FAIR-CAM™ Model FAQ

OCTOBER 2021

Q: What is the FAIR Controls Analytics Model? (FAIR-CAM™)

A: FAIR-CAM™ model is a formal description of how risk management controls operate, both individually and within a system of other controls, to affect the frequency or magnitude of loss.

Q: How does the FAIR-CAM™ model differ from FAIR?

A: FAIR is a model for measuring risk, whereas the FAIR-CAM™ model is a model that describes how controls affect risk. It doesn't change how you measure risk. You should think of this as an extension of the FAIR model, which provides the means to reliably map and account for risk management controls when performing a FAIR analysis. When combined with FAIR, this enables FAIR analysts to more easily and reliably measure the risk reduction value of controls.

Q: What's the need for the FAIR-CAM™ Model?

A: We tend to treat controls as if they operate independently and in isolation. For example, when an audit or vulnerability scan finds that a patch is missing from a system, we tend to rate the severity of that condition as if it's the only element that's in play. In fact, there can be many other controls in place that minimize or maximize the relevance of that missing patch.

For that matter, even if a control is currently operating as intended, how reliable is it, and is it providing enough risk reduction value to warrant its cost?

None of the security assessment tools used in the industry today consider the many factors that affect a control deficiency's significance, which makes their results inherently unreliable.

Q: How is this different and better than existing controls frameworks?

A: Existing control frameworks are lists of individual controls or control objectives. However, none of these frameworks formally define the many ways in which controls directly or indirectly affect risk.

The FAIR-CAM™ model provides a formal description of the system of control functions that directly or indirectly affect the frequency or magnitude of loss.

A useful analogy is the difference between the anatomy of a human body, and its physiology. Anatomy is a list of the parts (bones, muscles, nerves, organs, etc.), while physiology is a description of how those parts function both individually and as a system. Existing frameworks provide a useful "anatomy" for cybersecurity controls, and the FAIR-CAM™ model describes control physiology.

Q: Will the FAIR-CAM™ model replace the cybersecurity frameworks I now use?

A: No, it is complementary to existing frameworks. Applying it should make measuring the efficacy and value of controls easier and much more reliable. An effort is underway to map existing frameworks to the FAIR-CAM™ model, which will clarify how each element in those frameworks affects risk.

Q: How would this help cybersecurity teams evaluate and validate controls?

A: Most control assessment practices in use today simply express control conditions as ordinal scores (1 through 5, red, yellow, green, etc.). These ordinal values are abstract and subjective -- i.e., they aren't actual units of measurement, like percentages, time, units of money, etc. As a result, control measurements tend to be less reliable, and it's very difficult to translate control improvements into risk reduction.

The FAIR-CAM™ model will provide units of measurement (%, $, time, etc.) for each control function, which will mean that cybersecurity teams can empirically measure the efficacy of controls. And because the FAIR-CAM™ model overlays its control functions on top of the FAIR model, you'll be able to determine how much less risk will exist as controls improve (or vice versa).

Q: Is it necessary for me to use an application like RiskLens to use the framework?

A: RiskLens has begun integrating the FAIR-CAM™ model analytics into its platform. That said, although leveraging a technology like RiskLens will make it easier to apply FAIR-CAM™ model in an enterprise-scalable way, there isn't anything about the FAIR-CAM™ model that prevents its use for simple analyses in spreadsheets or even on a whiteboard.

Q: Will my controls environment get a maturity score from this? Or a rating of individual controls?

A: The FAIR-CAM™ model is primarily intended to enable measuring the value of risk management controls. That said, it also will provide the means of creating far more accurate maturity scores. This improvement in accuracy will result because the FAIR-CAM™ model accounts for systemic control relationships and dependencies, which aren't accounted for in current maturity scoring models.

Q: What training will I need to use this? Do I have to re-learn a new version of FAIR?

A: Training is being developed for FAIR-CAM™ model. Also, various printed materials will be available to become familiar with what it is and how to use it. And no, you won't need to re-learn FAIR. This should be considered an extension to FAIR.

Q: Let's take an example. How would the FAIR-CAM™ model have helped prevent the SolarWinds hack?

A: SolarWinds is similar to every other successful breach in the sense that the victim organization(s) had been making significant investments in security and yet they still got breached.

And, as with every breach, detailed analysis after-the-fact always shows that the organizations weren't able to focus on and maintain the controls that matter most. They're busy chasing compliance, or managing to a risk register that, ninety-five times out of a hundred, isn't risk-focused.

The FAIR-CAM™ model combined with a well-defined controls "anatomy-like" framework (e.g., NIST 800-53) and a solid risk measurement model like FAIR will improve an organization's ability to focus on the controls that matter most, and significantly reduce the odds of making the news due to a breach.

Q: When will the FAIR-CAM™ model become generally available?

A: A white paper is scheduled to be published in mid-October in coordination with this year's FAIR Conference.

Q. What rights do I have to use the FAIR-CAM™ materials and related content and what are the restrictions on use?

A: FAIR-CAM™ is a copyrighted work owned by the FAIR Institute. The final version will be available to you under Creative Commons Attribution-Non Commercial-No Derivatives 4.0 International Public License (the link can be found at https://creativecommons.org/licenses/ by-nc-nd/4.0/legalcode).

You may use the FAIR-CAM™ ontology for non-commercial purposes only. Additionally, if you remix, transform, create derivative works of, or otherwise change and/or build upon the FAIR-CAM™ ontology, you may not distribute the modified materials. Users of FAIR-CAM™ are also required to refer to (http://www.fairinstitute.org/FAIR-CAM/) when referring to the model in order to ensure that users are employing the most up-to-date guidance. You may not remove the trademark FAIR-CAM from any content provided by the FAIR Institute as part of the work and any use of the trademark FAIR-CAM other than on exact reproductions of documents provided to you by the FAIR Institute is prohibited.

Commercial use of the FAIR-CAM™ ontology and related materials is prohibited without the prior approval, in writing, of the FAIR Institute. Please direct questions and inquiries to info@fairinstitute.org.