KOVRR
Cyber Decisions. Financially Quantified.

Abercrombie & Fitch Co.
Abercrombie & Fitch | YPB | abercrombie kids | HOLLISTER

CASE STUDY

Abercrombie & Fitch Elevates Cyber Board Reporting With Quantification

www.kovrr.com

Overview of Company

Abercrombie & Fitch Co. (NYSE: ANF) is a global apparel retailer headquartered in Columbus, Ohio. Founded in 1892, the company now operates more than 800 stores worldwide across its portfolio of brands. In fiscal year 2025, the company reported $5.3 billion in net sales and employed more than 40,000 associates. As a publicly traded enterprise with international operations, Abercrombie & Fitch Co. (A&F) maintains significant digital and operational exposure across regions.

Demonstrating Tangible Impact on Enterprise Risk

The Opportunity

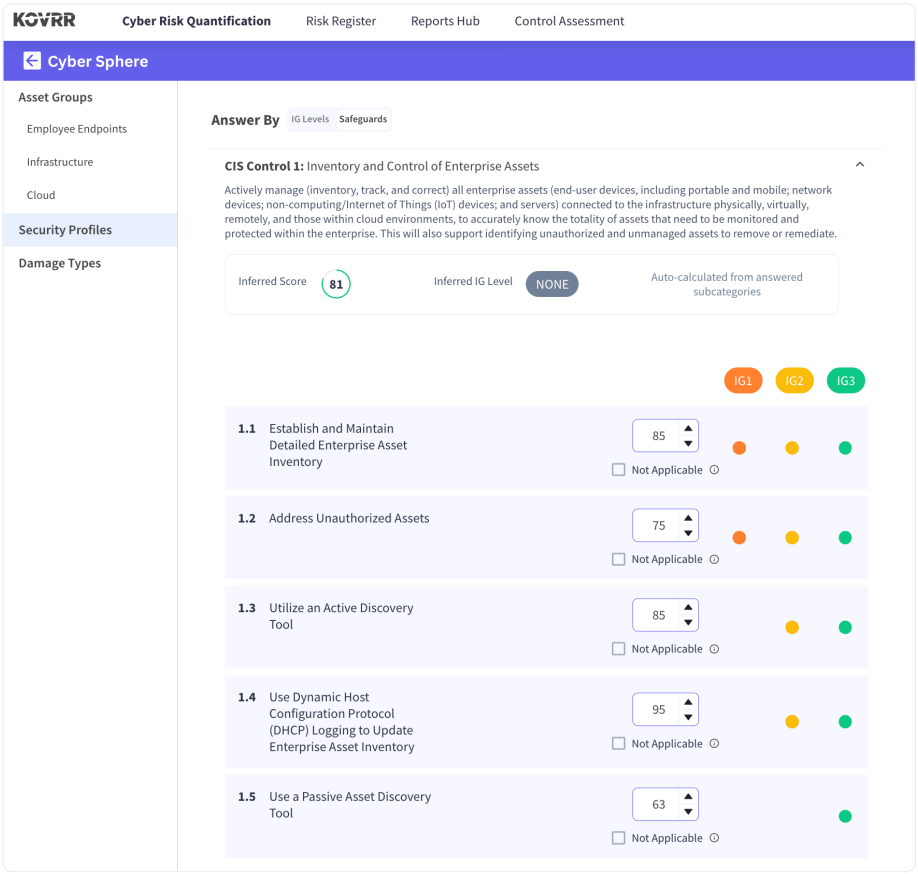
At A&F, executive leadership expects to be well briefed on the organization's exposure so insights can inform broader risk management strategies. However, the information security team needed a better way to communicate that exposure. Traditional updates, rooted in technical details and control maturity alone, did not always translate clearly into a business-relevant context. There was a desire to expound upon how industry risk factors interacted with internal control changes to paint a picture of changing risk.

> "We could describe our control posture in detail, but we were missing the added value of being able to describe changing cyber risk in dollars and cents in a way that executives and the board could easily understand."

To facilitate more meaningful conversations regarding cybersecurity, the team decided it was time to enhance its reports with quantified, financially grounded metrics that would supplement existing qualitative assessments. As such, they began looking for a cyber risk quantification (CRQ) solution that would allow them to track changes in exposure over time, demonstrate how security initiatives were influencing overall risk, and communicate how the external risk landscape was evolving.

The Solution

A&F partnered with Kovrr to optimize cyber risk quantification in a structured and iterative manner. The initiative, spearheaded by a Sr. Manager of Information Security and an Information Risk Analyst, began with the creation of A&F's customized Cyber Sphere within the Kovrr CRQ platform. They mapped their existing safeguards according to the CIS Controls v8 framework, specifying the sub-control maturity levels to reflect their current security posture. This process established an initial quantified baseline to support further analysis.



Kovrr's CRQ platform captures CIS Controls v8 safeguard maturity at the control and sub-control level, transforming technical inputs into monetary implications.*

Using these inputs, the team ran their first quantification, and within minutes, the platform produced a range of modeled outputs, including high-level financial metrics such as Average Annual Loss, 1:100 Annual Loss, and Annual Event Likelihood, along with peer benchmark comparisons. These metrics provided the A&F information security team with an additional, financially oriented lens on their exposure profile and were incorporated as a component of board-level reporting.

* Disclaimer: The figures shown are illustrative and do not reflect Abercrombie & Fitch's actual control maturity assessments.

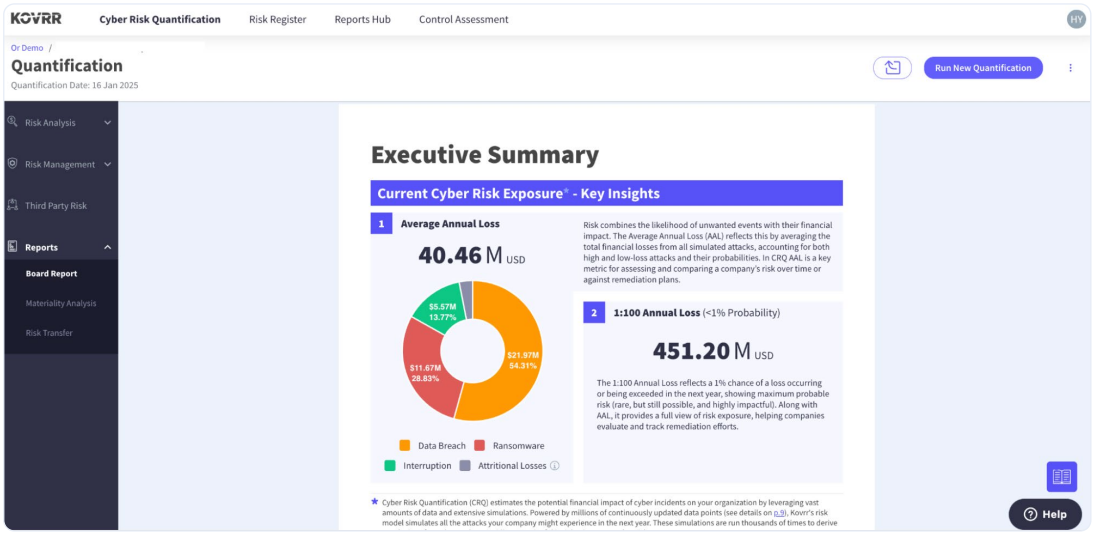
> "Kovrr's CRQ outputs gave us another way to frame cyber risk, not as a replacement for existing reporting, but as a complementary input that executives and the board could more easily relate to and incorporate into broader enterprise risk discussions."

After reviewing the initial results, the team sought deeper insights into how incremental control improvements might influence modeled exposure. While Kovrr's CRQ platform provides control-level recommendations as the standard, A&F worked closely with the Kovrr team to examine the modeled impacts of modest sub-control maturity improvements. This deeper analysis supported the organization in evaluating how targeted safeguard enhancements would affect modeled loss forecasts.

These sub-control impact scenarios became a key input for the team not only to prioritize mitigation initiatives but also to defend those decisions at the board level. As their security program evolved, A&F updated their maturity inputs and reran the quantification. This iterative approach ensured that the model reflected both internal control improvements and changes in the external threat landscape. The team incorporated quarterly reruns into their reporting cycle, leveraging updated threat intelligence insights to explain shifts in exposure over time.

The Outcome

The quantified cyber risk metrics became a structured, vital component of A&F's reporting process, emerging as their main use case. By incorporating the potential loss insights into their updates, the information security team achieved its goal of being able to present cyber exposure in intelligible business terms. Reports included top-level organizational indicators and peer benchmarks, providing the executive team with a more tangible understanding of the company's risk profile.



*Kovrr's out-of-the-box Board Report translates quantified cyber exposure into executive-ready insights.**

* Disclaimer: The figures shown are illustrative and do not reflect Abercrombie & Fitch's actual control maturity assessments.

The team also incorporated Kovrr's quantification platform into their assessment rhythm. By rerunning the model as both internal inputs and external threat intelligence evolved, they were able to discuss drivers of change in exposure over time. The team regularly pulled insights into what had changed most quarter over quarter and used fluctuations in ransomware costs as an example of how continuously updated threat data supported discussions.

In conjunction with reporting, quantification outputs also supported discussions around control improvements. Through sub-control impact modeling aligned to CIS Controls v8, the team assessed how gradual, calculated upgrades would influence exposure levels. With these more granular details, they were able to compare initiatives based on relative modeled impact and connect project execution to observable movement within the model.

> "Being able to show how the projects we're executing and the investments we're making are reflected in the model helped reinforce the story we were telling."

Ultimately, the ability to tie cybersecurity resources to modeled changes in risk supported clearer board-level discussions around cybersecurity strategy. The board gained greater visibility into the initiatives being funded and how approved investments were expected to influence the organization's overall risk posture.