elasticito

NormShield

# USING THE FAIR® MODEL TO QUANTIFY CYBER RISK

# Cyber Risk with FAIR™

Having the capacity to use a FAIR assessment at scale for third-party risk management (TPRM) will elevate your risk management program and help you communicate the probable financial impact of potential cyber incidents in business terms. This tool will help attain the goal of cost effectively achieving and maintaining an acceptable level of loss exposure, while also clearly conveying the breadth of risks factors across the organization.

First, let's talk about what FAIR is and why you should care about using it in assessing third-party risk.

## What is FAIR?

- **Factor Analysis of Information Risk (FAIR)** is the only international standard quantitative model for information security and operational risk.[1] The model:
    - Provides a model for understanding, analyzing and quantifying information risk in financial terms.
    - Is unlike risk assessment frameworks that focus output on qualitative color charts or numerical weighted scales.
    - Builds a foundation for developing a robust approach to information risk management.
- FAIR model components are specifically designed to support risk quantification, through:[2]
    - A standard taxonomy and ontology for information and operational risk.
    - A framework for establishing data collection criteria.
    - Measurement scales for risk factors.
    - A modeling construct for analyzing complex risk scenarios.
- FAIR model analysis complements existing risk management frameworks by building on qualitative efforts in order to better quantify risk.[3] Shortcomings in risk management frameworks include:
    - Organizations such as **NIST, ISO, OCTAVE, ISACA**, etc. are useful for defining and assessing risk management programs, but go no further than those parameters.
    - Most frameworks prescribe the need to quantify risk, but for the most part, they leave it up to the practitioners to figure that process out.
    - Some are silent on the subject of how to compute risk, while others are open in the allowance of third-party methods.
    - Frameworks such as NIST 800-30 attempt to measure risk, but fall short as they rely on qualitative (not quantitative) scales and flawed definitions.

---

[1] FAIR Institute. 2019. Https://www.fairinstitute.org/; What is FAIR? From a Compliance-based to a Risk-based Approach to Information Security and Operational Risk https://www.fairinstitute.org/what-is-fair

[2] FAIR Institute. 2019. https://www.fairinstitute.org/what-is-fair; What is FAIR? From a Compliance-based to a Risk-based Approach to Information Security and Operational Risk https://www.fairinstitute.org/what-is-fair

[3] What is FAIR? From a Compliance-based to a Risk-based Approach to Information Security and Operational Risk https://www.fairinstitute.org/what-is-fair

FAIR helps fill the gaps in other risk management frameworks by providing a proven and standard risk quantification methodology that can be leveraged on other frameworks.


Figure 1: The FAIR Model

## How NormShield integrates and scales FAIR to calculate third-party risks

From a high level, technical data is used to feed FAIR calculations to achieve a data-based score. This technical score alone gives you an overall cyber-hygiene grade and is part of a greater risk assessment. But just because a company is assigned a certain grade does not necessarily mean that there is a high risk posed to your organization. A score alone lacks context related to business impact.

Through 3D Vendor Risk@Scale (SM) with FAIR a more useful probability can be calculated of the probable financial impact a vendor might make by using technical data, not just the score, in conjunction with other peer-related data. Such data can be garnered from such research as the annual IBM/Ponemon study, Verizon Data Breach report, Normshield's ongoing monitoring of publicly announced breaches.

For example, a probability is calculated of the probable financial impact in the event that a vendor were to have a cyber incident occur in the next twelve months. A minimum/maximum and probable amount is set by the analysis, resulting in a company receiving a C- grade; however, the financial impact is determined to be very low. Based on risk appetite, your business may decide that doing a deeper dive or committing more resources to requiring the vendor to improve their grade may not make good business sense. Additionally, you might have a vendor with a B+ grade, yet that vendor shows a high probable financial impact. To further and more effectively limit risk and financial loss, you would want to also prioritize continuous monitoring, alerting on variance, etc. as part of ongoing third-party assessments for this B+ vendor.

The Normshield FAIR report gives you the guidance to make these types of decisions, and also gives you the capability to tailor specific analysis where more complete data is available to you. You can easily and instantly update numerous indicators and data points to tailor the results for your vendors whenever more data becomes available.

## Steps to integrate NormShield's FAIR analysis into your third-party risk program

**Step 1: Find a FAIR evangelist on your team.** Not everyone in the TRPM program will need to be fluent in FAIR, but having one member who has taken the time to learn, train, and understand FAIR's use and value will help the rest of the team as they learn the platform and the program. *This person needs to be an adept critical thinker.*

**Step 2**: **Find FAIR support in other parts of the organization.** Many organizations today are embracing FAIR in Enterprise Risk Management and the larger cyber security world. Identifying those folks inside your organization and sharing your roadmap for integrating FAIR into your organization's TPRM will gain you broad support at all levels of management. If no one has yet embraced FAIR in your company, then your FAIR evangelist should prepare briefings about what it is, how it will be used in TPRM, and the value 3D Vendor Risk@Scale℠ with FAIR will bring to the company.

**Step 3: Develop a clear, specific value prop for the program.** Look for the initial project to prove FAIR using some key characteristics – meaningful results achieved quickly that are easily visible to executive decision-makers.[4]

**Step 4: Training.**

- The FAIR evangelist should read and be familiar with the following books, blogs and other information.
    - Books: *Measuring and Managing Information Risk: A FAIR Approach*; *How to Measure Anything in Cybersecurity Risk* – Hubbard, Seiersen
    - OpenFAIR Certification

[4] copeland, J.G. Expert Tips on Adopting FAIR from Our Breakfast Meeting at Gartner Gartner Security & Risk Management Summit. June 8, 2018. https://www.fairinstitute.org/blog/expert-tips-on-adopting-fair-from-our-breakfast-meeting-at-gartner

    - Blogs: https://www.fairinstitute.org/blog; https://www.risklens.com/blog/
- The challenge of biases including changing reliance on heatmaps and *qualitative* risk assessments may also need to be faced. Cybersecurity experts have been using heatmaps for quite some time and may be invested in their use, even though they are of little value in communicating actual risk, primarily due to their subjective or qualitative nature. Become familiar with the shortcomings of heatmaps. The following provides a good starting point:
    - *How to Measure Anything in Cybersecurity Risk by Geer, D.E., and McClure, S., Wiley Press.;* https://www.fairinstitute.org/blog/13-reasons-why-heat-maps-must-die; https://blog.protiviti.com/2019/02/21/cyber-risk-assessment-moving-past-the-heat-map-trap/

## Establish the basics

**Step 1: Determine what vendors are in scope for monitoring.** If you don't have a basic understanding of what vendors should be in scope for your TPRM monitoring program, then you can follow a simple tiering system model: if a vendor will receive or have access to sensitive data, will have persistent access to your network, or are critical/material to your company then they are in scope for monitoring.

When you have a list of vendors that meet that criteria, you can simply add the primary domain (URL) of that vendor into the NormShield platform and begin monitoring.

**Step 2: Use NormShield's ecosystem capability to create a bucket for each class of vendor (access to sensitive data, etc.).** If you already have a tiering system in place, simply create ecosystems around your model. Now you can begin to take action on the information that is presented. When just getting started with the program, you can use a technical score as your first red-flag. Start with the lowest technically ranked vendor, then review the FAIR impact of that vendor. If the impact is near or close to your company risk tolerance, then that vendor is a candidate for action.

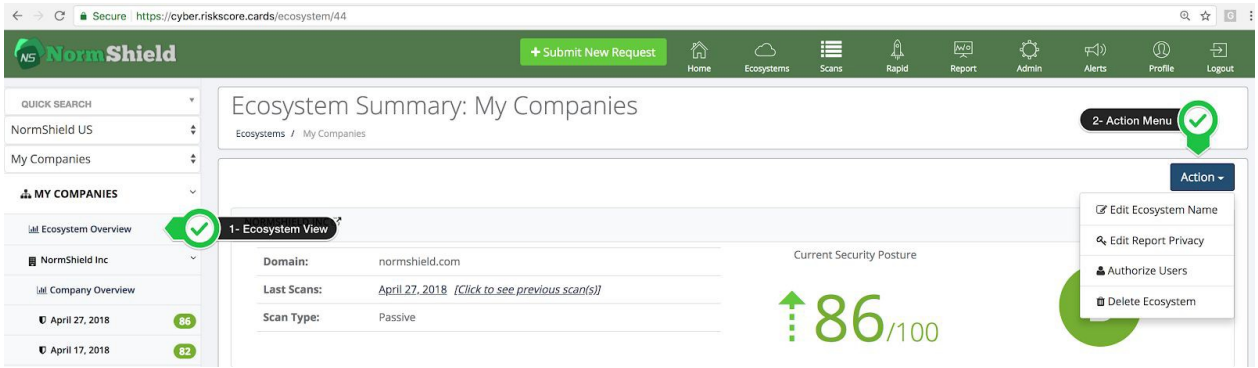



Figure 2: Risk Exposure Gradient

**Step 3: Flag vendors for action.** There are several avenues to take once you flag a vendor for action. The first is to review the FAIR Factors (Controls). Review the list of control items. If you

have knowledge of any that are in use at the vendor, adjust the FAIR analysis controls accordingly. Also review the number of records that the vendor has access to and update the controls list if you have that data. Additionally, if the vendor has (or will have) access to your network, check that box on the screen that shows they are accessing data on your network. After fine tuning these adjustments, if the financial impact is still near or above appetite, then it is time to address controls with that vendor.

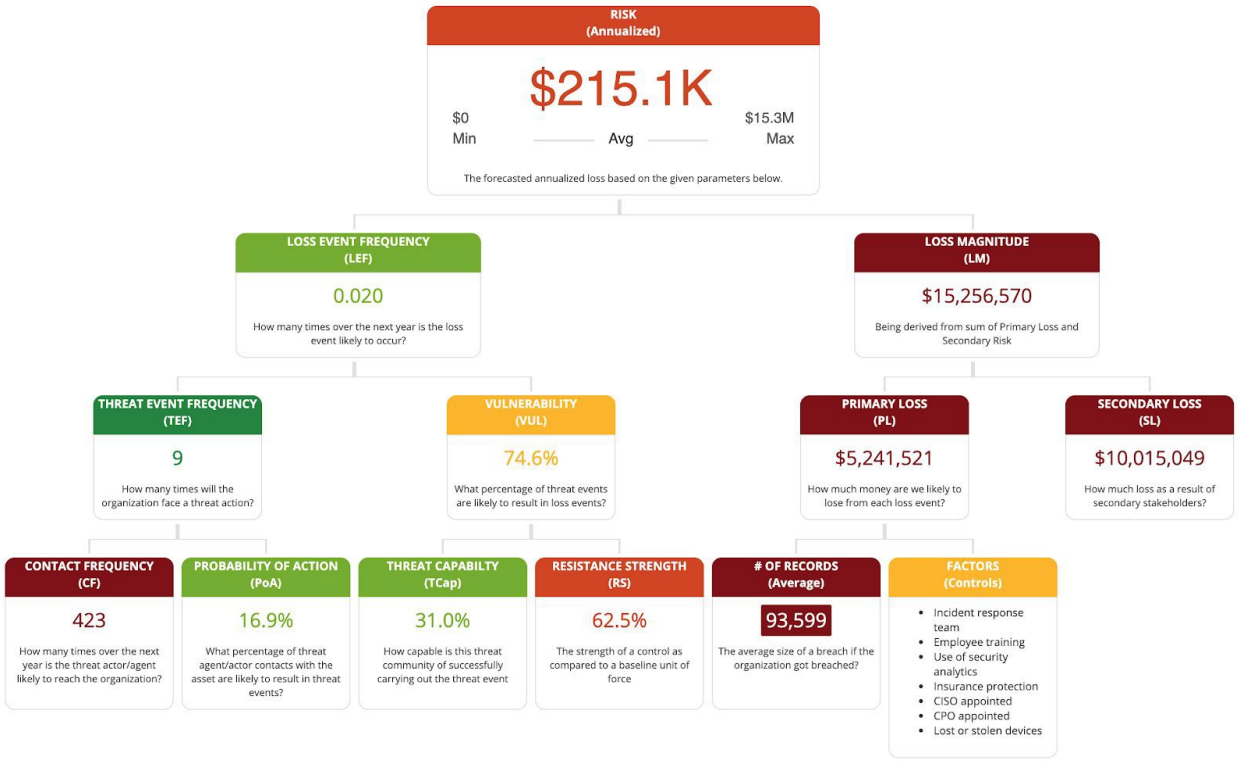



Figure 3: Risk Factors Controls Options within Threat Flowchart

**Step 4: Use the reporting features to filter for the highest risk issues and address those first with the vendor.** As you work with the vendor you may discover false positives. Identify and mark false positives, and then re-calculate the score and check the change in probable financial impact.

## Maturing a TPRM program to improving due diligence and action plans

As you continue to build the program, incremental optimization can be achieved on vendors that have been categorized as critical, material, and those that have shown the probability of a high dollar impact from the FAIR report. There are several ways that this can be done.

First, you will want to conduct an inventory of what you know about the selected vendor. Procurement or the business unit may have additional details or artifacts around compliance that have been previously collected. If a questionnaire such as the SIG (Standardized

Information Gathering) has already been collected, you can upload those details into the platform via the Compliance Report, Upload Compliance File. If you have an artifact such as a PCI-DSS ROC, you can go to the Compliance Reporting section, select the specific tab for the framework, then review the results column. You can add or adjust information based on the report. *Be sure to recalculate when finished with these additions.*

If you have more accurate details from the business unit about the vendor engagement, you can make those changes in the FAIR report, either through specific numeric data or other factors such as:


Figure 4: Data Breach Factor Options

When the new information is added to the assessment, review the three dimensions of risk (technical grade, compliance percentage, and probable financial impact numbers) to determine if direct follow-up action would be required.

- Follow-up may include:
    - Work with the business unit to reduce the need to share data.
    - Work with the vendor to improve their security hygiene and/or compliance posture.

- Work with your technical team to isolate vendor access to the network.
- Other refinements, as appropriate to your unique setting and relationships.
- Schedule continuous or periodic monitoring based on these results.

## Full maturity and optimization

One of the keys of moving your program to full maturity is understanding the relationship between assessments and risk appetite. Many organizations base their risk tolerance on a qualitative measure of low, medium, or high. The use of the NormShield platform will give you the tools to elevate the third-party risk conversation to a more advanced level. The first step is to know what your organization's risk appetite is when it comes to third parties. We won't cover the specifics of how to do that here, but refer you to a great blog to get started: https://www.fairinstitute.org/blog/define-your-companys-appetite-for-risk-with-fair-analysis

When you understand what your company risk appetite and tolerance is, then you can compare that to the FAIR probability of financial loss for a vendor.

- If the FAIR impact amount is *at or below* your appetite, then a vendor can be scheduled for fewer recurring monitoring and assessments.
- If the FAIR impact amount is *above* your appetite, but within risk tolerance levels, a deeper dive into the assessment process for that vendor would be warranted to improve accuracy. If it is beyond appetite but still within your company's risk tolerance, than a more frequent monitoring assessment schedule is suggested.
- If the FAIR impact amount is *beyond* your risk tolerance, then a deeper dive into the assessment process is warranted to improve the accuracy of the analysis. If it is beyond tolerance, then a plan of action should be identified for corrective action that the vendor could take to improve their risk posture. The time it takes for vendors to close any deficiencies that are identified is a good source of data for a key risk indicator (KRI), both for the vendor and your TPRM program.

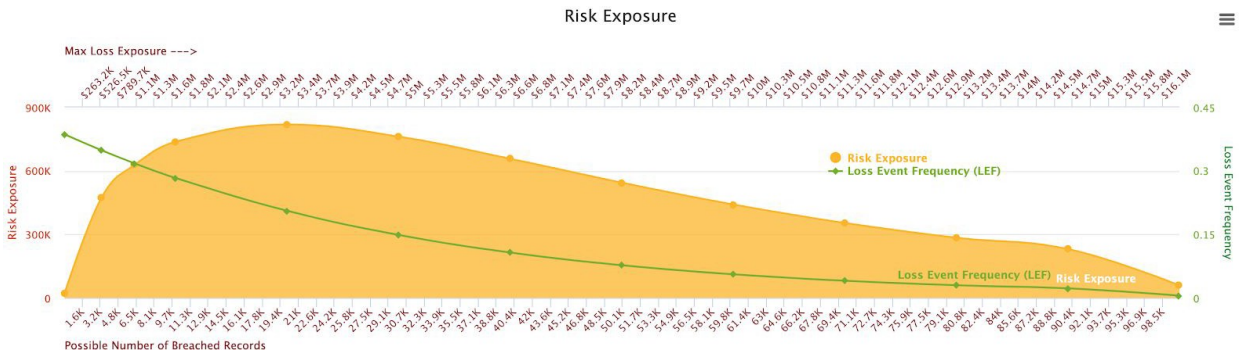



Figure 5: Risk Exposure Gradient

A well-documented and justified program meets regulator questions. It's no longer a matter of High/Medium/Low heat-maps. You can now create a process document that includes all of the analysis, review, and steps outlined above and reflects your more mature level of corporate

customization. When your analysis is tied to the pre-established corporate risk picture, regulators will understand your program is mature. Developing meaningful KRIs and key performance indicators (KPIs) is an essential part of building mature processes. Meaningful measurements enable effective comparisons, which in turn enable well-informed decisions. Measurement of variance relative to expected norms (such as variance from risk appetite) is the most effective method of obtaining good KRIs and KPIs.

The purpose of this guide is not to instruct you in creating those metrics, but to help you better understand the value of good indicators. "Variance is the true enemy because variance from and intended state of control almost always exists when a significant event occurs."– Chapter 13 of *Measuring and Managing Information Risk: A FAIR Approach.*

The final stage in achieving a fully mature program is understanding that nothing remains static. To that effect, adopting a strategy called the Observe, Orient, Decide, Act loops (OODA) is highly recommended. OODA is far more than a simple loop – it is a strategic way to help meet the goal of cost effectively achieving and maintaining an acceptable level of loss exposure. A great whitepaper prepared by the Shared Assessments Program goes into further detail on employing the OODA strategy in third party continuous monitoring and is available at: https://sharedassessments.org/tp-continuous-monitoring/

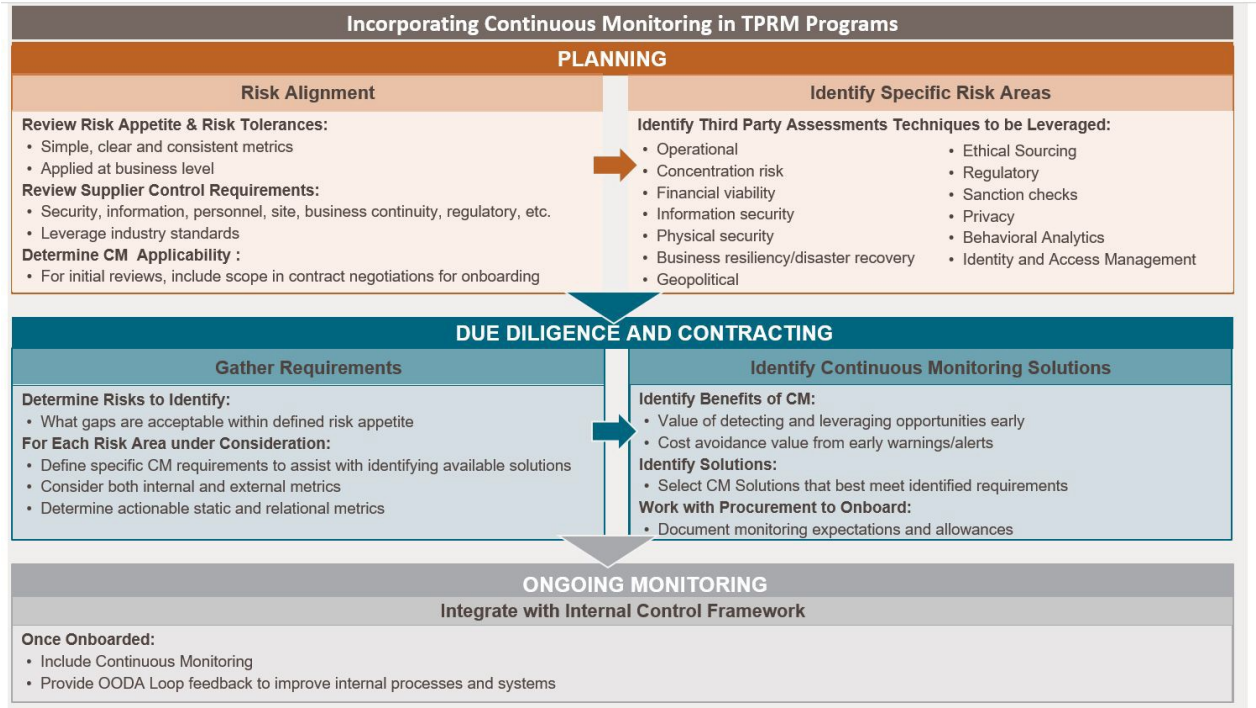
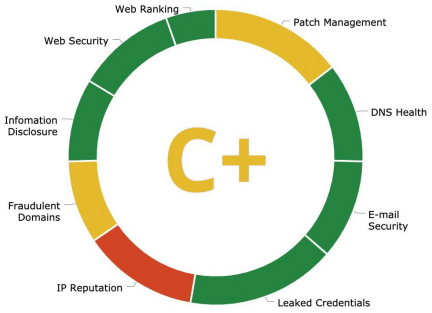



Figure62: Incorporating Continuous Monitoring in TPRM Programs[5]

[5] Innovations in Third Party Continuous Monitoring: With a Name Like OODA, How Hard Can It Be? The Santa Fe Group, Shared Assessments Program. 2018. https://sharedassessments.org/tp-continuous-monitoring/

NormShield is the only company taking a multidimensional approach to risk rating and assessment. It is not enough to simply score risk based on qualitative factors or to make business decisions on grade ratings alone. Risk assessments must be able to convey information in relatable terms to all stakeholders, and result in quantifiable, tangible business outcomes. This is the key to TPRM program success.

NormShield's vision is to give a complete risk picture of a vendor by providing NormShield Cyber Risk Scorecards (**technical assessment and monitoring**),FAIR results (**the probable financial impact of a breach caused by a supplier**), and Shared Assessments' SIG Questionnaire (**assessing that suppliers have appropriate policies and processes in place**).






**Technical Cyber Risk Score**

NormShield cyber risk scorecards enable organizations to self-monitor their cyber risk posture and perform a non-intrusive 60 second cyber risk assessment of their suppliers. Executives get easy to understand scorecards with letter-grade scores and IT security teams can drill down to the technical details in each risk category.

**Risk in Financial Terms**

NormShield uses the FAIR model to calculate the financial impact (risk) to an organization in the event that a cyber event were to occur at a chosen supplier to cost-effectively achieve and maintain an acceptable level of loss exposure. FAIR has become the only international standard for Value at Risk (VaR) model for cybersecurity and operational risk.

**Questionnaire & Compliance Correlation**

NormShield correlates findings to industry standards and best practices. The classification allows you to measure the compliance level of the target company for different regulations and standards including **NIST 800-53, ISO27001, PCI-DSS, HIPAA, GDPR** and **Shared Assessments SIG**.