HITRUST®

FAIR INSTITUTE

Integrating HITRUST® and FAIR™

Adding both of these approaches to your arsenal, and using them in tandem, will set your organization up for unparalleled information risk management success.

Table of Contents

List of Figures

List of Tables

This paper was first presented on October 7th at the FAIR Conference 2020.

Introduction

Imagine the following all-too-common scenario: A CISO walks into a board meeting with the following "Top Risk" report excerpt in search of a budget increase:

Risk	Likelihood	Impact	Risk Level
Weak Passwords	Very Likely	Major	**High**
Insider Threat	Moderate	Extreme	**High**
Cloud	Likely	Major	**High**
BYOD	Very Likely	Moderate	**High**
Third-Party Risk	Likely	Moderate	**Medium**

Table 1. Traditional Risk Reporting

It is fairly easy to imagine the next questions the CISO will probably get: "What does it mean that 'Cloud' is 'likely'?", "Of the four 'High' risks, which one is the biggest risk the organization?", "Does this mean we do not need to deal with third-party risk right now?" and "How much money will it take to address these risks?" Presenting information risk to leadership in this way creates a difficult environment for making well-informed decisions. The "risks" listed are a combination of control deficiencies, threat communities, information assets, and policies. The "risk level" doesn't provide enough detail to understand where to focus first or how much fiscal or other resources to devote to mitigation. Instead, consider the improvement of presenting the board with the following:

Business Threat	Risk Exposure	Control Improvement Opportunity
Cybercriminals stealing customer data from end-of-life-databases	$1.5M-$2.7M	Segregation in Networks
Insiders stealing intellectual property	$500K-$1.75M	Classification Guidelines Monitoring System Use
System failure at cloud provider for key business application	$800K-$1.45M	Addressing Security in Third-Party Assessments
Malware infection of company assets from personal devices on network	$350K-$700K	Controls Against Malicious Code

Table 2 . FAIR Quantified Risk Reporting

Questions will still arise, but with the rigor and defensibility of a thorough quantified assessment of threats, assets, and controls, those questions are easier to answer and defend than for qualitative and highly subjective approaches. Moving towards the result in Table 2 is what this and subsequent technical white papers regarding the integration of the HITRUST CSF® and the Factor Analysis of Information Risk (FAIR)™ methodology will achieve. By wielding the strengths of both the HITRUST framework and the FAIR methodology, organizations will be well-suited to tackle this challenge.

Since its inception in 2007, the HITRUST Approach has become one of the most successful solutions for organizational and third-party risk management and is responsible for the development of the HITRUST CSF. The HITRUST CSF is a comprehensive, prescriptive, and certifiable framework that meets the requirements of international, federal, and state regulations and industry standards, including HIPAA, GDPR, ISO 27000, and more than 40 others. The control-focused rigor that the HITRUST CSF enforces is critical to not only ensuring an organization is and remains secure, but also to generating controls-related data that FAIR risk assessments can consume.

FAIR™ is the foremost quantitative approach to cyber risk measurement and management. It consists of a standard risk taxonomy and an analytics model that provide organizations with the conceptual structure and approach to make a number of significant improvements over qualitative analysis that is ubiquitous in risk management. FAIR was developed with specific purposes in mind: applying greater rigor to risk analysis, quantifying exposure in a business-friendly language, using consistent terms when discussing or communicating risk, and modeling risk analysis in a repeatable manner. FAIR improves upon the practice of comparing qualitative statements on the likelihood and impact of a negative occurrence to come up with a descriptive term for the resulting risk exposure (e.g., High, Medium, Low, etc.). These terms in the FAIR methodology are replaced with the probable frequency and probable magnitude of future loss events. FAIR describes "risk" in financial terms, allowing for more discrete, effective comparisons between loss scenarios.

One of the chief characteristics of the HITRUST Approach that has made it so successful is an ongoing dedication to meeting the evolving needs of industries through continuous improvement. HITRUST's program is ever-evolving, with improvements typically focused on providing stakeholder communities with complementary tools and methodologies to support various types of risk analyses. The enhancements discussed here are focused on integrating FAIR's quantitative risk analysis processes into various components of the HITRUST Approach, along with mapping HITRUST CSF controls to the FAIR risk ontology. These enhancements will provide decision-makers with more ability to understand and manage their information risk environment than they would have with HITRUST or FAIR alone.

Integration Benefits

Aligning the FAIR methodology to the HITRUST Approach provides a basis for assessing the possible reduction of risk using the implementation and ongoing management of information security and privacy controls. By providing a single, unified approach to quantitative, control-based risk management, HITRUST and the FAIR Institute can help organizations improve their information risk management programs. This will include more knowledgeable risk management decision-making, ensuring scarce resources are deployed more efficiently, improving regulatory compliance and the protection of sensitive information, better communication of risk to senior management, board members, and other stakeholders, and ultimately prioritizing and optimizing information risk management investments.

In order to understand the benefits that an integration between HITRUST and FAIR may offer, and why the two working in tandem are more powerful to an organization than either on its own, it is important to understand the nature of effective risk management.

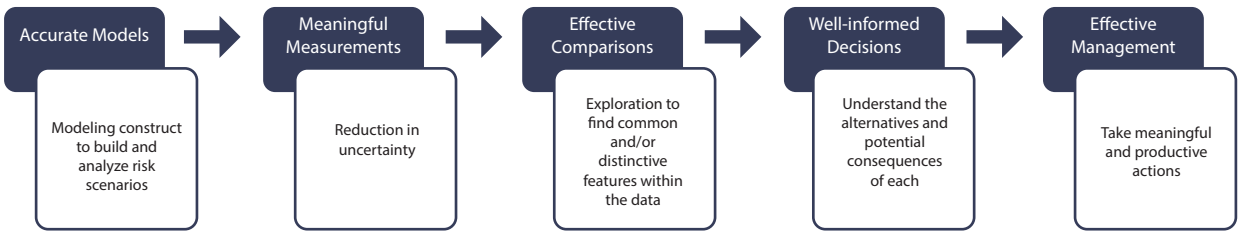

Figure 1. Risk Management Stack

As Figure 1 displays, effective risk management is predicated on well-informed decisions. Those well-informed decisions are dependent upon effective comparisons, which in turn are dependent upon meaningful measurements and accurate models. It is the preeminent goal for cybersecurity departments to ensure that each of the noted components are functioning as successfully as possible to facilitate effective risk management. The components in Figure 1 serve as a useful construct to highlight the strengths of HITRUST and FAIR, and how both contribute to an organization's effective information risk management.

The strength of the FAIR methodology lies in its ability to consistently define risk scenarios (probable loss events) and to determine discrete components for any given loss scenario that contributes to that scenario's frequency or magnitude.

At its most basic level, FAIR describes risk scenarios as probable loss events, where assets of value are being affected by threats, resulting in impacts to the organization, including loss of productivity, response costs, replacement costs, loss of competitive advantage, privacy liability, and reputational loss.

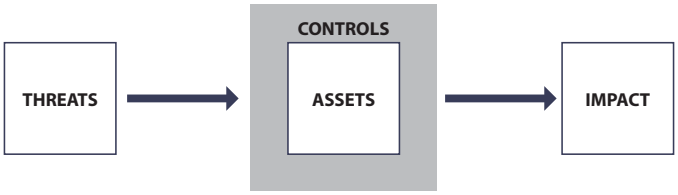

Figure 2. Risk Scenarios

Once risk scenarios are defined, FAIR provides a model to quantify the associated risk via the following model (FAIR ontology). The FAIR ontology decomposes risk into factors that analysts can measure by using historical or actual company data, industry data, or calibrated subject matter expert estimates.

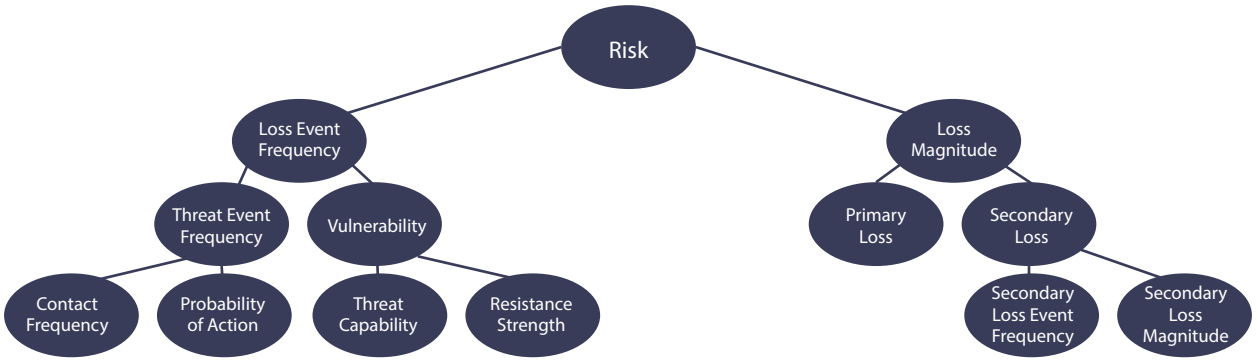

Figure 3. FAIR Ontology's Decomposition of Risk

The FAIR ontology provides a useful modeling framework to build and analyze risk scenarios. This, in conjunction with the FAIR methodology's emphasis on accuracy over precision, ultimately leads to accurate modeling, the first component of effective risk management outlined in Figure 1.

The second component of effective risk management outlined in Figure 1 is meaningful measurement. While the FAIR methodology is useful for providing those meaningful measurements, it is not purposefully built to install many of the components of effective governance over security control-related metrics at an organization, whereas HITRUST is. The HITRUST Approach is built to define control requirements, allow organizations to assign control ownership, and determine if their controls are well designed, mature, and functioning effectively. This control-focused governance pays dividends when it comes to collecting meaningful measurements about the controls themselves.

Control efficacy data is crucial to determining how well a particular risk scenario is controlled against and, conjoinedly, how much exposure is present. Control data can be mapped to several of the ontology variables, depending on the control type and the scenario being assessed. The HITRUST Approach allows for reliable, useful data inputs for FAIR risk calculations.

As meaningful measurements are collected and modeled accurately, effective comparisons can be made. These comparisons can take many forms, including comparing exposure among different loss scenarios and security control investments. HITRUST enables comparisons for decision-making by determining a set of security controls that aren't functioning effectively. The FAIR methodology enhances comparisons by measuring risk in financial terms, which enables direct comparisons across multiple risk scenarios. Both methodologies have strengths suited to supporting the components of effective risk management. By leveraging the strengths between the two in a defined manner, an organization will experience a myriad of risk management benefits.

Specific benefits of the integration work planned by HITRUST and the FAIR Institute include, but are not limited to:

- Improving the accuracy and precision of risk analyses needed for ongoing management of an organization's HITRUST CSF control environment, including those conducted for:
  - Risk acceptance
  - Gap analysis and corrective action prioritization
  - Alternate control selection
  - Operational portfolio management and resource allocation
  - Control specification
- Improving investment decisions and optimizing the cost of an organization's information protection program by providing a unified approach to quantitative, control-based risk management
- Facilitating industry adoption of the HITRUST Approach by existing users of the FAIR methodology
- Facilitating industry adoption of the FAIR Methodology by existing HITRUST organizations

These beneficial outcomes will come about by defining appropriate HITRUST and FAIR integration use cases and solutions for organizations. Viewed through the lens of the effective risk management stack, the solutions planned include, but are not limited to:

- Accurate Modeling
  - Defined process for converting an identified HITRUST CSF control gap into a quantifiable risk scenario with discrete, contributory components
- Meaningful Measurements
  - Defined process for collecting HITRUST CSF control efficacy information to be leveraged in the quantification of an identified risk scenario
- Effective Comparisons and Decision-Making
  - Defined process and decision-making framework for the outcomes of a HITRUST assessment and managing your security controls environment in an ongoing fashion

By leveraging HITRUST and FAIR in your organization's toolbox, you will be able to build an effective cyber risk management program, where the best cybersecurity decision is always determinable.

Integration Approach

HITRUST and the FAIR Institute will be working together to create a number of processes and integrations. These will provide a unique opportunity for a substantial number of organizations to adopt practical methods of incorporating risk quantification into their existing practices.

The integrated risk management processes and mappings developed by HITRUST and the FAIR Institute will help organizations answer important questions such as:

1. Is it valuable for my organization to leverage the strengths of both the FAIR methodology and the HITRUST framework?
2. If so, where and how can my organization best incorporate FAIR into existing practices within the fiscal, resource, and other operational constraints in a way that maximizes business value?
3. Where and how can my organization best incorporate HITRUST into existing FAIR assessment processes to provide more accurate and defensible results?

By providing predefined integrated risk management methods and processes, this approach will offer positive outcomes for organizations:

1. Makes FAIR adoption easier for HITRUST users
2. Uncovers the foundational value HITRUST provides to many FAIR processes
3. Facilitates the implementation of both approaches, resulting in quicker value realization

It's worth providing a bit more context for each of these points, as there are important nuances that are worth thinking about in the context of how FAIR could benefit existing HITRUST-based organizations or vice-versa.

Integration will be greatly facilitated for HITRUST organizations adopting FAIR when there are predefined use-cases. This is particularly important for resource-constrained organizations. There is a value in limiting integration to that which is needed to ensure consistency between FAIR and HITRUST while facilitating a relatively simple, 'out-of-the-box' but tailorable quantitative risk analysis capability that allows HITRUST-implementing organizations to achieve the intended benefits of this integration effort.

Organizations face significant fiscal, resource, and other operational constraints for building out mature, compliant cybersecurity programs. The idea of adopting a quantitative cyber risk program from scratch can be challenging for some organizations. Incorporating predefined use cases for FAIR integration into existing HITRUST efforts solves many of these challenges – it's another way of having a clearly defined initial value proposition for adopting FAIR in HITRUST organizations:

- FAIR is incorporated into existing HITRUST Approach processes
- There is clear guidance on how FAIR will be incorporated into the HITRUST CSF
- There is tangible business value for incorporating risk quantification

Using predefined methods and processes significantly eases the thought and effort required by HITRUST organizations to implement quantification into their program. HITRUST organizations have complex and sometimes competing priorities, which can be more easily compared and selected using FAIR. Without a predefined integrated approach, HITRUST organizations would likely need to process FAIR implementation through a formal change process. This could entail roadblocks, less than optimal implementation decisions, and implemented practices that could conflict with existing priorities. Having a predefined FAIR adoption method eliminates these problems. As there would be no conflict between FAIR and existing security and privacy practices, HITRUST organizations could subsequently focus on adopting FAIR without concern.

Case Study

To further detail the value that an organization may realize by the pursuit of integration between their HITRUST program and FAIR, take Highmark, Inc.'s experience as an example. Highmark, Inc. (Highmark) is a health and wellness organization located in Pittsburgh that operates health insurance plans in multiple states. Highmark has maintained HITRUST certification since 2017 and began its FAIR journey at the end of the same year. Since that time, Highmark's Information Security and Risk Management department has been defining an effective marriage between the two methodologies and leveraging their unique strengths with the ultimate goal of making measured, informed cybersecurity decisions to achieve an acceptable level of risk.

The Highmark team has found numerous integration points between HITRUST and FAIR that provide value to an organization. Ideally, every healthcare organization should understand the overall landscape of cybersecurity threats and corresponding risks in order to properly manage their exposure, prevent interruptions in healthcare services, and protect the confidentiality of their patients. This is where Highmark saw an opportunity for synergy between the HITRUST Approach and the FAIR methodology.

Using defined controls and related threat events, Highmark has developed a joint process that allows for both development of discrete FAIR loss scenarios and determining which HITRUST controls play a role in overall quantified risk exposure.

Identifying threats and corresponding controls is where Highmark uses the categorized and labeled cyber threats from the HITRUST Threat Catalogue™ and the controls from the HITRUST CSF mapped to those threats for assistance and guidance. So, as a fictional but plausible example of how this might come together, consider that most healthcare providers probably list their Electronic Health Records (EHR) system as one of their most critical assets. In looking through the HITRUST Threat Catalogue, one of the threat vectors the risk assessor may choose as a probable event is a combination of "LIN30 – Phishing" and "LIN32 – Ransomware" representing cybercriminals executing a phishing attack designed to deploy ransomware against healthcare providers. So now we have a fully defined FAIR risk scenario:

Threat Actor	Threat Vector(s)	Targeted Asset	Loss Effect
Cybercriminals	Phishing, Ransomware	EHR System	Availability

Table 3. Risk Scenario Components

This, however, is not enough on its own; the organization still needs to understand how its controls affect the scenarios. Again, this is where Highmark looks to its work with HITRUST to inform the FAIR process. The Threat Catalogue maps applicable controls from the HITRUST CSF to specific threat vectors. Highmark leverages that list to identify which are key controls and determine how they would input to the FAIR risk ontology. To continue with the fictional example, the organization now has something resembling this:

Threat Actor	Threat Vector(s)	Targeted Asset	Loss Effect	HITRUST CSF Control Reference	FAIR Control Type
Cybercriminals	LIN30 - Phishing LIN32 - Ransomware	EHR System	Availability	02.e Information Security Awareness, Education & Training	Avoidance
				09.j Controls Against Malicious Code	Avoidance
				01.m Segregation in Networks	Avoidance
				10.m Control of Technical Vulnerabilities	Resistive
				09.l Backup	Responsive

Table 4. Scenario with HITRUST CSF Controls

The information from both FAIR and HITRUST now supports an understanding of Highmark's loss scenarios and the effect controls have on them. The FAIR control types (e.g., avoidance) help to determine where data inputs in the FAIR model are informed by controls. HITRUST, in turn, provides a framework for understanding their controls' maturity and effectiveness, as well as identified control owners with whom the FAIR practitioners meet to define and collect relevant metrics or key risk indicators to support quantification.

Once the organization has a full understanding of risk scenarios (Threat, Asset, Effect, Controls), they can quantify risk to make specific and measured decisions. A good example of a specific use-case for Highmark is the prioritization of response to control gaps or deficiencies. Let's consider a small part of a HITRUST CSF Assessment that had the following results:

HITRUST CSF Control Reference	Assessment Result
02.e Information Security Awareness, Education & Training	Corrective Action Needed
09.j Controls Against Malicious Code	Operating Effectively
01.m Segregation in Networks	Operating Effectively
10.m Control of Technical Vulnerabilities	Corrective Action Needed
09.l Backup	Corrective Action Needed

Table 5. HITRUST CSF Assessment Results

Recognizing that this example is a very small set of controls and that a full HITRUST CSF Assessment is going to have a much larger set of results to analyze, prioritizing efforts and investment can present a significant challenge. Highmark turns to FAIR to assist with those assessment and prioritization decisions. Highmark analyzes how much improvement to key metrics and data inputs would occur if control deficiencies or gaps were effectively addressed. As Highmark has an understanding of their threat landscape, how their controls map to those threats, and the resulting risk, they are able to use a combination of FAIR software (RiskLens) in conjunction with "before and after" assessments to demonstrate potential reductions in loss exposure.

Again, realizing that a real list of controls could be significantly longer after a full HITRUST CSF Assessment and that, in reality, controls are likely to affect multiple scenarios, the table below provides a simplified example using the scenario above and the controls previously identified in Table 5 as needing corrective action. (Note: while the results here are fictional, they do accurately reflect the nature of results presentable to management and senior leadership.)

HITRUST CSF Control Reference	Assessment Result	Risk Reduction Opportunity
02.e Information Security Awareness, Education & Training	Corrective Action Needed	$200K-$800K
09.j Controls Against Malicious Code	Operating Effectively	
01.m Segregation in Networks	Operating Effectively	
10.m Control of Technical Vulnerabilities	Corrective Action Needed	$2M-$3.8M
09.l Backup	Corrective Action Needed	$750K-$1.7M

Table 6. Risk Reduction Results

Armed with results like these, Highmark can prioritize efforts and investments to improve those controls with the largest risk reduction impact first. While all controls are important on some level, rarely are organizations in the position to throw time and money at all control deficiencies or gaps at once. Trying to correct them simultaneously is therefore unlikely to have a meaningful effect on any of them.

This is just one use-case implemented by a single healthcare organization. Other opportunities abound, including choosing between competing mitigation strategies to address a singular HITRUST control gap. Having a sufficiently detailed process with appropriate integration points between HITRUST and FAIR defined will prove invaluable to IT organizations looking to enhance their cyber risk management.

Next Steps

The FAIR Institute and HITRUST will be developing and publishing predefined integration methods, processes, and mappings. The expectation is that organizations can take the results of a HITRUST CSF Assessment and use them to support risk calculations and comparisons using the FAIR methodology, allowing for enhanced HITRUST-informed decision-making.

Integration activities being considered include:

1. Quantitative analysis of the excessive risk incurred due to gaps in the implementation of specified HITRUST CSF control requirements to support the design/development and prioritization of corrective actions
2. Quantitative analysis of alternate HITRUST CSF controls to confirm a commensurate reduction in the amount and type of risk prior to accepting an alternate to a specified control
3. Quantitative risk-based decisions around operational portfolio management and resource allocation
4. Mapping of HITRUST CSF controls to the FAIR ontology
5. Initial selection (specification) of HITRUST CSF control requirements based on the inherent risk of specific activities or technologies

The results of this work will be published in future technical white papers.

How to Prepare for Leveraging FAIR and HITRUST

In the meantime, organizations should learn more about what FAIR and HITRUST currently offer and consider how the types of integration discussed in this paper could be leveraged in your existing risk management methods, processes, and tools. Examples include identifying how corrective actions for gaps in HITRUST CSF control implementation might be prioritized based on quantified risk reduction (as discussed in the case study) and valuing information assets to support risk quantification.

For more information on the overall HITRUST Approach, including the HITRUST CSF and HITRUST CSF Assurance Program, visit the HITRUST Website at https://hitrustalliance.net/the-hitrust-approach/. The HITRUST Website also offers numerous white papers, presentations, and data sheets via its Resources tab:

- Content Spotlight (https://hitrustalliance.net/content-spotlight/)
- Publicly Available Downloads (https://hitrustalliance.net/downloads/)
- Industry Insights (https://hitrustalliance.net/industry-insights/)

For more information on FAIR and best practices in cyber risk quantification, please visit the FAIR Institute Website at https://www.fairinstitute.org/. For access to the FAIR Institute's full resource library and to be kept up to date with industry news and upcoming events, individuals can apply to become a member of the FAIR Institute for free here: https://www.fairinstitute.org/get-involved-apply-today. Some public learning resources are below:

- "Measuring and Managing Information Risk: A FAIR Approach" (https://www.fairinstitute.org/fair-book)
- eBook: An Executive Guide to Cyber Risk Quantification (https://www.fairinstitute.org/download-executive-guide-to-cyber-risk-economics-ebook)
- eBook: An Adoption Guide to FAIR (https://www.fairinstitute.org/download-adoption-guide-to-fair-by-jack-jones-ebook)

Acknowledgements

A special thank you to the contributing authors:
Greg Rothauser, Highmark Health, Senior Risk Quantification Consultant
Marshall Lambert, Highmark Health, Cyber Risk Management Consultant
Tyler Britton, FAIR Institute member, RiskLens Risk Consultant
Bryan Cline, Ph.D., HITRUST, Chief Research Officer

About HITRUST

Since it was founded in 2007, HITRUST has championed programs that safeguard sensitive information and manage information risk for organizations across all industries and throughout the third-party supply chain. In collaboration with privacy, information security and risk management leaders from the public and private sectors, HITRUST develops, maintains, and provides broad access to its widely adopted common risk and compliance management frameworks as well as related assessment and assurance methodologies.

For more information, visit www.hitrustalliance.net.

About FAIR

The FAIR Institute is an expert, non-profit organization led by information risk officers, CISOs and business executives, created to develop and share standard information risk management practices based on FAIR. Factor Analysis of Information Risk (FAIR) is the only international standard analytics model for information security and operational risk. FAIR helps organizations quantify and manage risk from the business perspective and enables cost-effective decision-making.

To learn more and get involved visit: www.fairinstitute.org.


HITRUST®


FAIR
INSTITUTE