify the FAIR framework to address these issues. They can assist them in determining the significance of each risk and the appropriate course of action. For instance, they may discuss topics like service outages, which occur when a cloud service is unavailable for a while, or data breaches, which occur when information is disclosed without authorization. A report written by authors Charles Kalodgy and Doug Cahill and published by the Enterprise Strategy Group states that the FAIR model can help businesses recognize and manage cybersecurity risks. They discuss various aspects of cybersecurity risk, such as the likelihood of a threat and its potential impact on an organization. The authors offer guidance on how businesses can quantify and prioritize cybersecurity risks using the FAIR model. They advise on how to obtain data, examine potential dangers, and estimate the financial impact of a security issue. Furthermore, Kolodgy and Cahill exchange concepts regarding how businesses can apply the FAIR model to determine where and what to prioritize when it comes to cybersecurity spending. The development, industry adoption, training initiatives, research endeavors, framework integration, and creation of auxiliary tools and resources are all included in the earlier work on the FAIR cybersecurity framework.

Based on the provided document, the content for the specified sections about the FAIR Cybersecurity Framework's components, implementation tiers, core framework, profiles, and each of the five key functions (Identify, Protect, Detect, Respond, Recover) can be outlined as follows:

4. Framework Components

The FAIR (Factor Analysis of Information Risk) Cybersecurity Framework offers a structured and quantitative approach to managing cybersecurity risks. This framework enables organizations to calculate and interpret the financial impact of cybersecurity threats, providing a clear basis for risk management decisions.

4.1 Implementation Tiers

The FAIR framework does not explicitly outline "Implementation Tiers" as found in other frameworks like NIST. However, it emphasizes a maturity model approach where organizations can gradually improve their risk management processes. The progression involves moving from qualitative to quantitative risk assessments, enhancing data quality, and refining risk models over time.

4.2 Framework Core

The core of the FAIR framework comprises a unique approach to risk analysis that breaks down into the following components:

4.2.1 Identify

This component involves identifying critical assets, threats, and vulnerabilities within the organization's infrastructure. FAIR emphasizes the significance of enumerating and classifying everything that is at risk, laying the foundation for a comprehensive risk assessment process.

4.2.2 Protect

Protection in the FAIR model involves implementing measures to mitigate the likelihood or impact of cybersecurity threats. Although FAIR is primarily a tool for risk assessment and quantification, it guides organizations in prioritizing protective measures based on financial impact.

4.2.3 Detect

The detection phase under FAIR involves monitoring and identifying potential cybersecurity events that could threaten organizational assets. This includes the analysis of threat likelihood and frequency, aiding in the prioritization of detection capabilities.

4.2.4 Respond

Response strategies in the FAIR framework are informed by the quantitative analysis of risk. By understanding the potential financial impact of cybersecurity incidents, organizations can develop effective response plans that minimize losses and restore normal operations.

4.2.5 Recover

Recovery focuses on restoring services and capabilities that were impaired by a cybersecurity event. The FAIR framework's quantification of risk assists organizations in planning and prioritizing recovery efforts to minimize financial losses and operational disruptions.

4.3 Profiles

The FAIR framework uses profiles to categorize and analyze different risk scenarios and outcomes. These profiles help organizations understand the range of potential impacts from various threats, enabling them to make informed decisions about risk mitigation and management strategies. Profiles in FAIR can be tailored to specific organizational needs, considering different asset types, threat actors, and potential loss scenarios.

5 STEPS

One of the best approaches for managing cybersecurity risk is the FAIR (Factor Analysis of Information Risk) framework, which offers seven suggested steps for creating a strong cybersecurity risk management program. To improve the cybersecurity framework's

implementation, it is suggested that these procedures be repeated on a regular basis. It's crucial to remember that the FAIR cybersecurity framework is optional, and these actions are meant to help firms create their own cybersecurity frameworks. I'll go over the seven stages that FAIR suggests doing to put their cybersecurity strategy into practice below.

5.1 Step 1: Establish Objectives and Scope

Organizations define their broad business goals and priorities at the first stage of the FAIR framework implementation, which establishes the parameters for the range of cybersecurity initiatives. This comprises a comprehensive analysis to pinpoint vital resources, systems, and particular organizational areas where cybersecurity efforts will be focused. Clearly defining goals at the outset helps firms make sure that they are in line with the enterprise's top priorities. This procedure not only helps to create a targeted strategy for cybersecurity, but it also makes it easier to allocate resources to protect the most important systems and assets. Organizations can also customize their cybersecurity strategy to address demands and obstacles by knowing the business goals, which improves overall resilience. By taking a proactive stance, organizations may strategically install cybersecurity solutions to better manage risks and defend against possible threats. In the end, defining goals and scope is crucial to the FAIR framework's successful application since it offers a path for efficient risk management that is in line with corporate objectives.

5.2 Step 2: Understand Regulatory Requirements and Risk Management Approach

It's critical to confirm and fully grasp the regulatory duties controlling the industry and geographic area in which the organization works during the period of comprehending regulatory requirements and designing the organization's risk management approach. This entails a thorough analysis of all relevant laws, rules, and industry standards to guarantee complete compliance and adherence to legal requirements. Organizations can reduce the risk of non-compliance and related penalties by developing a strong foundation for risk management processes that are compliant with legal requirements by comprehending these regulatory duties. Determining the organization's overall approach to risk management, including its position on risk tolerance, mitigation techniques, and risk assessment methodology, is another task included in this step. Organizations can promote consistency and coherence in their efforts to detect, evaluate, and reduce risks across the enterprise by creating a defined risk management methodology. This stage lays the foundations for the identification of vulnerabilities and possible threat scenarios, which is a crucial component of the FAIR framework implementation. In the end, a solid grasp of regulatory requirements and a clearly defined strategy to risk management establish the foundation for efficient risk mitigation tactics and strengthen the organization's resistance to new threats.

5.3 Step 3: Assess Current Risk Management Practices

Organizations start compiling a comprehensive profile of their present risk management procedures in the third stage of the FAIR framework implementation process. This procedure, which makes use of FAIR's profiling components, entails carefully outlining the results attained by the company's current risk management system. Organizations create a baseline through this assessment, which makes it possible to identify the advantages and disadvantages of their present risk management strategy. This thorough analysis clarifies how well-suited current tactics are for reducing information threats and safeguarding vital resources. Moreover, it facilitates the identification of areas in which processes, resources, or technology require enhancement by businesses. Organizations can use FAIR's methodology to make better data-driven decisions by gaining insights into the quantitative parts of their risk picture. In the end, this evaluation is an essential first step toward improving the organization's overall readiness and resilience against changing cybersecurity threats. Organizations can effectively enhance their risk management capabilities by prioritizing activities and strategically allocating resources by having a thorough awareness of present practices.

5.4 Step 4: Conduct Detailed Risk Assessment

During the fourth phase of FAIR framework implementation, companies carry out an extensive risk assessment procedure that is based on the FAIR methodology. To find possible threats, weaknesses, and dangers, this entails a careful analysis of the operating environment, historical evaluations, and current risk management procedures. Employing the methodical framework of FAIR, entities can measure these hazards in monetary terms, offering a more precise evaluation of their possible influence on the enterprise. The purpose of this assessment is to find areas of vulnerability and possible exposure to cyber-attacks by examining several facets of the organization's systems, procedures, and infrastructure. Organizations can learn more about the possibility of different cybersecurity events happening as well as the possible impact size by conducting a thorough investigation. Organizations can prioritize risk mitigation activities according to their potential cost-effectiveness and alignment with strategic objectives by evaluating risks in terms of dollars and cents. Furthermore, by proactively addressing vulnerabilities prior to their escalation into severe security events, this assessment enables businesses to deploy resources more efficiently and forms the basis for the development of effective risk management strategies. All things considered, carrying out a thorough risk assessment based on the FAIR methodology gives enterprises the ability to make wise decisions and better safeguard their assets from online threats.

5.5 Step 5: Define Desired Outcomes and Goals

Defining the intended results and goals comes next, organizations translate the insights gained from their risk assessment into actionable goals and outcomes. It's not enough to merely understand the risks; organizations must also define what success looks like in terms of cybersecurity. This involves setting specific, measurable, achievable, relevant, and time-bound

(SMART) objectives that align with the organization's overall risk management strategy. For example, desired outcomes could include reducing the frequency of security incidents by a certain percentage, minimizing financial losses from cyber threats, or enhancing the overall resilience of the organization's cybersecurity posture. By defining these outcomes, organizations can effectively prioritize their efforts and allocate resources where they are needed most. Moreover, setting quantifiable goals enables continuous monitoring and evaluation of progress, ensuring that cybersecurity initiatives remain aligned with the organization's overarching objectives.

5.6 Step 6: Identify and Prioritize Gaps

Once the desired outcomes and goals are established, the organization must identify and prioritize any gaps in its current cybersecurity posture. This involves comparing the results of the risk assessment to the targeted outcomes and identifying areas where improvements are needed. These gaps could include deficiencies in security controls, weaknesses in existing policies and procedures, or high-risk areas requiring additional attention. It's essential to prioritize these gaps based on their potential impact on organizational goals and the resources required to address them effectively. By doing so, organizations can ensure that limited resources are allocated efficiently to address the most critical security gaps and mitigate the highest-priority risks. This step lays the groundwork for developing a focused and effective action plan to strengthen the organization's cybersecurity defenses.

5.7 Step 7: Implement Action Plan and Monitor Progress

With identified gaps prioritized, the organization proceeds to develop and execute an action plan to address them. This action plan should outline specific tasks, deadlines, and responsible individuals or teams for each identified gap. By breaking down the remediation process into manageable steps, organizations can ensure systematic progress towards strengthening their cybersecurity posture. Additionally, continuous monitoring and assessment of progress are essential to tracking the effectiveness of implemented measures. Regular evaluations of the action plan allow for necessary adjustments in response to emerging risks, changes in the organization's risk landscape, or insights gained from past endeavors. This iterative approach to cybersecurity risk management ensures that the organization remains proactive in addressing new threats and continuously improves its security posture to adapt to evolving challenges. Overall, implementing an action plan based on prioritized gaps ensures that cybersecurity efforts are targeted, efficient, and aligned with the organization's strategic objectives.

6 ADVANTAGES:

We have a number of advantages with the FAIR approach when handling cybersecurity risks in organizations. First of all, FAIR offers a methodical and structured way to evaluate and control risks. Organizations may efficiently identify, evaluate and rank cybersecurity threats by following a clear methodology which promotes more informed decision-making.

The FAIR framework ability to put cybersecurity concerns into financial constraints is one of its primary features. Organizations can also prioritize risk mitigation activities according to the possible cost-effectiveness of various techniques due to this financial scale.It makes it possible for companies to assign a value to many risk factors including the potential for financial harm due to a cyberattack.By evaluating risks in this way organizations can gain a better understanding of the possible effects of cyber threats on their operations

Furthermore, by offering a defined methodology FAIR encourages comparability and consistency in risk evaluations.Organizations can guarantee that risk assessments are uniform among several departments or companies by following a standard set of rules and procedures.Better coordination and communication amongst everyone involved in controlling cybersecurity threats are made possible by this standardization.

FAIR offers a language and structure for addressing cybersecurity threats that is generic. This strategy improves communication between many stakeholders, including risk managers and IT specialists. FAIR aids in a better understanding of the possible effects of cyber risks on the company through the use of appropriate vocabulary and techniques, resulting in more productive teamwork and risk-reduction strategy decision-making.

Additional advantages are the scalability and flexibility of the FAIR framework. FAIR provides an orderly method for risk assessment and allows businesses to modify the framework to their own needs.Because of its adaptability which enables companies to scale it to fit their particular risk profiles and work situations, the framework is appropriate for enterprises of all sizes. The FAIR framework gives companies a practical tool for managing cybersecurity risks with the implementation of a methodical approach, financial computation, consistency, and scalability. FAIR improves cybersecurity and helps companies in selecting sensible risk-reduction strategies.

7 DISADVANTAGES:

The FAIR framework has some drawbacks even though it provides a methodical and structured way to measure and manage cybersecurity threats. The difficulty of implementation and understanding is one major drawback. FAIR necessitates a thorough comprehension of risk analysis principles and procedures, which can be difficult for organizations with little resources or specialized knowledge. The intricacy of the methodology could lead to erroneous

interpretation of the findings or uneven implementation, weakening its ability to precisely evaluate and rank hazards.

The FAIR framework's dependence on arbitrary inputs and presumptions is another drawback. Making educated assumptions or estimations based on the information at hand and the expertise of others is sometimes required when quantifying elements like loss event frequency, threat capability, and control strength. Subjectivity adds a degree of unpredictability and uncertainty to risk assessments, which could provide biased or incorrect conclusions. Furthermore, the quality and dependability of the data used—which can be challenging to collect or validate in real-world scenarios—have a major impact on how accurately FAIR calculates risks.

Furthermore, the complexity and interconnectivity of contemporary cybersecurity threats and environments may be beyond the scope of the FAIR framework. Cyber hazards are dynamic and ever-changing, involving a wide range of interrelated factors such as organizational, technological, and human components. The non-financial effects of cyber-attacks, such as reputational harm, fines from authorities, or operational disruptions, may go unnoticed by FAIR because of its emphasis on financial quantification. Furthermore, the framework's focus on risk monetization may cause one to ignore qualitative factors or intangible risks that are difficult to quantify.

Apart from the intricacies of execution, subjectivity in evaluating risks, and possible neglect of non-financial effects, the FAIR framework encounters obstacles with expandability and flexibility. It can be difficult and resource-intensive to scale the FAIR technique to large, diversified organizations with intricate IT systems and different risk profiles. Companies may find it difficult to implement FAIR consistently across divisions, business units, or geographical areas, which could lead to disjointed risk management procedures. Furthermore, FAIR's ability to evolve and stay relevant may be outpaced by the speed at which cyber threats and technology are emerging. There could be gaps in risk coverage or out-of-date risk assessments if the framework is unable to keep up with new attack vectors, expanding regulatory requirements, and developing cyber hazards. As a result, even while FAIR gives businesses a useful tool for ranking and evaluating cybersecurity threats, its drawbacks should be carefully addressed and balanced out with other strategies to guarantee thorough risk management.

8 SUMMARY:

The FAIR (Factor Analysis of Information Risk) Framework offers organizations a structured and quantitative approach to managing cybersecurity risks. FAIR focuses on assessing the financial impact of cybersecurity threats and providing a clear basis for risk management decisions. FAIR does not explicitly outline implementation tiers like the NIST framework but emphasizes a maturity model approach enabling organizations to gradually improve their risk management processes.

The core components of the FAIR framework include identifying critical assets, threats, vulnerabilities and protective measures and these components align with the five key functions of cybersecurity risk management which are Identify, Protect, Detect, Respond and Recover. FAIR utilizes profiles to categorize and analyze different risk scenarios and outcomes with helping organizations understand potential impacts and prioritize mitigation strategies.

The implementation steps of the FAIR framework involve establishing objectives and scope, understanding regulatory requirements, assessing current risk management practices, conducting detailed risk assessments, defining desired outcomes and goals, identifying and prioritizing gaps, and implementing action plans while monitoring progress.

Advantages of the FAIR framework include its methodical and structured approach to risk evaluation, financial quantification of risks, scalability, flexibility, and encouragement of comparability and consistency in risk evaluations. However, challenges include complexity, subjectivity, and potential limitations in addressing non-financial impacts and evolving cyber threats. Overall, the FAIR framework provides organizations with a practical tool for managing cybersecurity risks, though careful consideration of its complexities and limitations is necessary for effective implementation and risk management.

9 CONCLUSION

This paper provides a detailed examination of the FAIR (Factor Analysis of Information Risk) Cybersecurity Framework. Section 1 introduces the FAIR framework providing insights into its origins and the development. Section 2 is about the background information and creation process of the FAIR framework. Section 3 discusses previous academic work regarding the implementation and effectiveness of the FAIR cybersecurity framework, offering insights into its real-world applications and outcomes.

Section 4 provides the detailed exploration of the components comprising the FAIR framework, emphasizing its structured approach to risk analysis and management. This section outlines the core components of FAIR which include its unique methodology for assessing and quantifying cybersecurity risks. It contains the various categories within the framework core component illustrating the breadth and depth of risk management practices encompassed by FAIR.

Section 5 discusses how to put the FAIR framework into practice, stressing the methodical methodology that FAIR promotes for businesses to successfully identify, rank, and reduce cybersecurity risks.

The benefits and drawbacks of the FAIR cybersecurity framework's adoption and implementation are detailed in Sections 6 and 7. Users can decide whether or not FAIR is appropriate for their organizations by using the insights provided by this critical study, which highlights both its benefits and disadvantages.

In conclusion, Section 8 provides a summary of the main ideas covered in the paper, while highlighting the FAIR framework's potential to become an internationally recognized standard for cybersecurity risk management. It highlights how crucial it is to keep enhancing and improving the FAIR framework in order to guarantee its adaptability and efficacy in a variety of organizational situations and, eventually, to support better cybersecurity practices on a larger scale.

Reference Page

https://www.securitymagazine.com/articles/93509-the-importance-of-a-cybersecurity-framework#:~:text=When%20it%20comes%20to%20cybersecurity%2C%20a%20framework%20serves,promote%20the%20protection%20and%20resilience%20of%20your%20business.

https://www.rsisecurity.com/fair-risk-assessment/#:~:text=The%20Factor%20Analysis%20of%20Information%20Risk%20%28FAIR%29%20framework,of%20cyber%20attacks%20on%20critical%20data%20and%20systems.

https://www.cisecurity.org/insights/blog/fair-a-framework-for-revolutionizing-your-risk-analysis

https://www.fairinstitute.org/

https://www.cybersaint.io/blog/a-pocket-guide-to-factor-analysis-of-information-risk-fair