Drive Business Decisions Using Continuous Control Monitoring

Simplify FAIR™-CAM with SAFE One

Every CISO seeks answers to basic questions about control effectiveness to balance risk reduction and investment:

- *What's the most valuable control for risk reduction?*
- *What's the least valuable control?*
- *How do the controls work together to reduce risk?*
- *What's the best control to handle a particular risk?*

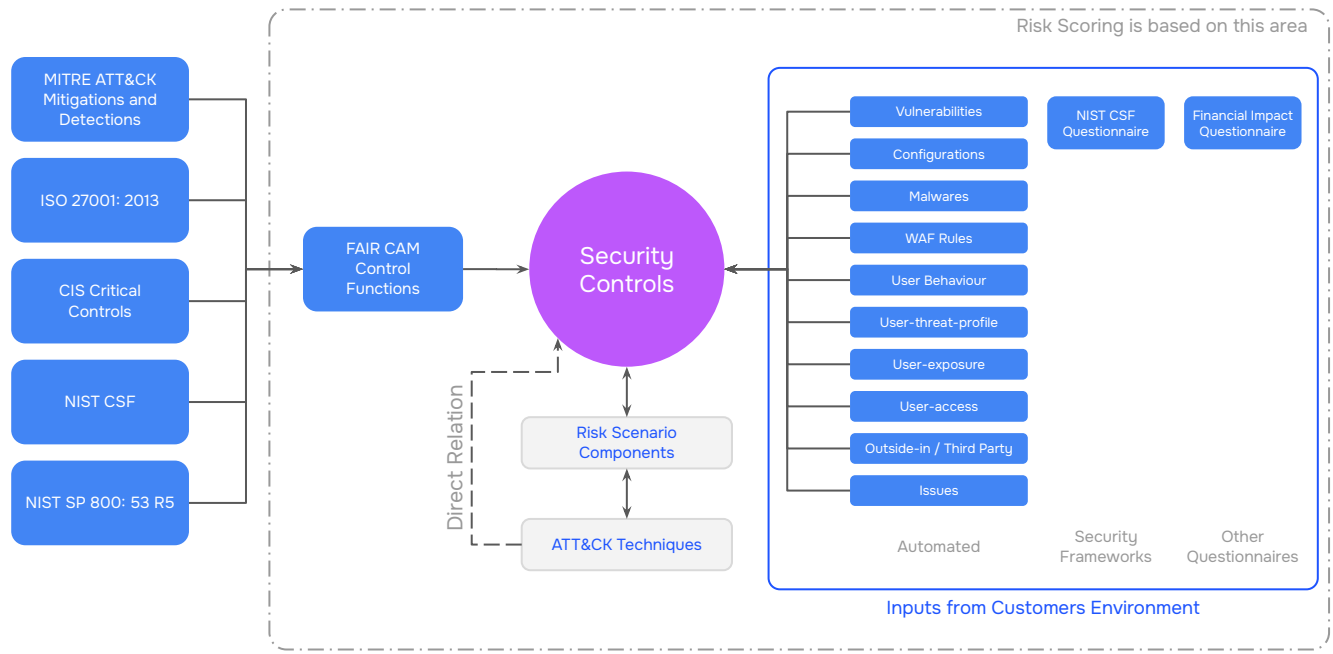
Unfortunately, assessing controls and their maturity has traditionally been spreadsheet-driven; based on manual inputs and subjective assumptions. Managing a full suite of cybersecurity controls a holistic approach – one that needs to be supported by an industry standard which measures control effectiveness and their impact on cyber risk. FAIR™-CAM is the answer to this critical challenge.

Leverage FAIR™-CAM with SAFE One

- Adjust controls maturity based on risk reduction insights
- Prioritize critical control gaps by understanding the ROI
- Assess if the business is sufficiently protected against loss events
- Visualize risk burndown by adjusting controls maturity
- Drive business decisions regarding resource reallocation

Finding a Solution: What is FAIR™-CAM?

FAIR™-CAM overlays the original FAIR™ model and takes controls analysis to a granular level. It describes and quantifies the function of each control for risk reduction, documents the interdependence among controls, and the effectiveness of a controls system overall. **To summarize, FAIR™-CAM maps the controls physiology and quantifies the effect of controls on risk reduction.**



The Foundation of the FAIR-CAM Controls Library

How FAIR-CAM Measures Risk Reduction

The FAIR-CAM™ model accounts for multiple ways that controls impact risk burndown. It factors how various cybersecurity controls act together to change threat event frequency (TEF) and susceptibility.

For Threat Event Frequency, FAIR-CAM assesses avoidance, deterrence, resistance, detection, and response controls. For susceptibility, FAIR-CAM evaluates:

- **Loss Event Controls (LEC)** which function by directly affecting the frequency or magnitude of loss.
- **Variance Management Controls (VMC)** that function by affecting the reliability of controls.
- **Decision Support Controls (DSC)** which function by affecting decisions.

Every control is evaluated on the basis of three parameters to determine the control maturity:

- **Capability:** What is the intended efficacy of a control?
- **Coverage:** Is the control well implemented in the context of intended efficacy?
- **Reliability:** How reliable is the control regarding variant conditions from intended efficacy? Does the control 'fail' frequently?

FAIR-CAM takes a comprehensive approach to mapping controls to risk, thereby facilitating risk-informed decision-making. To curate the FAIR-CAM library of controls, it leverages:

Primary reference(s):

- ISO 27001: 2013
- CIS Critical Controls
- NIST CSF
- NIST SP 800:53 R5
- MITRE ATT&CK Detections & Mitigations

Cross-referenced with:

- 33 Secure Controls Framework domains
- MITRE ATT&CK Mitigations and Techniques
- Initial Attack Method(s) supported in SAFE
- Attack Outcomes supported in SAFE

SAFE-One's Implementation of FAIR-CAM

SAFE One is the first and only automated implementation of FAIR-CAM into a cyber risk management platform for analysis of controls effectiveness. FAIR-CAM is automated and simplified in all the critical functions of the platform:

- **Controls Library:** Users upload their NIST CSF documentation or other roster of controls, and the platform automatically maps them to a FAIR-CAM controls library.
- **Controls Center:** Via telemetry, a dashboard gives real-time view on the status and maturity level (capability, coverage, reliability) of the organization's controls, as well as gaps in control coverage. Safe supports 100+ integrations with cybersecurity products.
- **Risk Scenario Modeling:** SAFE One automatically maps controls to out-of-the-box cyber risk scenarios leveraging the MITRE ATT&CK framework. This enables users to side step the long and arduous process of control identification for risk scenario modeling.
- **Identifying and Addressing Critical Control Gaps:** The SAFE platform equips users to visualize how modifying maturity levels for the relevant FAIR-CAM mapped controls impacts the risk of a cyber event. It does so from the perspective on ROI using its "what-if" analysis feature.

An Example on How SAFE One uses APIs to Automate FAIR-CAM's Control Maturity Assessment:

SAFE One's integration with M365 Defender automates the reliability of FAIR-CAM controls such as Data in Transit Encryption, Multi-Factor Authentication, Email Security and Protection, Hardened SaaS Application, and more.

Benefits of FAIR-CAM in SAFE One

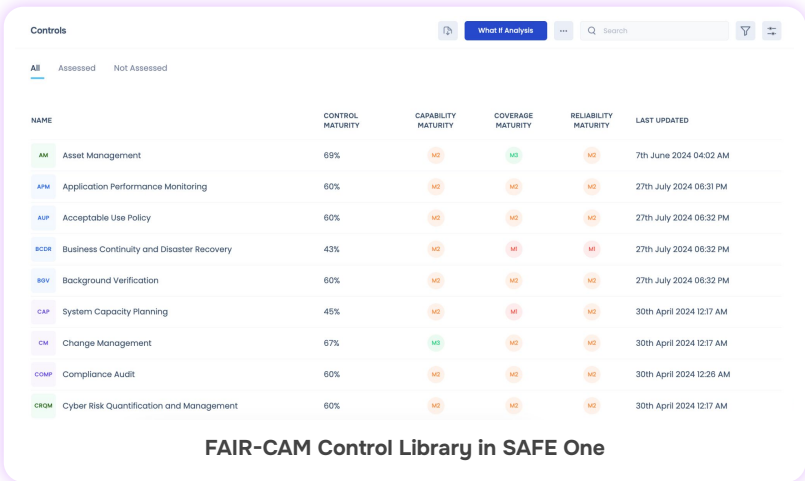
SAFE One is the first and only integration of FAIR-CAM into a cyber risk management platform for analysis of controls effectiveness scientifically and transparently. FAIR-CAM figures in all the critical functions of the platform:

- **Adjust control maturity to learn which has most or least value**
  SAFE One's "What-If" analysis enables risk leaders to visualize the direct impact of modifying controls maturity (coverage, capability, reliability) on the likelihood and loss magnitude. Determine the course of action that aligns most practically with your business's risk appetite and risk tolerance.

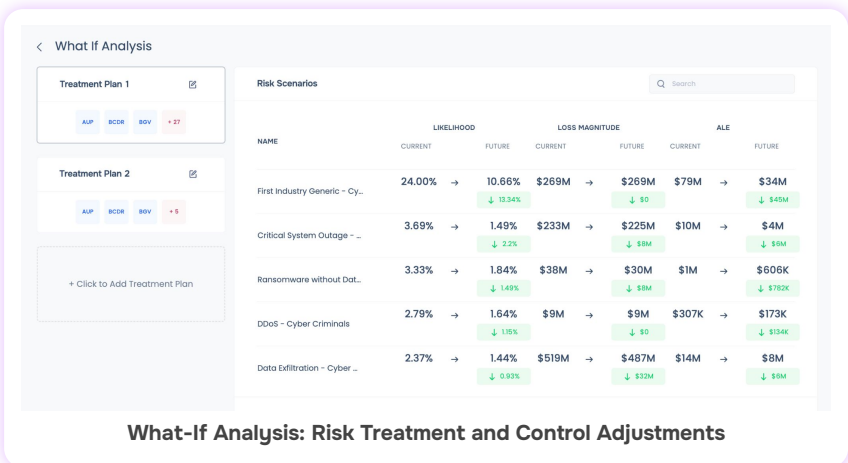
- **Prioritize the most critical controls gaps to maximise risk burndown**
  With SAFE One's comprehensive risk scenario modelling, learn which controls have the greatest impact on reducing the risk for ransomware, data exfiltration, DDoS, and more. Identify and prioritize the most critical controls to ensure your most significant risks are covered.

- **Efficiently communicate if the business is protected against loss events**
  SAFE One enables risk leaders to assess control effectiveness. Visualize how each control interacts with your business's cybersecurity stack and get data-driven insights on how to modify control maturity (coverage, capability, and reliability) to maximize loss exposure reduction.

- **Learn the Return On Investment from controls modification**
  SAFE One provides a ROI-driven visibility to control modification. With this insight, risk leaders are equipped to drive business decisions around cybersecurity investments and insurance – ensuring the CISO has a permanent seat in the boardroom.



FAIR-CAM Control Library in SAFE One



What-If Analysis: Risk Treatment and Control Adjustments

CASE STUDY: Leveraging FAIR™-CAM as a Decision-Support Tool with SAFE One

A $76B operator of the world's largest vendor-neutral multi-tenant data center aimed to elevate information security to a trusted decision-support asset while reducing costs as the organization's digital initiatives grow.

BUSINESS PROBLEM
The Integrated Risk Management (IRM) team wanted a data-driven way to decide whether or not to invest in a complete asset management (CMDB) product.

BEFORE SCENARIO

- Perform an internal audit or hire external services to perform an audit
- Identify the correct and exhaustive list of assets and controls that need to be factored
- Manually corroborate information from external and public data sources
- Determine acceptable susceptibility and loss magnitude ranges
- Carry out the risk assessment and risk quantification exercise

AFTER FAIR-CAM (SAFE One Platform)

- All relevant controls and assets are already mapped with SAFE One's implementation of FAIR-CAM
- External data and internal telemetry automatically layered for business context
- SAFE One calculates susceptibility, likelihood, and loss magnitude for various risk scenarios
- Clear ROI-driven "this vs. that" what-if analysis to determine the next steps

POSITIVE BUSINESS OUTCOMES

- Accurate and transparent mapping of controls
- Automated process which reduced manual dependencies/errors
- No more guesswork before adding, deleting, modifying control maturity
- Decision support time reduced from 4-5 business days to under 30 minutes
- Enhanced team efficiency

Driving Business Decisions with FAIR™-CAM and SAFE One

The only factor an enterprise can directly influence to minimize loss event frequency and susceptibility and ensure risk burndown is controls. With FAIR™-CAM automated by SAFE One, modifying controls to suit enterprise risk appetite and budget is straightforward, transparent, and defensible.

Want to learn more about how you can start or enhance your FAIR™ journey? Schedule your 1:1 demo with a SAFE cyber risk expert today.

RESEARCH SPONSOR
MITRE ATT&CK, TOP CONTRIBUTOR

PUBLISHER'S CHOICE AWARD
RISK MANAGEMENT
GLOBAL INFOSEC AWARDS - RSAC 2023

BEST NEXT GEN
CYBER INSURANCE PLATFORM
GLOBAL INFOSEC AWARDS - RSAC 2023

BEST RISK
MANAGEMENT SOLUTION
CISO CHOICE AWARDS 2022™