CASE STUDY

How FAIR Risk Quantification Enables Information Security Decisions at Swisscom

Swisscom is Switzerland's leading telecom provider. Due to strategic, operational and regulatory requirements, Swisscom Security Function (known internally as Group Security) has implemented quantitative risk analysis using Factor Analysis of Information Risk (FAIR). Over time, Swisscom's FAIR implementation has enabled Group Security to objectively assess, measure and aggregate security risk. Along the way, Swisscom's Laura Voicu, a senior security architect, has led the Swisscom security risk initiative.

Introduction

Information risk is the reason businesses have security programs, and a risk management process can be a core security program enabler. With an effective risk program, business risk owners are well-informed about risk areas and take accountability for them. They are able to integrate risk considerations into managing value-producing business processes and strategies. They can express their risk tolerance (i.e., appetite) to technical and operational teams and, at a high level, direct the risk treatment strategies those teams take.

Most organizations now operate as digital businesses with a high reliance on IT. They can benefit by shifting the corporate culture from one that focuses on meeting IT compliance obligations to one that targets overall risk reduction. Visibility into the overall security of the organization plays an important role in establishing this new dialog. Security leaders can prioritize their security initiatives based on the top risk areas that an organization faces.

Dan Blum, CISSP, Open FAIR
Is an internationally recognized strategist in cybersecurity and risk management. His forthcoming book is *Rational Cybersecurity for the Business*. He was a Golden Quill Award-winning vice president and distinguished analyst at Gartner, Inc., has served as the security leader at several startups and consulting companies, and has advised hundreds of large corporations, universities and government organizations. Blum is a frequent speaker at industry events and participates in industry groups such as ISACA®, FAIR Institute, IDPro, ISSA, the Cloud Security Alliance and the Kantara Initiative.

Laura Voicu, Ph.D.
Is an experienced and passionate enterprise architect with more than 10 years of experience in telecommunication and other industries. She is a leader in enterprise and data architecture, cybersecurity and quantitative risk analysis. Her latest passion is data science and driving innovation with a focus on big data and machine learning. Voicu frequently presents at conferences and volunteers as an ISACA SheLeadsTech Ambassador.

Swisscom uses quantifiable risk management enabled through Open FAIR to:

- Communicate security risk to the business
- Ascertain business risk appetites and improve business owner accountability for risk
- Prioritize risk mitigation resources based on business impact
- Calculate the return on investment (ROI) of security initiatives
- Meet new and more stringent regulatory requirements

Company Background

Swisscom is the leading telecom provider in Switzerland and one of its foremost IT companies, headquartered in Ittigen, near the capital city of Bern. In 2019, 19,300 employees generated sales of CHF 11,453 (USD $12,490) million. It is 51 percent confederation-owned and is considered one of Switzerland's most sustainable and innovative companies. Swisscom offers mobile telecommunications, fixed network, Internet, digital TV solutions and IT services for business and residential customers. Swisscom's Group Security, which is a centrally managed function at Swisscom, provides policies and standards for all lines of business, while allowing each business to operate independently.

Digitization, changing customer requirements, predatory competition in the saturated core market and new providers with disruptive business models put the business under pressure. The long-term corporate strategy aims to compensate for the decline in revenue and profit, thus maintaining the financial strength to invest heavily in new technologies. Whatever its many benefits, digitization in the virtual world also has a darker side and organizations are facing new kinds of risk. Therefore, Swisscom defined security as one of its strategic capabilities, and having a risk-based decision-making capability is a critical success factor.

"WHATEVER ITS MANY BENEFITS, DIGITIZATION IN THE VIRTUAL WORLD ALSO HAS A DARKER SIDE AND ORGANIZATIONS ARE FACING NEW KINDS OF RISK."

Qualitative Risk Analysis Pain Points

Prior to 2019, Swisscom managed and assessed information risk using qualitative analysis methods. The process was well-suited to quick decisions and easy to communicate with a visually appealing heat map. However, the Swisscom security team identified several fundamental flaws, including bias, ambiguity in meaning (e.g., What does "red" or "high" really mean?) and a probability that the person doing the measurement had not taken the time to clearly define what it is he or she just measured.

For reference, **figure 1** illustrates a sample 5x5 heat map plotting nine risk areas (R1 to R9) on a graph where the vertical access plots the probability of a risk materializing and the horizontal access plots the hypothetical impact.

Risk Terminology

- **Risk (per FAIR)**—The probable frequency and probable magnitude of future loss
- **Open FAIR**—Factor Analysis of Risk (as standardized by The Open Group)
- **Information risk**—Risk of business losses due to IT operational or cybersecurity events
- **Qualitative risk analysis**—The practice of rating risk on ordinal scales, such as 1 equals low risk, 2 equals medium risk or 3 equals high risk
- **Quantitative risk analysis**—The practice of assigning quantitative values, such as number of times per year for likelihood or frequency, and mapping impact to monetary values
- **Enterprise risk management**—The methods and processes used by organizations to manage the business risk universe (e.g., financial, operational, market) as well as to seize opportunities related to the achievement of their objectives

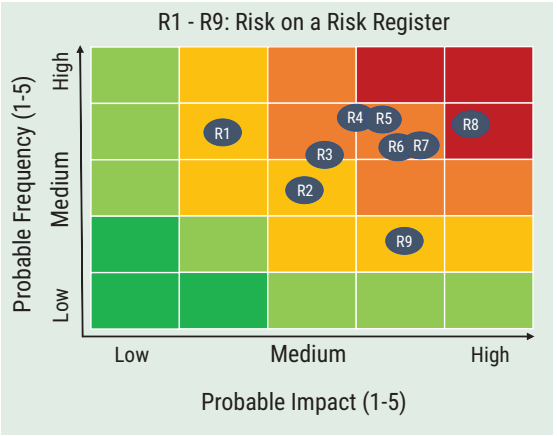
Enjoying this article?

- Read *Risk IT Practitioner Guide, 2nd Edition. www.isaca.org/risk-it-pg2*
- Learn more about, discuss and collaborate on risk and assurance in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Inconsistent Risk Estimates
Qualitative risk estimates tended to be calculated in an inconsistent manner and were often found to be unhelpful. Because analysts did not use a rigorous risk quantification model such as FAIR to rate risk, they relied on the mental models or years of habit.

Early staff experiments with quantifying security risk also failed; per a senior security officer at Swisscom, the reasons for this were, "Too little transparency and too many assumptions. In short: a constant discussion about the evaluation method and not about the risk itself."

Figure 1—Qualitative Risk Estimates Graphed as a Heat Map



Too Many "Mediums"
Odd things happened: Virtually all risk areas were rated "medium." A high rating is a strong statement and draws unwanted attention to the risk from business management, who might then demand some strong justification for the rating. A low rating would look foolish if something bad actually happened. Rating risk "medium" equals the safe way out.

Inability to Prioritize Risk Issues
Although utilizing qualitative methods may provide some prioritization capability (a risk rated red is some degree worse than one rated yellow), Swisscom had no way of economically evaluating the difference between a red and yellow, between one red or two yellows, or even between two yellows such as R1 and R9 as shown in **figure 1**. In short, Swisscom had poor visibility into the security risk landscape, thus potentially misprioritizing critical issues. Over time, Swisscom staff came to share the FAIR practitioner community objections articulated in the article "Thirteen Reasons Why Heat Maps Must Die."[1]

Demand for More Accurate Risk Assessments After a Breach
In 2018, Swisscom went public to announce a large data breach. Swisscom took immediate action to tighten the internal security measures to prevent such an incident from happening again. Further precautions were introduced in the course of the year.

Following the data breach, Swisscom IT and security executives sought to improve the risk assessment process. Staff had made early attempts to quantify security risk using single numerical values, or single-point estimates of risk by assigning values for discrete scenarios to see what the outcome might be in each. This technique provided little visibility into the uncertainty and variability surrounding the risk estimate.

Establishing a Quantitative Risk Analysis Program

Swisscom's Group Security team learned about FAIR in 2018 and became convinced that its model was superior to in-house risk quantification approaches that the team had attempted to use in the past. FAIR allows security professionals to present estimates of risk (or loss exposure) that show decision-makers a range of probable outcomes. Using ranges brings a higher degree of accuracy to estimates with enough precision to be useful.

> "FAIR ALLOWS SECURITY PROFESSIONALS TO PRESENT ESTIMATES OF RISK (OR LOSS EXPOSURE) THAT SHOW DECISION-MAKERS A RANGE OF PROBABLE OUTCOMES."

The decision was made to use FAIR in 2018 and Senior Security Architect Laura Voicu was assigned to lead a core team of a few part-time FAIR practitioners. The risk project's initial phase was to define risk scenarios in a consistent manner throughout Swisscom. As result of this work effort, the team produced a formal definition and consistent structure

for normalizing risk register entries into FAIR-compliant nomenclature, shown in **figure 2**.

The FAIR team performed multiple analyses and continued to deepen its experience with the quantitative approach. As a best practice, the team interviewed or held workshops with subject matter experts (SMEs) on controls, incidents, impacts and other areas representing variables in the FAIR analysis.

Starting in early 2019, a small group of stakeholders within the security organization conducted a proof of concept (POC) to perform assessments of the customer portal data breach risk, risk associated with different cloud workload migration strategies, outage of systems or networks due to ransomware and, recently, remote working use cases to continue operating amid the COVID-19 disruption.

In parallel, Group Security defined roles, analysis processes and risk management processes. The team defined the following roles:

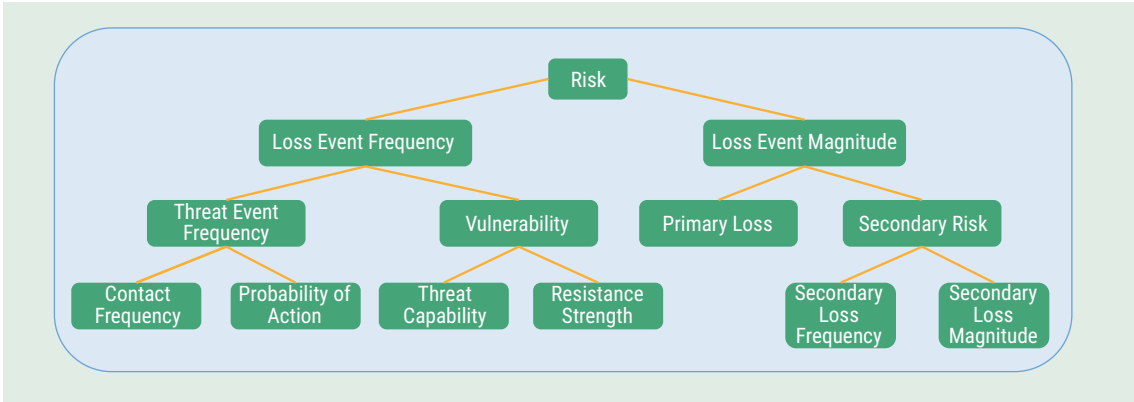
- **Risk reporters**—Security professionals who help identify and report security risk. Risk reporters work interdepartmentally to identify, assess and reduce security risk factors by recommending specific measures that can improve the overall security posture. They also have the overall responsibility to oversee the coordinated activities to direct and control risk.
- **Risk owners**—Business owners and operations managers who manage the security risk scenarios that exist within their business areas. They are responsible for implementing corrective actions to address process and control deficiencies, and for maintaining effective controls on a day-to-day basis. They assume ownership, responsibility and accountability for directly controlling and mitigating risk.

> "THE RISK ANALYSIS PROCESSES NORMALIZE RISK SCENARIOS INTO THE FAIR MODEL, PRIORITIZE THEM AND ASSESS THE ACTUAL FINANCIAL LOSS EXPOSURE ASSOCIATED WITH EACH RISK SCENARIO."

The team also established the following processes:

- **Identification**—Uncover the risk factors (or potential loss events) and define them in a detailed, structured format. Assign ownership to the areas of risk.
- **Assessment**—Assess the probable frequency of risk occurrence, and the probable impacts. This helps prioritize risk. It also enables comparison of risk relative to each other and against the organization's risk appetite.
- **Response**—Define an approach for treating each assessed risk factor. Some may require no actions and only need to be monitored. Other risk factors considered unacceptable require an action plan to avoid, reduce or transfer them.

Figure 2—Open FAIR Risk Ontology



- **Monitoring and reporting**—Reporting is a core part of driving decision-making in effective risk management. It enables transparent communication to the appropriate levels (according to Swisscom's internal rules of procedure and accountability) of the net or residual risk.

Thus, the risk analysis processes normalize risk scenarios into the FAIR model, prioritize them and assess the actual financial loss exposure associated with each risk scenario. In parallel to the strategic risk analysis of the top risk areas, the FAIR team can also provide objective analysis to support tactical day-to-day risk or spending decisions. These analyses can help assess the significance of individual audit findings and efficacy of given controls, and can also justify investments and resource allocations based on cost-benefit.

The FAIR team is constantly improving and simplifying the process of conducting quantitative risk assessments using the FAIR methodology. In a workshop-based approach, the team tries to understand the people, processes and technologies that pose a risk to the business.

Ongoing Work Items

As of early 2020, Swisscom's core FAIR team consists of three part-time staff members. This team is part of a virtual community of practitioners concerned with security risk management in the company.

The team continues to drive the following work items:

- Risk scenario analysis
- Risk scenario reporting
- Risk portfolio analysis and reporting
- Internal training
- Improving the tool chain
- Improving risk assessment processes

Risk Scenario Analysis

The FAIR team performs the deep analysis of risk scenarios using an open-source tool adapted for Swisscom's use. Based on the analysis, it provides quantitative estimates for discussion with risk, IT and business analysts (**figure 3**).

Figure 3's loss exceedance curve depicts a common visualization of FAIR risk analysis output. The Y axis, Probability of Loss or Greater, shows the percentage of Monte Carlo simulations that resulted in a loss exposure greater than the financial loss amount on the X axis. Each Monte Carlo simulation is like a combination of random coin tosses of all the risk components of the FAIR risk ontology shown in **figure 2**. During the analysis, the FAIR team generates calibrated estimates for the range of values for each risk component. A calibrated estimate is an SME's best estimate of the minimum, maximum and most likely probability of the risk factor. Each estimated risk factor in the ontology is fed into the Monte Carlo simulation by the FAIR tool.

> "THE FAIR TEAM PERFORMS THE DEEP ANALYSIS OF RISK SCENARIOS USING AN OPEN-SOURCE TOOL ADAPTED FOR SWISSCOM'S USE."

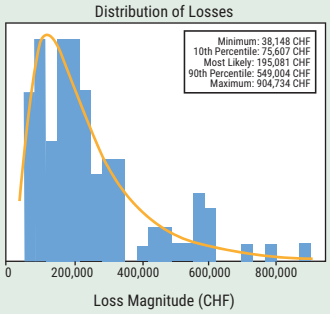
Although the SMEs tend to provide fact-based, objective information for use in estimates to the best of their abilities, challenges can arise when presenting initial completed analyses to stakeholders.

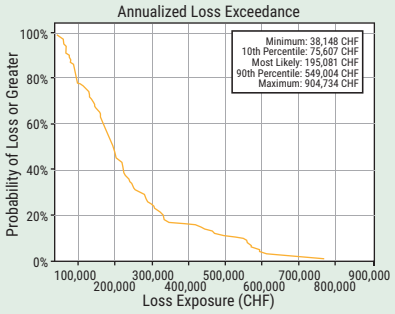
"Risk owners tend to want to push the numbers down, but security leaders try to keep them up," Voicu explained.

Often, however, the stakeholders can meet in the middle for a consensus and come together on risk treatment proposals with a strong return on security investment (ROSI) measured by the difference between the inherent risk analysis and the residual risk analysis.

In the case of the customer portal data breach scenario, the FAIR team and the business stakeholders agreed on adding two-factor authentication (2FA) for portal users. This solution had a low cost because Swisscom already possessed the 2FA capability and needed only to change the default policy configuration to require 2FA. **Figure 5** shows a diagram of the current (or inherent) vs. residual risk analysis amounts using

Figure 3—Results of a FAIR Analysis





Annualized View

Per-Event View

Per-Event Primary Losses			
	Min	ML	Max
Loss Events/year	0	0.3	1
Loss Magnitude	18,048	50,200	104,734
Vulnerability			**81.76%**

Per-Event Secondary Losses			
	Min	ML	Max
Loss Events/year	0	0.07	1
Loss Magnitude	20,100	144,881	800,000
Total Single Loss Event	**38,148**	**195,081**	**904,734**

fictional numbers aligned with the assessment shown in **figure 4**. The current risk depicts the amount of risk estimated to exist without adding new controls to the current state. The residual risk shows the amount of risk estimated to exist after the hypothetical addition of the new 2FA control.

Risk Scenario Reporting

Once the analysts reach a consensus on estimates during working meetings, the FAIR team provides management reports using one-page summaries with quantitatively scaled, red-yellow-green diagrams based on the risk thresholds (i.e., risk appetite) of the risk owner (**figure 4**). The Swisscom FAIR team has found that often management trusts the teams' analysis and does not want to see the FAIR details. However, the numerical analysis drill-down is available if management wishes to understand or question the risk ratings and recommendations.

Risk Portfolio Analysis and Reporting

Strategic risk analyses are typically driven by boards and C-level executives with the intent of understanding, communicating and managing security risk holistically and from a business perspective. This enables executives to define their risk appetite and boards to approve it. The organization can also right-size security budgets, prioritize risk mitigation initiatives and accept certain levels of risk. Strategic risk analyses conducted by the FAIR team can be used to measure risk trending over time. The FAIR team began providing a strategic risk analysis report on a quarterly basis to the board of directors in early 2020. **Figure 6** provides an example.

Internal Training

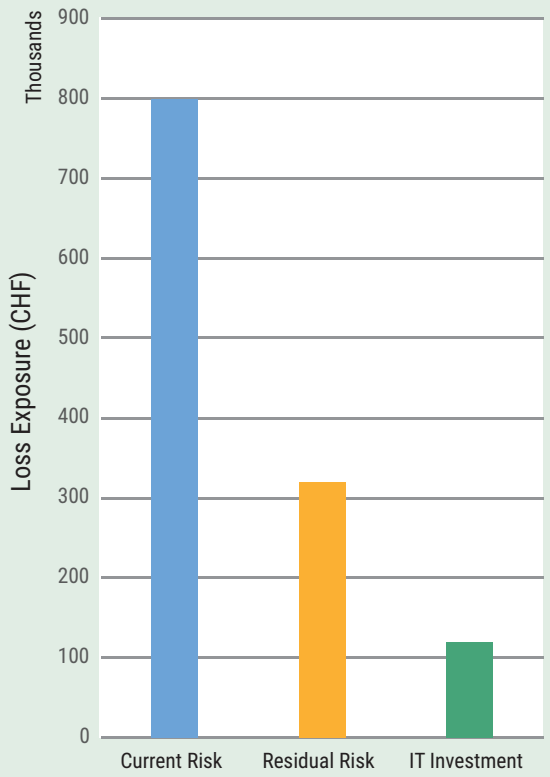
The team began by socializing FAIR concepts among the cybersecurity functions and other internal groups to establish a broader FAIR adoption. The team provided workshops and training for additional security staff as well as stakeholders and aims to further extend training offerings.

Improving the Tool Chain

Swisscom has assessed several FAIR risk quantification tools:

- **Basic risk analysis**—Pen and paper, qualitative method using *Measuring and Managing Information Risk: A FAIR Approach*[2]
- **FAIR-U**—Free, basic version of RiskLens. For noncommercial use only. Registration required.
- **RiskLens**—Commercial, fee-based FAIR application
- **Evaluator**—Free open-source application, OpenFAIR implementation built and run on R + Shiny

Figure 4—Risk Treatment Evaluation



CHF 480,000 Average Risk Reduction
CHF 120,000 IT Investment

Figure 5—One-Page Summary Risk Report

RISK-00000—Data Breach Customer Data on Swisscom Customer Portal

Risk Scenario Description:
Data loss/data breach of sensitive customer data (e.g., customer data records, billing information) due to weak authentication (username and password). Potential violation of legal and regulatory requirements according to DSG and FMG as well as contractual infringement (compliance).

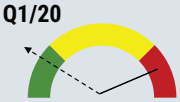
Risk Owner: Customer Portal Product Owner
Security Responsible: Security Officer Residential Customers

Status Measures: On track

- Monitoring access control
- Regulating access rate (throttling)
- Verification of external employees (Identity management)

○ Not started ◑ In Progress ● Implemented

Target: Q1/20



Value at risk

Financial	● ● ● ●
Regulatory	● ● ● ○
Reputation	● ○ ○ ○

Business unit at risk

Primary	**Residential customers**
Secondary	n/a

Assets at risk

Confidentiality	●
Integrity	○
Availability	○
Safety	○

Ease of exploitability

Insider	● ● ● ○
External attacks	● ○ ○ ○

Risk mitigation strategy

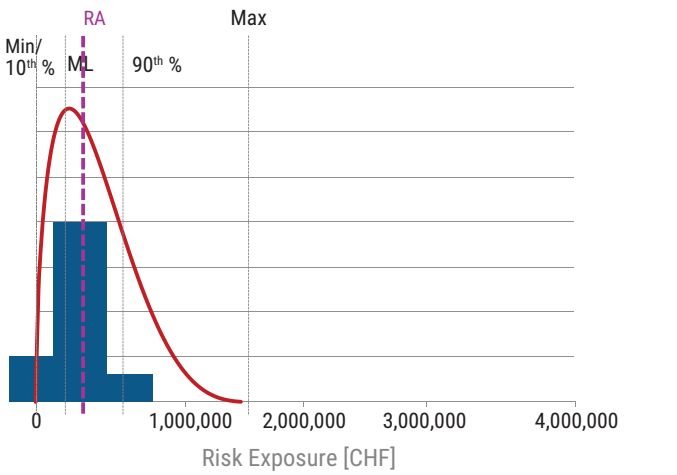
Avoid	○	Reduce	●
Accept	○	Transfer	○

- **PyFair**—FAIR implementation built on Python
- **FAIR Tool**—Free open-source application built on R + Shiny
- **OpenFAIR Risk Analysis Tool**—OpenGroup's Excel-based application. Registration required.
- **RiskQuant**—Open-source application built in Python

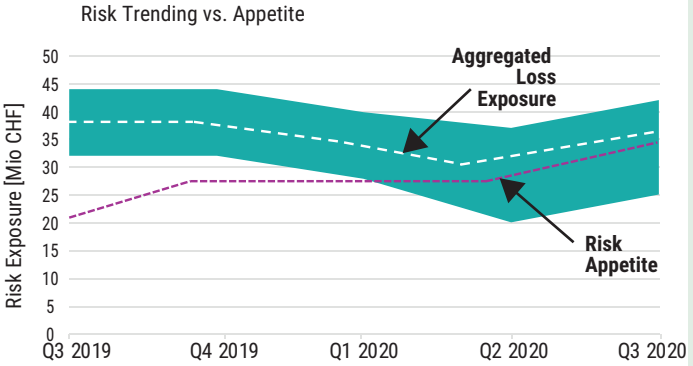
In the end, Swisscom has opted for developing the tool in-house by adapting the RiskQuant analysis module. Swisscom is improving the tool chain by enhancing the analysis module with reporting capabilities and multiscenario aggregated analyses capabilities. The in-house tool is designed to support the entire security risk management life cycle—from risk identification and scoping to risk analysis and prioritization to the evaluation of risk mitigation options to risk reporting. The team is progressively adding additional modules to the in-house tool, such as:

- **Decision support**—Enabling decisions on the best risk mitigation options based on their effectiveness in reducing financial loss exposure. The tool already provides the capability for conducting comparative and cost-benefit analyses to assess what changes in security strategy or what risk mitigation options provide the best ROI.
- **Security data warehouse**—Swisscom's existing security data warehouse defines, stores and manages critical assets in a central location. Risk tools can leverage this information in risk

Figure 6—Risk Portfolio Reporting



Maximum: 15 Million **90th %:** 6.25 Million **Most Likely:** 2.25 Million
10th %: 0.5 Million **Minimum:** Million



Risk **Top 10 Risks**

RISK-ID		Status
R-00123	Data breach/confidentiality loss on crown jewel database due to cybercriminals.	▼
R-00456	Data breach/confidentiality loss on crown jewel database due to insiders.	▶
R-00789	Availability loss on critical business service due to cybercriminals.	▶
R-00xxx	Availability loss on critical business service due to malicious insiders.	▲

Control Risk **Top 10 Control Deficiencies**

CD-0123	Audit and monitoring	87%
CD-00456	Segregation of duties	55%
CD-00789	Configuration and patch management	36%
CD-00xxx	Access control	29%

Initiatives **Top Security Initiatives**

SI-0012	Security Initiative 1	
SI-0034	Security Initiative 2	
SI-0056	Security Initiative 3	
SI-0xxx	Security Initiative 4	

> WHAT STARTED AS A SHORT-TERM OPPORTUNITY TO NORMALIZE AND PRIORITIZE RISK TURNED INTO A LONG-TERM JOURNEY TO MANAGE A PORTFOLIO OF SECURITY INVESTMENTS.

scenarios related to assets. Stakeholders can also view the risk areas and issues associated with their assets and understand the risk posture on a continuous basis.

- **Risk portfolio**—The module aims to provide a deeper understanding of enterprise risk as well as aggregate or portfolio views of risk across business units. This module will also allow Swisscom to set key metrics to measure and manage cyberrisk, such as risk appetite, and conduct enterprise-level what-if analyses.

Improving Risk Assessment Processes
To enhance Swisscom's ability to identify risk scenarios deserving full FAIR analyses, the FAIR team is creating a triage questionnaire that will enable IT and security staff to perform a quick assessment of issues before submitting them as risk areas for analysis. The triage consists of 10 yes-or-no questions and requires less than 15 minutes to complete.

Lessons Learned

It is instructive to review lessons learned after establishing a risk program:

- **Bring the discussion to the business owners of the risk and the budget.** Prior to the FAIR program, the risk acceptance process was not formally aligned to Swisscom's rules of procedures and accountability. These rules provide a process whereby executives are authorized to accept risk up to certain levels, and how to decide whether higher risk can be accepted. When the FAIR program was introduced, Swisscom began identifying the executives who will end up covering the losses if risk scenarios actually materialize. With very rare exceptions, those identified business executives should also be responsible for owning or accepting risk.
- **Focus on the assumptions, not the numbers**. As noted earlier, risk ratings or quantities can become politicized. Some parties may desire lower or higher results depending on their own agendas. The FAIR model can act as a neutral arbiter if stakeholders understand the assumptions. Although participants in the risk process will always have agendas, focusing on assumptions puts the discussion on a more logical footing.
- **Be flexible about reporting formats.** Once risk analysts learn FAIR, there can be a temptation to take a "purist" position and evangelize the methodology too ardently. However, not all stakeholders were interested in the complexity of simulations and ontology. The Swisscom FAIR team found that the one-page risk summary using a familiar "speedometer" diagram (**figure 4**) facilitated easier acceptance of quantitative analysis results from the business risk owners. It should be noted that quantitative risk values still underlie the one-page summary. Behind the scenes, quantitative risk appetites and risk estimates determine a risk's status as red, yellow or green.
- **Maintain momentum.** When the FAIR journey started, the project scope was fluid. The FAIR team has found that the more the scope expanded, the more resources were required to provide increasing value. What started as a short-term opportunity to normalize and prioritize risk turned into a long-term journey to manage a portfolio of security investments.

Metrics

Swisscom is currently preparing to begin tracking formal risk metrics. **Figure 7** displays planned metrics and observations on the data collected or expected at this time.

Figure 7—Swisscom Proposed Metrics	
Metric	**Post-FAIR Implementation**
Percent of risk below/above risk appetite	Approximately 5 percent of risk above risk appetite
Percent of critical assets with loss exposure above the risk appetite	Undisclosed number has been calculated
Percent of business units covered by the security risk management process	Approximately 80 percent
Percent of large solutions and agile release trains undergoing risk assessments	Approximately 60 percent of security projects that get worked on are now validated by quantitative risk assessments
Complies with regulatory requirements (Yes/No)	Yes
Dollar value of inherent risk exposure reduction due to risk program	Swisscom has reduced millions of dollars of loss exposure by its own measurements.
Cost savings (dollar value)	Saved on canceled projects or phased-out systems
Number of trained risk specialists	8
Number of trained stakeholders conversant with the methodology	Security risk team and stakeholders are able to perform "on the fly" quick assessments using the FAIR model
Average time required to perform quantified assessment	Typical risk assessment takes a couple of days to two weeks depending on the scenario's scope
Number of identified control gaps or vulnerabilities contributing to top risk	Undisclosed number has been calculated
Number of top gaps resolved during reporting period	Undisclosed number has been calculated

Benefits

Swisscom considers the benefits of the FAIR process to be that the company can:

- Objectively assess information risk, which enhances the ability to approve large security initiatives
- Measure aggregated information risk exposure
- Break out risk exposure for business units, risk categories and top assets or crown jewels

Next Steps

The team is optimistic as of 2020 about the ability of the FAIR program to enable data-driven decision-making. The team is improving its risk reporting portfolio to produce reports such as the ones shown in **figure 6** both at an enterprise level and at the business unit level. The team plans to conduct ROI analyses to assess the effectiveness of security spending. It is also currently in discussions with operational risk management and enterprise risk management (ERM) functions on the possibility of expanding the use of FAIR, especially in the domain of operational availability risk.

Endnotes

1 Salah, O.; "Thirteen Reasons Why Heat Maps Must Die," FAIR Institute Blog, 28 November 2018, *https://www.fairinstitute.org/blog/13-reasons-why-heat-maps-must-die*

2 Freund, J.; J. Jones; *Measuring and Managing Information Risk: A FAIR Approach*, Butterworth-Heinemann, United Kingdom, 2014, p. 205–214