THE Open GROUP

Calculating Reserves for Cyber Risk

Integrating Cyber Risk with Financial Risk

A White Paper by:

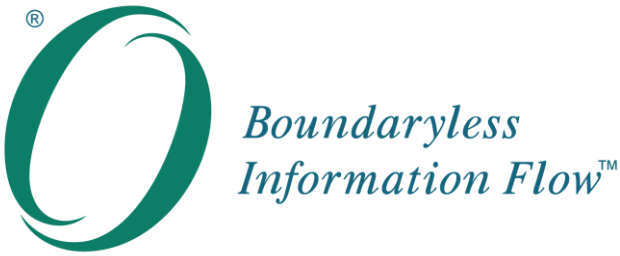
Mike Jerbic and Dr. Robert Mark

November 2021

Calculating Reserves for Cyber Risk: Integrating Cyber Risk with Financial Risk
Document No.: W215

Published by The Open Group, November 2021.
Any comments relating to the material contained in this document may be submitted to:
The Open Group, Apex Plaza, Forbury Road, Reading, Berkshire, RG1 1AX, United Kingdom
or by email to:
ogpubs@opengroup.org

Table of Contents



Boundaryless Information Flow ™
achieved through global interoperability
in a secure, reliable, and timely manner

Executive Summary

Financial Institutions (FIs) must have sufficient reserves to ensure that they can survive expected plus unexpected reasonably foreseeable losses in their banking book and trading book. FIs include losses associated with cyber risk in their reserve calculations, but calculating these cyber risk reserves has been a significant challenge. This document demonstrates to Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), Chief Risk Officers (CROs), and cyber risk analysts in FIs how cyber risk can be quantified in economic terms as well as calculate reserve requirements. Quantifying cyber risk in economic terms integrates cyber risk with other risks too, which allows boards and management to treat cyber risk as an enterprise risk, not just an IT risk. Presenting cyber risk in enterprise risk terms provides information security professionals with a new insight into a security program's business value to management and the board.

FIs have always had to reserve capital to cover their operational risks, including cyber risk, but the significance of cyber risk has risen along with the specialization of financial technology service providers and deeper information technology supply chains. Effectively measuring and managing cyber risk is essential to building and operating a globally interoperable, secure, and reliable financial system.

Introduction

Verizon corrected two "myths" in its 2020 Data Breach Investigation Report.[1] First, external, not internal, actors are responsible for the majority of data breaches; and second, the motivation behind breaches is primarily financially motivated, in contrast with highly publicized but rare espionage-motivated attacks. Globally, cybercrime is estimated to inflict damages of $6 trillion in 2021 and grow to $10.5 trillion by 2025.[2] To put this damage figure into perspective, 2021 world gross domestic product is estimated at $87.3 trillion.[3] Cybercrime is estimated to represent a transfer of wealth to criminals of about 6.9% of world output, or approximately one out of every 14.5 dollars of total world production.

Financial Institutions (FIs) are targets for two reasons: first, banks are where the money is; and second, banks have Personally Identifiable Information (PII) that bad actors can monetize on the dark web.[4] Systemically Important Financial Institutions (SIFIs) have a lot of both. With the impact of cybercrime estimated at 6.9% of global output and with the role the financial sector has as an intermediary in keeping the global economy functioning, FIs are both unique targets for cyber criminals and systemically significant risks to global prosperity. FIs are attractive targets for financially motivated criminals seeking both the cash and the valuable information these institutions have.

In addition to the attractiveness of the target, new vulnerabilities to the financial services sector have emerged through the Financial Technology (FinTech) and Information Technology (IT) supply chain. FIs focus on their core competencies and outsource the rest – such as to other specialists in FinTech and cloud service providers – in order to innovate new services cost effectively. This deep, multi-layered, and highly specialized supply chain exposes FIs to new third-party risks. The multiple layers of third-party risks often obscure those risks. Although FIs can innovate and specialize through outsourcing, they cannot outsource the risk that results from it. Ultimately, the FI itself must assess, manage, and reserve capital against the risk faced from its outsourcing and innovation choices.

For example, a key cybersecurity tool supplier whose product is widely used by cloud-based IT service providers to both government and the private sector suffered a major breach that exposed the tool supplier, its cloud service provider customers, and, ultimately, the customers of the service providers to data exfiltration risk.[5] At the time of writing, the implications of the breach are still being investigated. The suspected hacker is a nation state actor, and the primary target appears to be government data. There are estimates that the cyber insurance industry faces losses of up to $90 million[6] and that the overall cost to all parties affected could cost up to $100 billion.[7]

[1] Refer to Verizon: Data Breach Investigations Report 2020 (see References).

[2] Refer to Cybersecurity Ventures: Cybercrime to Cost the World $10.5 Trillion Annually by 2025 (see References).

[3] From the World Bank graphic on GDP and the Global Economic Prospects (Full Report) – see References. The 2019 figure of world GDP of $87.8 trillion was multiplied by estimated growth rates for 2020 and 2021 of -4.3% and +4.0%, respectively.

[4] According to ZDNet (see References), PII and payment account information associated with a US-issued payment card sells for about $17 per card on the dark web. Internationally issued payment card information sells for about $210 per card.

[5] Refer to Wall Street Journal: Suspected Russian Cyberattack Began with Ubiquitous Software Company (see References).

[6] Refer to Insurance Business America: SolarWinds Trojan Hack Estimated to Cost Cyber Insurers $90 Million (see References).

[7] Refer to Roll Call: Cleaning up SolarWinds Hack May Cost as Much as $100 Billion (see References).

Calculating Reserves for Cyber Risk: Integrating Cyber Risk with Financial Risk

FIs need to set aside sufficient reserves to cover both expected and unexpected losses. Expected losses are the estimated average losses over a given time period (for example, one year). Unexpected losses are the estimated losses beyond the estimated average losses up to a particular confidence level (for example, 99%). Reserves are the sum of the expected losses and unexpected losses over a particular time period.

FIs have extensive experience and analytical resources to measure and prudentially manage risk for two reasons. First, FIs need to manage their own risk effectively to stay in business and therefore measure risk in economic terms in order to have sufficient reserves to absorb losses within a given degree of confidence. Second, FIs need to comply with international financial risk management regulation. For example, banks need to comply with Basel III Capital Accords,[8] which requires a bank to have sufficient reserves to absorb losses as calculated through regulatory accords.

Operational risks arising from IT, external cyber criminals, and unreliable data are increasing and must be included in an institution's overall risk calculations so that reserves can be allocated to these risks. In this document, we show how cyber risk can be measured in the same economic terms as other risks, such as the credit risk associated with loan portfolios or the market risk associated with trading stocks and bonds. In particular, the Open FAIR™ Body of Knowledge[9] can be used as an input to calculate regulatory and economic reserves for cyber risk.

Effective Enterprise-wide Risk Management (ERM) in FIs is a responsibility shared by the board of directors, senior executive management, and business units. They must align on common business objectives using the language and framework of risk management to inform effective decision-making. This document argues and demonstrates through example that:

- Cyber risk should be measured in economic terms, which in turn provides FIs a clear connection between cybersecurity and the institution's business performance
- Cybersecurity controls can be valued by how they affect regulatory and economic reserve requirements

  A sophisticated cybersecurity program's ability to reduce required reserves gives the Chief Risk Officer (CRO) and Chief Information Security Officer (CISO) the foundation they need to influence a bank's decisions on reserve requirements. Management and the board can also make effective cost-benefit trade-offs by measuring cyber risk and its effect upon Risk-Adjusted Return on Capital (RAROC).
- Quantifying cyber risk in economic terms lets the financial risk modeling and cyber risk modeling communities share common concepts, such as the distribution of Loss Event Frequency (LEF) and Loss Magnitude (LM) to integrate cyber risk with other FI risks

  Using the language and analytic framework of quantitative risk analysis, executive management and the board can expect to see how ongoing information security operations and new information security

[8] See https://en.wikipedia.org/wiki/Basel_III. The Basel III Capital Accords set the rules for the amount of regulatory capital that banks must hold. These accords assign regulatory capital to market risk, credit risk, operational risk, business risk, and "other" risk. Reputational risk and strategic risk are the two risk types that are typically included in "other" risk. Economic capital is the amount of capital banks need to hold based on using their own internal risk models to capture the amount of risk.

[9] The Open FAIR Body of Knowledge is comprised of The Open Group Standard for Risk Taxonomy (O-RT) and The Open Group Standard for Risk Analysis (O-RA) (see References).

control investment strategies affect business performance.

This White Paper series helps the board, senior executives, and information security organization to work collaboratively to effectively manage the business implications of the risk associated with adverse cyber events.

This document (the first of the series) covers how to quantify an FI's cyber risk in economic terms, including the impact of cyber risk in economic and regulatory capital requirements. To do that, this document is organized as follows:

- Value at Risk (VaR): A Core Concept of Financial Risk Management (on page 8) discusses Value at Risk (VaR) as a common financial risk measure and how that measure is used to measure the market risk of a financial asset
- Value at Risk (VaR): Credit Risk (on page 13) discusses VaR as a measure of credit risk associated with bond and loan obligations
- Capital (on page 19) presents the role of capital reserves as a backstop to withstand adverse financial outcomes in an FI
- Risk of a Portfolio that Includes Cyber Risk (on page 20) discusses and provides an example of measuring VaR for cyber risk so that capital reserves can be applied to cyber risk just as they are for market and credit risk
- Risk-Adjusted Return on Capital (RAROC) (on page 33) presents the RAROC metric and approach to making informed risk-based business decisions on financial deals
- Measuring Return on Security Investment (ROSI) (on page 38) compares and contrasts RAROC and the conventional ROSI technique to make informed security control investment decisions
- The Conclusion (on page 41) closes the document by emphasizing the commonality among measures of market risk, credit risk, and quantitative cyber risk and some of its implications

The second White Paper of the series – Calculating Reserves for Cyber Risk: Vetting Cyber Risk Models – discusses how a quantitative cyber risk model reflects what is known, unknown, knowable, and unknowable about a cyber risk scenario. In particular, the second White Paper:

- Describes what is known as the anatomy of a cyber risk scenario and the taxonomy of risk factors that apply to it
- Reflects what is unknowable about the scenario by representing risk factors as distributions whose parameters must be estimated
- Discusses how to account for that uncertainty parsimoniously

Throughout the second White Paper, the parsimony between financial risk models and cyber risk models is emphasized to demonstrate the accuracy and relevance of applying quantitative cyber risk analysis in FI risk modeling.

Value at Risk (VaR): A Core Concept of Financial Risk Management

The risk management community converged on a Value at Risk (VaR) approach for measuring risk, which necessitated exploring the key features of VaR.

VaR can be defined in the case of market risk as the worst-case loss that might be expected from holding a security or portfolio over a given period of time (say a single day, or 10 days) at a specified level of probability (known as the "confidence level", designated *c*). For example, if a position has a daily VaR of $10 million at the 99% confidence level ($c = 0.99$), the realized daily losses from the position will on average be higher than $10 million on only one out of every 100 trading days (i.e., two to three days each year). If returns (gains and losses) are normally distributed, then a 99% VaR corresponds to 2.33 standard deviations from the mean return, which for illustrative purposes is assumed to be zero (see Figure 1).

VaR can be thought of as a measure of the economic capital reserves needed to absorb unexpected losses to a given predetermined level, $1 - c$.

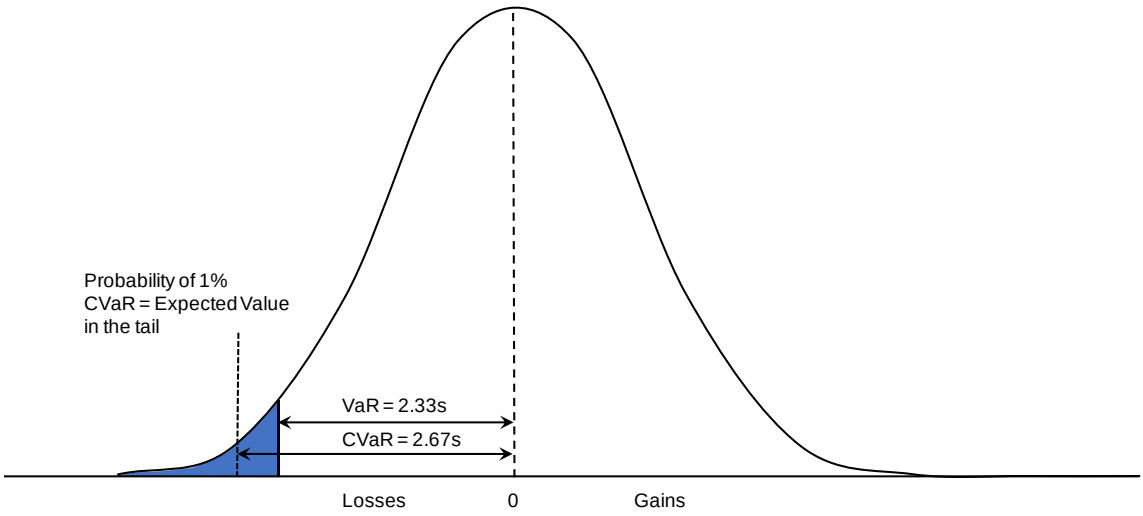


Figure 1: VaR Calculation at a 99% Confidence Interval

Ultimately, assumptions must be made about how losses are distributed. For example, VaR can be analyzed for any underlying distribution, such as a Triangular distribution, a Uniform distribution, a Normal distribution, or the resulting distribution derived from an historical data set or Monte Carlo Simulation (MCS).

This approach is similar to what has been adopted in the Open FAIR risk analysis method. An Open FAIR user must decide on the initial distribution (say the Triangular distribution) to calculate an LEF, which is subsequently translated into a selected number of cyber Loss Events in an MCS. Similarly, the analyst

models LM as a distribution of losses. Combining LEF and LM through an MCS yields a distribution of simulated annual loss outcomes that can be analyzed for a VaR.

Most of the time, banks pick a higher confidence level than the 99% set by the regulator[10] in order to determine economic capital. However, the time horizon in economic capital calculations in a trading portfolio may vary from one day for very liquid positions, such as a government bond, to several weeks for illiquid positions, such as long-dated Over-the-Counter (OTC) equity derivative portfolios. Regulators initially set the time horizon to 10 days for any position in the trading book for calculating regulatory capital.

More formally, if V denotes the current market value[11] of the position, $E(V)$ denotes the expected value of that position at the end of time horizon H, R is the rate of return[12] over the horizon H, μ is the expected rate of return over H, and R^*[13] denotes the rate of return corresponding to the worst-case over H at the c confidence level; e.g., 99%, and if the worst case $V^* = V(1+R^*)$,[14] then:

$$VaR(H; c) = E(V) - V^* = V(1+\mu) - V(1+R^*) = V(\mu - R^*)$$

Single Position Example

We will first take a single position example:

$V = \$100$, $\mu = 5\%$ and $R^* = -20\%$, then $VaR = \$100\,(0.05 - (-0.20)) = \$25$

A portfolio R_v that consists of multiple positions, each assumed to be normally distributed with an expected return μ_i and standard deviation σ_i, is normally distributed with an expected return μ_v and standard deviation σ_v and designated $R_v \sim N(\mu_v, \sigma_v)$. The portfolio's expected return μ_v is a weighted average of each position's expected return μ_i with the relative weighting factor ω_i. The portfolio's standard deviation is more complicated and depends upon how the positions are correlated with the correlation coefficient ρ.

[10] Regulatory capital is the minimum amount of capital imposed by the regulator. Economic capital may differ from regulatory capital because the chosen confidence level and/or the chosen time horizon differ in both calculations. FI management may have many reasons to have economic capital differ from regulatory capital. For example, a bank's major depositors may demand a bank to take lower risks than regulators require in order to do business with the bank. Capital requirements depend upon regulatory requirements and market requirements. The stricter of the two determines how much capital is needed for a particular situation.

[11] It is common practice to value each position at the end of each trading day – what is called "marked-to-market".

[12] The rate of return is measured in percent. Rates of return that are less than zero represent losses.

[13] R^* for a loss is a negative number.

[14] When R^* is negative, this sum is less than 1, so V^* is less than both V and its expected value $E(V)$.

For a two-position portfolio with a correlation of ρ between the two positions, μ_v and σ_v are calculated as shown below:[15]

$$\mu_V = \sum_{i=1}^{2} \omega_i \mu_i$$

$$\sigma_V^2 = \omega_1^2\sigma_1^2 + \omega_2^2\sigma_2^2 + 2\omega_1\omega_2 \operatorname{cov}(R_1, R_2) = \omega_1^2\sigma_1^2 + \omega_2^2\sigma_2^2 + 2\omega_1\omega_2\rho\sigma_1\sigma_2$$

The VaR of the portfolio now can be derived as done for a single position using μ_v and σ_v as the parameters in the VaR equation.

Multiple Position Example

We will now consider an example calculation for multiple positions.

Assume that the portfolio is composed of 100 shares of S_1 and 120 shares of S_2 valued at $91.7 and $79.1, respectively. Then, the value of the portfolio is:

V = n1 S1 + n2 S2 = $18,662

and the relative investments[16] in both stocks are respectively:

$\omega 1 = 0.49$ and $\omega 2 = 0.51$

Further assume that:

- S_1 has a mean return of .155% and standard deviation of 2.42%
- S_2 has a mean return of .0338% and standard deviation of 1.68%
- The correlation is .14 between S_1 and S_2

so that the one-day mean and standard deviation of the rate of return on the portfolio are equal to 0.093% and 1.55%, respectively.

The one-day VaRs at the 99% confidence level are:

VaR1(1; 99) = 2.33 σ1 n1 S1 = $517[17]

VaR2(1; 99) = 2.33 σ2 n2 S2 = $370

VaRV (1; 99) = 2.33 σV V= $677

[15] Matrix notation is used in risk analysis to simplify representation on how to calculate VaR in cases where the number of different shares of stocks become sufficiently large. The matrix below denotes the 1x2 weight vector: Ω is the variance–covariance matrix, σ is the 2x2 diagonal standard deviation matrix, C is the 2x2 correlation matrix, and w^T denotes the transpose of w. For this example, the matrix equation is equal to:

$$(\omega_1\ \omega_2)\begin{pmatrix}\sigma_1^2 & \rho\sigma_1\sigma_2\\ \rho\sigma_1\sigma_2 & \sigma_2^2\end{pmatrix}\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix} = (\omega_1\ \omega_2)\begin{pmatrix}\sigma_1 & 0\\ 0 & \sigma_2\end{pmatrix}\begin{pmatrix}1 & \rho\\ \rho & 1\end{pmatrix}\begin{pmatrix}\sigma_1 & 0\\ 0 & \sigma_2\end{pmatrix}\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}$$

[16] 0.49 = 100 * $91.7 / $18,662 & 0.51 = 120 * $79.1 / $18,662.

[17] $517 = 2.33 x 2.42% x 100 x $91.7.

Note that VaR_V (1; 99) = $677 is less than the sum of VaR_1(1; 99) and VaR_2(1; 99); i.e., $887. VaR is quite sensitive to the correlation structure of the risk factors. The difference, $210, represents the portfolio effect from the fact that correlation is less than 1 between equity returns. VaR is not a sub-additive measure;[18] therefore, the portfolio effect in certain cases may not occur.[19]

Tail Risk

One of the biggest criticisms of VaR is inherent in the methodology. VaR does not attempt to offer any indication of how large a loss might be once the loss exceeds the VaR number. In other words, VaR fails to capture what is known as "tail risk".

For example, we might hope that a portfolio with a daily VaR of $100 million at the 99% confidence level is unlikely to experience losses above $100 million more often than once every 100 days (i.e., 1% of the time), or two to three times in one year. We therefore *expect* losses of *over* $100 million on around three trading days for any particular year. The expected value of the losses in the tail is the Conditional VaR (CVaR), and gives an indication of the magnitude of the potential losses at a given confidence level (see Figure 1).

CVaR = The expected loss given that the loss exceeds the VaR[20] at a given confidence level.

Different approaches can be applied to estimate VaR and CVaR simultaneously. For a normal distribution, VaR and CVaR can be derived directly from the volatility of the portfolio return distribution. For example, assuming zero expected profit/loss and confidence levels of 99%, then VaR can be found directly from the normal distribution, which shows quantile values of 2.33, respectively. The corresponding CVaR is 2.67 or almost 15% higher than the VaR, respectively (see Figure 1). CVaR always exceeds the corresponding VaR at the same confidence level.

VaR as a Common Financial Services Risk Metric

The common risk metric VaR is defined as the difference between the magnitude of loss at a given confidence interval and the expected outcome (profit in the case of pursuing a business opportunity or a loss in the case of an operational risk such as a cyber risk). Subsequent sections in this document apply VaR techniques both to credit risk and to cyber risk using the Open FAIR risk analysis method. In each example, capital reserves can be calculated for the risk using the VaR metric. In each instance, VaR expresses:

- A frequency of loss derived from the time horizon *H* and confidence level *c*
- A magnitude of loss derived from the calculation VaR = $V(\mu\text{-}R^*)$

[18] VaR is not a sub-additive measure since the VaR of a portfolio can – in some cases – be larger than the sum of VaRs of the individual assets in the portfolio.

[19] For example, this occurs in cases where distributions that cluster around the mean and present only a few outliers far away in the tail of the distribution. Such a distribution is bimodal; i.e., it exhibits a hole between the tail and the mean. VaR may be very small at the 99% confidence level but may jump to a much higher value at higher confidence levels such as 99.9%.

[20] CVaR is also called Expected Shortfall (ES). ES is a conditional expectation that is obtained by dividing the probability weighted average of the losses beyond VaR by the probability of the losses beyond VaR; i.e., 1-α, where α is the confidence level. ES is a coherent measure but, as pointed out, VaR is not sub-additive. A risk measure is coherent if among other things it is sub-additive. A good discussion on a coherent measure can be found in Appendix 2 of Nan Tie & Mark: Parsimony – A Model Risk Paper (see References).

Calculating Reserves for Cyber Risk: Integrating Cyber Risk with Financial Risk

Converging upon a common unit of measure allows risk professionals across multiple specializations to communicate results that can be integrated and acted upon throughout the FI. The language and metrics of risk allow for meaningful communication across organizational specialties so that management can look at risk consistently throughout the enterprise. Only by measuring cyber risk in the same economic terms as other financial risk can an FI's board and senior management view cyber risk as an enterprise risk.

By measuring cyber risk in economic terms consistent with other enterprise risks, cybersecurity and risk professionals speak the language of business, not of their technical specialty. It has long been said that many cybersecurity professionals do not "understand the business" when they make proposals for new cybersecurity proposals. By presenting those proposals in the terms of risk and risk reduction upon which senior management bases decisions, cybersecurity professionals indeed demonstrate that they understand the business.

Value at Risk (VaR): Credit Risk

Credit risk refers to how the market price of a loan or a bond changes over time due to the obligor not fulfilling its commitments (defaulting within the period) or due to changes in the likelihood of the obligor not being able to fulfill commitments in the future as seen through the eyes and models of the credit rating agencies (changes in the estimated probability of default in the future) as measured by an upgrade or downgrade of an obligor's credit rating. Obligors have a probability of defaulting within a given time Period (PD), and lenders face a magnitude of Loss Given Default (LGD). The LGD is measured as the fraction of a loan or bond not repaid.[21] The change in a loan or bond's value as a function of the PD and LGD is reflected in the net present value of that obligation measured at some time in the future, say one year. The estimated market value of an obligation of one year from today is called its one-year forward price.

Bonds and loans are usually rated through the Nationally Recognized Statistical Ratings Organizations (NRSRO) such as Standard and Poor (S&P) Global Ratings, Moody's, and Fitch Group.[22] They have standardized analytic methods and defined qualitative labels that categorize the PD and LGD into credit ratings for the bond and issuer. By standardizing credit risk as a set of defined risk ratings, bonds can be aggregated into portfolios with known risk qualities. This makes them more easily managed within the financial sector.

A bank that lends to individual borrowers or a corporation establishes its own proprietary internal rating to evaluate borrowers. Credit risk evaluation is also informed by external credit risk analysis through an NRSRO, which is compared to a bank's own proprietary evaluation method.

Just as with other risks, it is insufficient to condense credit risk into one number such as the average loss of the bond. Bonds, just as other risks, have a VaR and economic and regulatory capital requirements associated with that VaR.

Credit VaR poses the following three significant challenges:

- First, the credit probability distribution is far from being a normal distribution
- Second, measuring the portfolio effect due to diversification is much more complex than for market risk
- Third, the information on loans is not as complete as it is for traded instruments such as bonds

The necessary steps to calculate a credit VaR for a bond[23] are as follows.

The first step is to specify a credit rating system, together with the probabilities of migrating from one credit quality to another over the credit risk time horizon. A transition matrix is the key component of the credit VaR model. A strong assumption is that all issuers within the same rating class are homogeneous credit risks – they have the same transition probabilities, the same PD, and the same LGD or recovery rates.

[21] As discussed later, the loss given default is equal to 1 – the recovery rate.

[22] Refer to: https://en.wikipedia.org/wiki/Big_Three_(credit_rating_agencies).

[23] Refer to Crouhy et al: The Essentials of Risk Management (see References).

Second, the risk time horizon needs to be specified. We will assume for illustrative purposes a one-year time horizon.[24]

The third step consists of specifying the forward discount curve at the risk horizon(s) for each credit category.[25] In the case of default, the value of the instrument should be estimated in terms of the "recovery rate", which is given as a percentage of face value or "par".

In the fourth and final step, this information is translated into the forward distribution of the changes in the portfolio value.

Example of Calculating VaR for a Bond

Step 1: Specify the Transition Matrix

The rating categories, as well as the transition matrix, are chosen from either NRSROs such as S&P or Moody's, or an FI's own internal rating system. Either way, a transition matrix that describes probabilities of credit rating migrating, in this example from one rating quality to another within one year, is shown in Table 1.

	Rating at Year-End (%)							
Initial Rating	**AAA**	**AA**	**A**	**BBB**	**BB**	**B**	**CCC**	**Default**
AAA	90.81	8.33	0.68	0.06	0.12	0	0	0
AA	0.70	90.65	7.79	0.64	0.06	0.14	0.02	0
A	0.09	2.27	91.05	5.52	0.74	0.26	0.01	0.06
BBB	0.02	0.33	5.95	86.93	5.30	1.17	0.12	0.18
BB	0.03	0.14	0.67	7.73	80.53	8.84	1.00	1.06
B	0	0.11	0.24	0.43	6.48	83.46	4.07	5.20
CCC	0.22	0	0.22	1.30	2.38	11.24	64.86	19.79

Table 1: Example of a Transition Matrix (Source: S&P Global Ratings)

Assume the bond issuer in the example is currently a BBB rating:

- The most probable situation is that the obligor will remain in the same rating category; for example, there is a probability of 86.93% that the BBB rating will remain the same rating one year from today
- The probability of the issuer defaulting within one year is only 0.18%

[24] If there is concern about the risk profile over a longer period of time, then multiple horizons can be chosen, such as one to 10 years.

[25] If we assume that the zero rates for 1 year and 2 years are respectively *R1* and *R2*, then the forward *Rate F(1,2)* is the interest rate 1 year from now such that $(1+R1) \times (1+F(1,2)) = (1+R2)^2$. *F(1,2)* is the forward rate one year from today for one year.

Step 2: Specify the Credit Risk Horizon

Assume the risk horizon is set at one year[26] and is consistent with the transition matrix shown in Table 1.

Step 3: Specify the Forward Pricing Model

The valuation of a bond is derived from the zero-curve corresponding to the rating of the issuer. A zero-curve is a set of discount rates for each credit rating used to discount cash flows of an obligation, taking into account its probability of default and loss given default over multiple years. "Spread" curves are required to price the bond since there are seven possible credit qualities in all possible future states. All issuers within the same rating class are then marked-to-market with the same curve. The zero curve is used to determine the present value of the bond.

The forward price of the bond one year from the present – that is, the estimated market value of a bond one year into the future including coupon payments – is derived from the forward zero-curve, one year ahead, which is then applied to the residual cash flows from year one to the maturity of the bond. Table 2 gives an example one-year forward zero-curves for each credit rating.

Rating	Year 1	Year 2	Year 3	Year 4
AAA	3.60	4.17	4.73	5.12
AA	3.65	4.22	4.78	5.17
A	3.72	4.32	4.93	5.32
BBB	4.10	4.67	5.25	5.63
BB	5.55	6.02	6.78	7.27
B	6.05	7.02	8.03	8.52
CCC	15.05	15.02	14.03	13.52

Table 2: Example of a One-Year Forward Zero-Curves (%) for Each Credit Rating (Source: CreditMetrics[27])

If the issuer remains at a BBB rating, then the one-year forward price, V_{BBB}, of the five-year, 6% coupon bond[28] is shown in Figure 2.

[26] The credit risk can also be calculated over an n^{th}-year time horizon by performing matrix multiplication. For example, if we assume for ease of illustration that the one-year transition matrix does not change over time, then the probability of a particular credit rating in the n^{th} year can be derived from the matrix multiplication of the one-year transition matrix.

[27] The CreditMetrics approach was initiated by JP Morgan and subsequently spun off to Risk Metrics, Inc. ,which in turn was acquired by MSCI in 2010. The reference is taken from Crouhy et al: The Essentials of Risk Management (see References).

[28] For simplicity of numbers, assume the par value of the bond is $100. Bonds are loans that pay the coupon interest each year and pay the par value and last year's interest at the end of the bond's term.

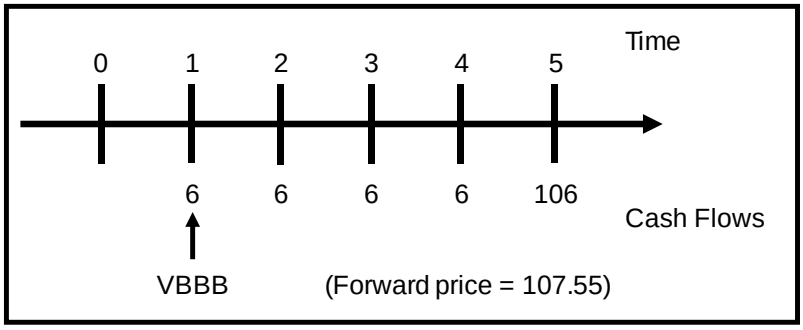


Figure 2: Calculating a Forward Price

The one-year forward price is:

$$V_{BBB} = 6 + \frac{6}{1.0410} + \frac{6}{1.0467^2} + \frac{6}{1.0525^3} + \frac{106}{1.0563^4} = 107.55$$

where the discount rates are taken from the one year forward zero curve in Table 2.

The bond could have its credit rating changed within that year according to the probabilities in the transition matrix shown in Table 1, making the one-year forward value of the bond uncertain. The probability and value of the bond's value one year forward in each of its possible states are shown in Table 3 by replicating the same forward price calculation for each possible bond rating.

For example, calculating the forward price for the bond should it change its BBB credit rating to A would be:

$$V_A = 6 + \frac{6}{1.0372} + \frac{6}{1.0432^2} + \frac{6}{1.0493^3} + \frac{106}{1.0532^4} = 108.66$$

Replicating the same calculations for each rating category gives the values shown in Table 3.

Year-End Rating	Value ($)
AAA	109.37
AA	109.19
A	108.66
BBB	107.55
BB	102.02
B	98.10
CCC	83.64
Default	51.13

Table 3: Example of a One-Year Forward Values for a BBB Bond (Source: CreditMetrics)

The value of a bond that defaults within the next year is measured by its recovery rate. Recovery rates are estimated from a variety of sources such as historical data provided by the rating agencies. Table 4 shows the expected recovery rates for bonds by different seniority classes. In this example, the recovery rate for senior

unsecured debt is estimated to be 51.13%, although the estimation error as measured by the associated standard deviation is quite large, so the actual recovery value lies in a fairly large confidence interval.

Seniority Class	Mean (%)	Standard Deviation (%)
Senior Secured	53.80	26.86
Senior Unsecured	51.13	25.45
Senior Subordinated	38.52	23.81
Subordinated	32.74	20.18
Junior Subordinated	17.09	10.90

Table 4: Example Expected Recovery Rates for Bonds (Source: Moody's)

Step 4: Derive the Forward Distribution of the Changes in Bond/Obligation Value

The distribution of the changes in the bond value, at the one-year horizon, due to an eventual change in credit quality is shown in Table 5. The probability of the state of a year-end rating comes from the transition matrix of Table 1. The forward price comes from Table 3 with the change in value coming from a reference of the bond maintaining its rating throughout the year.

Year-End Rating	Probability of State: p (%)	Forward Price: V ($)	Change in Value: V ($)
AAA	0.02	109.37	1.82
AA	0.33	109.19	1.64
A	5.95	108.66	1.11
BBB	86.93	107.55	0
BB	5.30	102.02	-5.53
B	1.17	98.10	-9.45
CCC	0.12	83.64	-23.91
Default	0.18	51.13	-56.42

Table 5: Example: Distribution of the Bond Values, and Changes in Value of a BBB Bond, in One Year (Source: CreditMetrics)

Credit VaR is based on the same underlying concept as market VaR. The VaR is measured at the 99th percentile loss less the expected loss. Because of the discrete distribution (as opposed to continuous distribution) of bond values shown in Table 5, there is no exact 99th percentile. The 99th percentile loss is conservatively interpreted at a cumulative probability less than or equal to 1%. In this example, that would be at a probability of 0.3%, or at the probability of the bond's year-end rating of CCC or less, for a change in value of -$23.91.

As described earlier for market risk, economic capital is the financial cushion to cover unexpected loss up to a given level of specified confidence (e.g., those related to credit events such as default and/or credit migration). A bank must reserve the right amount of economic capital if it is to remain solvent to any degree of confidence. That capital charge is a function of the portfolio's unexpected losses. As with market risk, the confidence level is set in line with the bank's risk appetite or solvency standard – often its target credit rating. For example, if the confidence level is 1%, then the bank would be able to reassure itself that 99 times out of 100 it would not incur losses above the economic capital level over the period corresponding to the credit-risk horizon (say, one year).

In this example (as is typical for bonds or loan obligations), the distribution in Table 5 exhibits a long "downside tail". The first percentile of the distribution of *V,* which corresponds to credit VaR at the 99% confidence level, is -23.91 (see Table 5). Contrast that to assuming a normal distribution for the bond's value at the end of one year. If we computed the first percentile, assuming a best-fit normal distribution for ***V*****,** it is a much smaller value than -23.91. In this case, the credit VaR at the 99% confidence level would be -7.43.

Summary: Key Credit Risk Points

Credit risk is the distribution of a borrower's probability of defaulting on an obligation combined with the LGD. The expected value (average) of that distribution is reflected in the interest rate of the obligation, given the average or expected loss of zero compared to risk-free obligations. The greater the expected default risk, the higher the interest rate on that bond.

NRSROs have developed standardized methodologies to estimate the PD and LGD of a bond. They define and use qualitative credit rating labels such as AAA, AA, and A to communicate their analysis of the PD of a bond or loan. Other firms research and communicate expected recovery rates should an issuer default. Banks use this information to assess the credit or default risk beyond the simple average.

Credit ratings can change during the life of the bond. As a credit rating changes, the value today of the bond changes as well. All other things equal, the better the credit rating, the more valuable the bond today. The implication is that the value of a bond unexpectedly changes over time. The uncertainty in the bond's price is a risk to an FI holding bonds.

The variation of a bond's price throughout its life is the credit risk a bank takes to originate, purchase, and hold debt instruments. A bond's VaR is the exposure a bank has to the uncertainty of the loss of the bond's value at a given confidence level. A bank must have sufficient reserves to cover the impact of losses in excess of the average loss in order to guarantee its safety, soundness, and stability. In other words, banks must have sufficient resources to withstand losses up to the VaR. A bank reserves capital to provide for the potential defaults so that the banks can remain solvent during those adverse events.

Capital

As discussed earlier, economic capital for an FI is the cushion which provides protection up to a given confidence level against the various risks inherent in its businesses that would affect the security of funds that are deposited with or loaned to the institution. Economic capital provides confidence to institutional claimholders such as depositors, shareholders, and creditors that the institution has sufficient capital reserves to absorb unexpected losses.

Economic capital is required to absorb unexpected losses, up to a certain level of confidence. Reserves are set aside to absorb the expected loss on a transaction that might occur during the life of the transaction. It would be too costly for an FI to operate at a 100% confidence level, for which the FI would never default. Economic capital is set at a confidence level less than 100%. For example, if the confidence interval is set at 99%[29] over a given time interval, then there is a probability of 1% within that interval that actual losses exceed the amount of capital.

Regulatory capital is derived from a set of rules, such as Basel III, in order to ensure that there is sufficient capital in the banking system, especially under stress. Regulatory capital serves as a cushion to protect the safety, integrity, and solvency of the banking system overall. Legislatures and regulators determine regulatory capital requirements.

The determination of economic capital, and its allocation to the various business units, is a strategic decision process that affects the risk/return performance of the business units and the bank as a whole and that influences dramatically how capital is allocated and reallocated among the various activities and projects. Management, business stakeholders, and markets determine economic capital requirements.

[29] In practice, the VaR may be measured at higher percent thresholds such as 99.7% over a one-year basis. The 99% is used here as a rough order of magnitude for explanatory purposes.

Risk of a Portfolio that Includes Cyber Risk

Regulators require a bank to apply regulatory capital requirements against an FI's cyber risk. Cyber risk falls under the same Basel III regulatory requirements as other operational risks.[30] To measure cyber risk economically, analysts[31] need a quantitative risk model and risk analysis method to estimate cyber risk in the same VaR terms as described in Value at Risk (VaR): A Core Concept of Financial Risk Management (on page 8) and Value at Risk (VaR): Credit Risk (on page 13).

The Open Group Open FAIR Body of Knowledge consists of two standards (see References) that provide a foundation for such an analysis:

- The Open Group Standard for Risk Analysis (O-RA)
- The Open Group Standard for Risk Taxonomy (O-RT)

The O-RT Standard is the risk taxonomy standard that defines a precise set of terms, definitions, and their relationships to each other to define a model of cyber risk. This model's primary value is in helping practitioners decompose and critically think through cyber risk scenarios and their associated risk factors. Practitioners frequently report that just thinking through a cyber risk scenario or question through the O-RT Standard gives decision-makers enough information to make informed cyber risk-based decisions. At its core, the O-RT Standard provides the logical foundation for reasoned analysis and clear, precise discussion of cyber risks between management and technical practitioners in managing risk associated with their IT.

The O-RA Standard provides a structured method to provide input to quantify cyber risk. This standard guides analysts on how to estimate the uncertain risk factors (LEF and LM) described by the O-RT Standard.

All estimates of risk factors are estimates of uncertain outcomes whose actual values will be revealed in the future. For example, an analyst may estimate next year's LEF to be between a minimum of once every three years and a maximum of once every year with a most likely value of once every two years. Estimates are updated when the actual value is discovered or revealed in the future (i.e., when the actual LEF becomes known or observed).

The O-RA Standard specifies that risk analysts:

- Ensure that each estimate is accurate; that its range captures the full uncertainty of the estimated risk factor

[30] Regulators define operational risk as "the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events". The Basel III Capital Accords consider seven Level 1 Loss Event types. These Loss Event types are as follows: 1. Internal fraud; 2. External fraud; 3. Employment practices and workplace safety; 4. Clients, products, and business practices; 5. Damage to physical assets; 6. Business disruption and system failures; and 7. Execution, delivery, and process management. Cyber risk is an operational risk under Basel III and can influence several of these Level 1 Loss Event types.

[31] The term "analyst" is used refer to those providing analytical estimates into the cyber risk models used throughout this document. This is synonymous with "risk analyst", "risk management analyst", or "cyber risk analyst".

- Have taken measures to reduce cognitive biases that lead to inaccurate, overly precise estimates that express more knowledge about the estimated risk factor than can be justified
- Characterize estimates as a distribution that best represents what the analyst knows about the risk factor being modeled

Analysts estimate the LEF and LM of cyber Loss Scenarios. The LEF is how many Loss Events occur within a given time period, conventionally one year. The LM is the economic damage measured in units of currency (e.g., dollars[32]) caused by the Loss Event. The rigorous tree-like breakdown of the Open FAIR taxonomy models how a Loss Event occurs and describes six categories of those losses once they do occur. Losses are modeled in two phases: a primary loss that always occurs from the given Loss Scenario, and a secondary loss that may occur, conditioned on the primary loss occurring in the first place.

To accurately estimate cyber risk factors, analysts use all available information about LEF and LM they have to make forward-looking estimates of those risk factors. Information available to the analysts includes their organization's internal history of loss and risk factors, industry-wide data published within their industry segment, Information Sharing and Analysis Centers (ISACs),[33] and subject matter expert opinion. Analysts combine information from these sources to estimate risk factors probabilistically. Risk factors can be modeled with any probability distribution (such as the beta-PERT,[34] uniform, or triangular distribution) that best represents the risk factor being modeled.

Once risk factors have been estimated, they are combined using MCS to generate a distribution of the modeled cyber risk exposure in dollars per year. From this simulation, typical financial risk metrics can be derived, such as VaR and CVaR.

That risk is mitigated through administrative, physical, and technical controls. These controls are implemented and operated by information security organizations consisting of information security specialists versed in a well-developed body of knowledge consisting of security architecture, engineering, and operations. Risk analysts must estimate the economic impact those controls have upon that risk to quantify how a proposed information security program would mitigate cyber risk. For a control to affect risk, it must affect one or more risk factors associated with either the LEF or LM, or both.

Just as there is a generally accepted body of knowledge around risk and risk management, so too there is a body of knowledge that applies to information security. One (of several) is the National Institute of Standards and Technology Cyber Security Framework (NIST CSF)[35]. Commonly used throughout the US Government and private sector critical infrastructure providers, including the financial services sector, the NIST CSF provides a framework for the information security professionals to think about and apply controls to identify, protect, detect, recover, and respond to cybersecurity incidents. The NIST CSF emphasizes that institutions should take a "risk-based approach" to cybersecurity and to perform risk assessments, but it does not prescribe how that assessment should be done or what necessarily a risk-based approach is. The Open FAIR

[32] Dollars will be used throughout the remainder of this document, but any currency may be used.
[33] One example of a financial services ISAC is Sheltered Harbor; refer to: https://www.shelteredharbor.org/about.
[34] PERT stands for Program Evaluation and Review Technique.
[35] The NIST CSF can be found at: https://www.nist.gov/cyberframework.

Body of Knowledge fills the gap in the NIST CSF (and many other cybersecurity frameworks) by providing a framework for defining and analyzing cyber risk. Senior management can see the economic, business value of an information security program when they compare their present state of cyber risk and their estimated mitigated risk after implementation of an information security program.

Quantifying Cyber Risk: An Example

The Open FAIR taxonomy defines risk as the probable frequency and probable magnitude of future loss, presenting a risk as a distribution of possible, albeit uncertain outcomes, with some outcomes having a higher probability of occurring than others. This definition of risk is highly consistent with financial risk measures, such as default risk or portfolio risk, which estimate the likelihood of an adverse financial event occurring within a given time period and the magnitude of that adverse event should it occur. When cyber risk is measured in the same economic terms as market and credit risk, regulators can integrate capital requirements for cyber risk with those other risks. This integration improves management's visibility into the total risk of the FI and the contribution IT makes to that risk. Regulators can see the significance of cyber risk as compared to other risks that the FI faces and adjust regulation and regulatory action accordingly. Through these means, FI management and regulators can more critically think about, discuss, and develop a consensus on the institution's cyber risk and its relative importance compared to other risks. Over time, that consensus should lead to a virtuous cycle of continuously improved risk management and regulation.

The Open FAIR taxonomy defines a set of terms and their relationships to each other that, taken together, define a risk model. The first level of risk is decomposed in Figure 3.[36]

Figure 3: The Open FAIR Taxonomy at its First Level

Suppose in making a new financial deal, financial management needed to assess the VaR associated with a breach of proprietary investor data used for marketing and business development purposes. As mentioned earlier, when applying the Open FAIR standards to estimate the LEF and LM risk factors, the analyst would use all information available. The analyst would generate a distribution of MCS outcomes, which would provide an estimated average and 99% confidence level, from which a VaR could be derived.

[36] The second White Paper of this series – Calculating Reserves for Cyber Risk: Vetting Cyber Risk Models – has a deeper treatment of quantifying risk through additional levels of analysis defined in the Open FAIR taxonomy and risk model. The second White Paper uses the same numbers as this example in this document to show the reader exactly how this section's analysis was derived; it also translates for the reader how the Open FAIR Risk Analysis Tool (see References) processes a subject matter expert's estimates to a distribution, the intermediate calculations made, and the final results.

Calculating Reserves for Cyber Risk: Integrating Cyber Risk with Financial Risk

Choosing an Analytic Perspective

In any analysis, the analyst must first choose the stakeholder whose losses count in the analysis. That stakeholder choice defines a perspective from which to view the analysis. The Open FAIR risk analysis was derived primarily from looking at LEF and LM from the perspective of the firm that stands to lose from the Loss Event. That perspective, however, ignores the costs of a breach or harm to others as a consequence of the breach.

For example, assume a bank suffers a breach of its customers' PII and members of the public are subsequently harmed by consequential identity theft/financial fraud committed against them after a breach of PII. Customer losses are ignored if they cannot (or do not) make a claim against the bank for restitution. In other words, the bank does not internalize non-bank losses when making risk calculations.

However, if the bank or its regulators require some internalization of these impacts, then the Open FAIR analyst must consider them in the valuation of the loss. That means that the analyst must decide how much the external costs are worth to the bank to mitigate. For example, how much is the bank willing to pay to mitigate its customers' consequential identity theft losses as a fraction of those customers' total loss? In other words, how much responsibility does the bank assume for (and how much is it willing to pay to mitigate) those losses?

There is a third, systemic perspective that applies to the stability or security of an entire cyber ecosystem or infrastructure. As previously stated, FIs whose operations have potential financial system stability implications are called Systemically Important Financial Institutions (SIFIs). Similarly, providers of highly ubiquitous information infrastructure – such as cloud service platforms, information security services, Domain Name Services (DNS), Internet Service Providers (ISPs), and highly successful platforms – are foundational to the functioning of the information infrastructure. Breach or failure of these can have wide-ranging effects beyond just the service provider and its customer base. They can affect stability or integrity of the critical infrastructure they support. This foundational set of infrastructural services can be analogized to the SIFIs as Systemically Important Cloud Infrastructure (SICI).

An example of a SICI breach is the SolarWinds® Orion® network monitoring product and service breach, commonly referred to as SolariGate, that was publicized by major news outlets such as the Wall Street Journal, New York Times, Washington Post, and many others in December 2020. At the time of writing, the impact of that breach was only beginning to be apparent, but published reports claim that a state-sponsored attack against SolarWinds affected up to 18,000 SolarWinds customers, including the US Government's Commerce, Treasury, and Homeland Security Departments, the largest high technology providers, and major cloud service providers. What information that nation state captured and what it will do with that information are unknown. The total costs of recovering from the breach have some preliminary estimates. Insurance Business America estimates that the cyber insurance industry may have a $90 million exposure in claims.[37] As reported in Roll Call: "American businesses and government agencies could be spending upward of $100 billion over many months to contain and fix the damage".[38] If this estimate proves to be accurate, it

[37] Refer to Insurance Business America: SolarWinds Trojan Hack Estimated to Cost Cyber Insurers $90 Million (see References).

[38] Refer to Roll Call: Cleaning up SolarWinds Hack May Cost as Much as $100 Billion (see References).

represents losses almost *twenty times as large* as the most extreme breach of the last five years.[39] SICI attacks are possible, with the total social costs of them believed to be potentially catastrophic, just as a SIFI failure is believed to be potentially catastrophic to the stability of the financial system.

The direct costs to SolarWinds, the private firm hacked/breached, pales in comparison to the consequential costs to customers of SolarWinds and the public at large. An analyst looking to estimate these losses and assign a reasonable and appropriate willingness to pay for precautions to SolarWinds against a state-sponsored breach are timely questions, but alas are questions for another day and document.

Economics teaches us that all value is subjective. Analysts must select the perspective, or stakeholder, around which the analysis revolves. That stakeholder subjectively values losses and willingness to pay for their reduction. In the example below, the analyst takes the firm-based perspective that Open FAIR analysts usually take in modeling and estimating cyber risk. Losses modeled in the analysis are those the example bank directly bears as a result of a cyber breach. External losses not borne by the bank – those losses borne by the bank's customers or other stakeholders and the public at large – are outside the scope of the analysis.

Example

In the course of developing a $100 million portfolio of 100 loans, a bank sets up a new legal entity to raise funds from new investors. In doing so, the bank collects, manages, and processes personally identifiable investor data to establish, manage, and maintain the business relationships with them. This data consists of names, addresses, personal financial information, signed agreements, bank account information to direct deposit interest payments, etc. and is an asset to the bank, both operationally and as a trade secret.

The bank incurs additional risk by collecting this information. If financially motivated actors breach this information's confidentiality[40] and use it against the bank and its investors, the bank would have to respond to the Loss Event. It would first have to discover how the Loss Event occurred and what information was compromised. Then, it would need to send breach notification notices to affected bank investors and offer credit monitoring to those affected. These are the primary losses the bank suffers with every breach of this kind.

The Open FAIR method models costs in two categories:

1. Primary losses that occur immediately and always upon detection of a Loss Event
2. Secondary losses that are the conditional fallout costs that others outside of the FI instigate against the institution as a reaction to the initial data loss

The Open FAIR method describes six forms of loss. Productivity and replacement costs are typically primary losses. Reputational, competitive advantage, and fines and judgment costs are typically secondary losses. Response costs are part of every loss, whether primary or secondary.

[39] The Cyentia Institute: IRIS 20/20 XTREME report (see References) analyzed the 100 largest cyber Loss Events from 2015 through the end of 2019. In that report, the maximum was the Facebook® $5.1 billion loss (page 6 of the report).

[40] Per Verizon: Data Breach Investigations Report 2020 (see References), the Financial and Insurance sector suffered 1,509 incidents with 448 confirmed data disclosures in 2019. The primary Threat Agent was the external financially motivated actor who sought easily monetized data.

The bank is exposed to potential secondary losses, such as a financially motivated hacker selling investor data to a bank competitor. The bank treats its list of qualified investors as a trade secret. Competitors would like to obtain that list to sell their services to those investors, probably at the expense of the bank itself. The bank potentially will suffer a competitive advantage loss if it loses control of its investor list to a competitor as a result of the investor data breach.

This incremental operational risk, and its associated capital requirements, must be included in the overall decision bank management makes about whether to approve the $100 million loan portfolio deal.

The bank may also consider adding controls to protect this information to reduce the risk. As the bank considers this action plan, the reduction in risk will reduce capital, but the bank also must include the cost of the controls as incremental operating expenses in calculating the RAROC expected for this deal.

Risk analysts use all the information they have to make informed estimates of going forward risk factors. Information commonly available would include any prior specific history the bank had with this kind of risk, FI sector research as published in data breach reports,[41] internal knowledge of Threat Agents specific to the institution making the deal, and observations of the institution's cybersecurity system that is detecting and responding to potential threats. Using all this information, analysts estimate the frequency of a successful future attack that results in a loss, and the magnitude of that loss when it occurs.

In this example, the analysts' best estimate that captures the full range of the probable frequency of a future successful attack is between a minimum of once every five years and a maximum of once a year, with a most likely frequency of a successful attack of once every two years. Table 6 shows what that estimate looks like in Open FAIR risk factor terms.

	Loss Event Frequency
Min	0.2 (once every five years)
Most Likely	0.5 (once every two years)
Max	1.0 (once a year)

Table 6: Loss Event Frequency (LEF) Parameters

When this loss occurs, the FI suffers direct costs associated with the need to respond to the incident, and sometimes (but not always) it faces competitive advantage and additional response costs associated with managing and mitigating the exploitation of that data by competitors.

In our example, subject matter experts, using all available information, estimate that losses from a breach of PII confidentiality would center on the institution's response costs to that breach. Costs include those associated with detecting the breach, researching security logs of how systems were accessed, forensic analysis of what investor data was breached, and management time to determine what measures the bank

[41] Examples of data breach and impact reports periodically published include Verizon: Data Breach Investigations Report, Demos: The Great Cyber Surrender, and IBM: Cost of a Data Breach Report (see References). Analysts can use these and other research reports to inform estimates of the frequency and magnitude of loss of data breach risk.

should take to protect investors from further harm, such as identity and credit theft protection. Published research shows that the total cost (that includes everything above) to an organization for a PII breach averages $175/record.[42] Assuming the bank has between 200-1,000 investors in this deal and that the actual costs are in a range of $150-$200, the primary loss exposure from responding to this incident is between $30,000 and $200,000, as shown in Table 7.

We assume in our example that the bank would not have a productivity loss, and therefore, business can still be conducted as usual. We also assume that there is no loss of equipment resulting in replacement costs.

Primary Loss	Response ($)
Min	30,000
Most Likely	100,000
Max	200,000

Table 7: Primary Loss Magnitude (LM) Parameters

The primary losses in Table 7 are estimated to occur with each future Loss Event. There are other losses that may, but will not always, occur. In this example, those "sometimes but not always" secondary losses[43] center around potential legal exposure the bank faces from regulators and the affected investors as a result of the loss of confidentiality of its investor information. If legal action is taken, the bank must respond to and recover from it. These secondary losses are represented by the probability that one occurs as a consequence of the primary Loss Event, and by the magnitude of that secondary loss once it occurs.

The probability of this secondary loss (conditioned upon the customer data breach in the first place) is called the Secondary Loss Event Frequency (SLEF)[44] and is measured as the conditional probability that given (in this example) the primary investor data breach loss, a secondary competitive advantage loss with its associated response costs is incurred.

The analysts in this example use expert opinion that is informed by quality risk information and subject matter expert opinion to arrive at a going forward estimate[45] that there is a minimum 20% chance that a malicious, financially motivated hacker would use the breached PII data in a way that would cause harm to the bank's investors or result in legal action. The analysts further estimate, again using the best information available to inform that estimate, that not more than half of maliciously hacked data sets would result in legal or regulatory action against the bank. The analysts estimate that the most likely probability that a compromised PII data set would result in legal or regulatory action is 30% (see Table 8).

[42] For example, see IBM: Cost of a Data Breach Report 2020 (see References).

[43] The Open FAIR Body of Knowledge models primary and secondary losses as having up to six forms of loss that each have a distribution. Each form of loss is statistically independent of the other.

[44] SLEF can be better described as the probability that a secondary loss occurs given a primary loss has occurred. The Open FAIR Body of Knowledge uses the term Secondary Loss Event Frequency.

[45] Refer to Mark & Krishna: How Risky is your Risk Information (see References).

	Secondary Loss Event Frequency (Probability)
Min	0.2
Most Likely	0.3
Max	0.5

Table 8: Secondary Loss Event Frequency (SLEF)

If these losses were to occur, they could be significant. The bank would mobilize additional response efforts to respond to legal and regulatory inquiries. In this example, the analysts estimate that between 100 and 400 hours (170 hours most likely) of response time would be devoted to preparing any defense for legal action and working with regulators at a fully loaded cost[46] rate of $150/hour.[47]

The analysts also estimate that fines and judgments imposed by regulators and the courts would cost between $1,000,000 and $1,500,000 ($1,200,000 most likely) to close the case. The complete estimates are shown in Table 9.

Secondary Loss Magnitude	Response ($)	Fines and Judgments ($)
Min	15,000	1,000,000
Most Likely	25,500	1,200,000
Max	60,000	1,500,000

Table 9: Secondary Loss Magnitude (LM) for Losses that Can but Do Not Always Occur

The MCS generates a desired number of trials to arrive at a distribution of simulated outcomes. Statistics including the average and a 99% loss are calculated. The simulation run in this example is based on 5,000 trials[48] which generates the distribution shown in Figure 4.

[46] Staff hours can be valued by their "fully loaded hourly cost" that includes wages, benefits, and overhead costs of employing a person for one hour.

[47] Observe that the minimum of $15,000 = 100 hours x $150/hour and that the maximum = 4 x minimum.

[48] A Monte Carlo Simulation for an FI would likely use far more than 5,000 trials to better capture low probability, high impact tail events. The 5,000 trials used here is convenient for demonstration purposes and when using a spreadsheet tool to do the simulation.

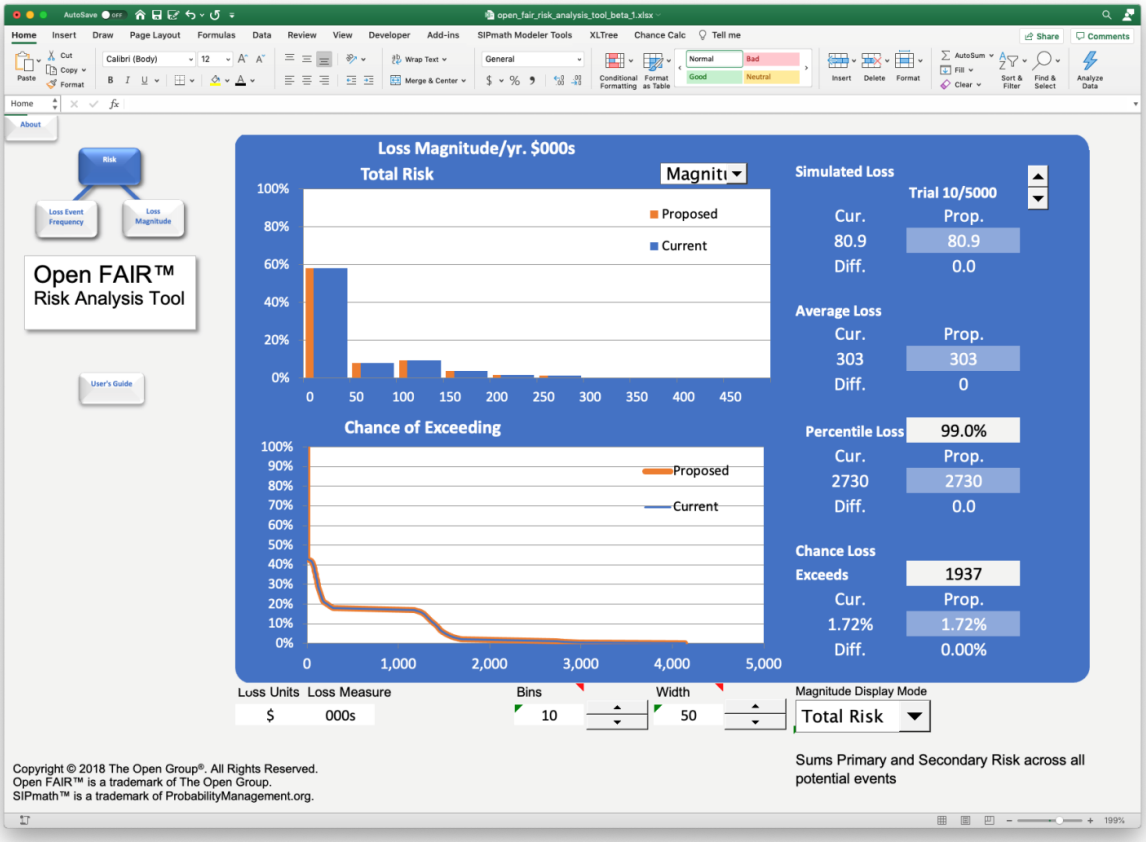


Figure 4: Monte Carlo Simulation Results

Table 10 shows the Current state of this example's risk metrics.

Risk Metric	**Current[49] ($)**
Average Loss per Year	303,000
99th Percentile Loss	2,730,000
Annual Value at Risk[50]	2,427,000

[49] The Open FAIR Risk Analysis Tool is a Microsoft® Excel spreadsheet that The Open Group developed as an illustrative example to demonstrate the Open FAIR method and how it could contribute to calculating cyber risk. The Tool develops a "Current" state and a "Proposed" state to analyze the present state of an information system's risk and what it would be should a proposed set of additional controls be added. "Current" refers to that current, initial state being analyzed, while the "Proposed" state is that Current state as changed by the set of additional controls. Here, "Current" and "Proposed" are the same because there is no set of additional controls yet proposed. Figures are rounded to the nearest thousand.

[50] The Annual VaR is the 99th Percentile Loss minus the Average Loss per year.

Risk Metric	Current[49] ($)
Economic Capital based on 1x VaR[51]	2,427,000
99th Percentile Tail Expected Value[52] (=CVaR)[53]	3,130,000
Economic Capital Based on 1x CVaR[54]	2,827,000

Table 10: Summary Cyber Risk Statistics

Similar to market and credit VaR, the difference between the 99th percentile and average loss represents an annual VaR associated with cyber losses from this loss scenario. The analysis also provides CVaR, an emerging VaR measurement that regulators are beginning to use, as an additional measure of required capital.

In summary, the CISO and risk analysts can quantify cyber risk in the same manner as other enterprise-wide risks. Financial firms can use the MCS results to allocate economic capital against those risks to comply with emerging cyber risk management regulation in the financial services sector.

Quantifying How Controls Mitigate Risk

The business value of the controls used to mitigate risk can be measured by the value of the risk they reduce. If risk is measured in economic terms, its reduction has tangible, economic value. This subsection outlines how the risk associated with the scenario in the previous section can be reduced by a combination of administrative and technical controls, leading to a change in the VaR that affects economic capital requirements.

In the previous subsection's example, the bank is exposed to legal liability that has a conditional probability of occurring between 20% and 50% of the time after a data breach. That loss is estimated to be between about $1,000,000 and $1,500,000 when it occurs. Suppose the bank adds Security Information and Event Management (SIEM)[55] tools to improve identification of cyber hackers and adds investigators to (more) aggressively identify, pursue, and prosecute those who try to use the bank's customer data as a weapon against the bank, and suppose further that the bank publicly commits to prosecuting those who exploit illegally gained trade secret PII so that they "know" that the bank will credibly execute this new policy. Such a policy serves to deter those actors who would try to use illegally obtained PII that results in legal exposure to the bank. Subject matter experts estimate the risk factor of SLEF will fall to an estimated range of 5% to 20%.

[51] Economic capital is a complex calculation. For simplicity we assume that the economic capital is 1xVaR.

[52] The Open FAIR Risk Analysis Tool does not calculate the expected value of a tail as part of its standard output. The authors accessed the internal MCS data within the Tool and manually calculated the expected value of the tail in this analysis.

[53] Regulators and FIs are beginning to use the CVaR as the primary risk measure for capital requirements.

[54] CVaR-based economic capital in our example equals the expected value in the tail from the 99th percentile to 100th percentile minus the average loss per year.

[55] SIEM tools are Security Information and Event Management tools that log and analyze information collected in a Security Operations Center. This information can assist in identifying where the hacking originated and what information was exfiltrated.

Table 11 shows the revised cyber risk factor SLEF if the proposed risk mitigation plan goes into effect.

Secondary Loss Event Frequency	Probability
Min	0.05
Most Likely	0.1
Max	0.2

Table 11: New Secondary Loss Event Frequency (SLEF) as a Result of Proposed Controls

Because this mitigation plan focuses on secondary loss prevention, it does not affect anything else in the risk scenario; everything else remains the same (LEF, Primary LM, and Secondary LM). Only the SLEF changes as a result of the new controls.

Under these assumptions and estimates, the risk model in Figure 5 shows how the proposed controls change risk compared to the Current state described in the previous section.

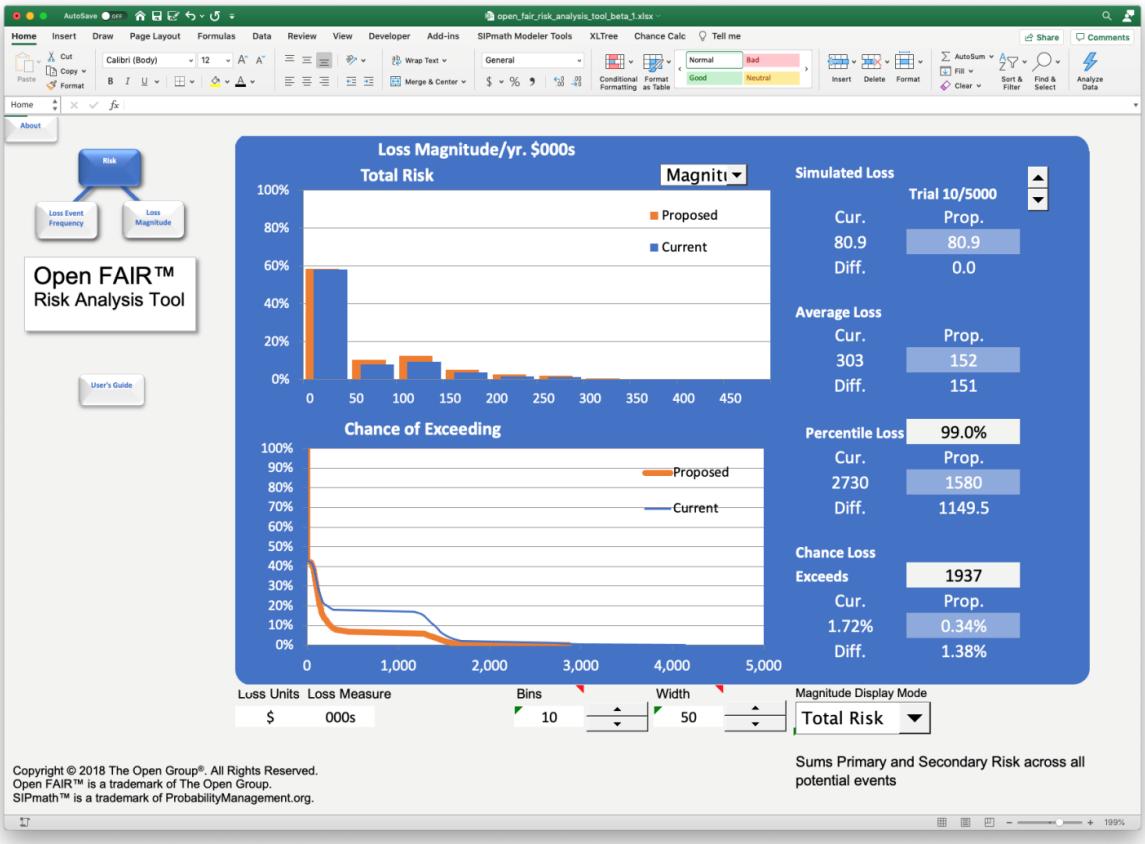


Figure 5: Results of the Proposed Control Mitigation

The MCS shows that the average loss deceases by $151,000 and the 99th percentile loss decreases by $1,150,000. The VaR decreases by $1,084,000 with a corresponding drop in economic capital requirements, as shown in Table 12.

	Current[56]	Proposed[57]	Difference[58]
Average Loss per year[59]	303,000	152,000	151,000
99th Percentile Loss	2,730,000	1,580,000	1,150,000
Annual Value at Risk	2,427,000	1,428,000	999,000
Economic Capital Based on 1x VaR	2,427,000	1,428,000	999,000
99th Percentile Tail Expected Value (=CVaR)	3,130,000	2,015,000	1,115,000
Economic Capital Based on 1x CVaR	2,827,000	1,863,000	964,000

Table 12: Summary Effect Upon Risk from New Controls

Note that economic capital can be derived from the conventional VaR or the emerging CVaR capital requirement analyses.

Factoring in the Cost of Mitigation

Administrative, physical, and technical risk reduction controls have a cost. In this example, to more aggressively deter attempts to cause these losses, the bank commits an additional $100,000 per year in the SIEM tool and investigation to support law enforcement's ability to investigate and prosecute those who would use breached information to try and cause a loss to the bank. This $100,000 per year is reflected as incremental annual operating costs associated with this particular deal.

Final Thoughts

This section gives the reader a stylized example of how a cyber risk scenario would be analyzed in the financial sector. The scenario was analyzed from the strict perspective of the FI, ignoring social costs for which the institution is not directly responsible. The analysis used The Open Group O-RT Standard to describe risk factors and The Open Group O-RA Standard as an input for analyzing and quantifying that risk. The analysts used all available information to accurately estimate and model risk factors using a distribution to characterize them. MCS was used to model the distribution of the risk associated with this scenario.

[56] The "Current" state reflects the risk as summarized and concluded by Figure 3 and Table 10.

[57] Here the "Proposed" state models the risk associated with the loss scenario after the administrative and technical controls described that reduce SLEF have been implemented.

[58] The value of the "Proposed" state over the "Current" state – that is, the value of additional controls – is the reduction in risk as measured by various metrics.

[59] Average loss per year is equivalent to annualized loss expectancy, which is a commonly used term in the information security profession.

Calculating Reserves for Cyber Risk: Integrating Cyber Risk with Financial Risk

There is no perfect method to conduct a cyber risk analysis due to the dynamic and volatile uncertainty of future cyber events. Nevertheless, an MCS approach using well-defined risk factors as inputs and VaR-based results as outputs can be used.

Risk-Adjusted Return on Capital (RAROC)

The Risk-Adjusted Return on Capital (RAROC) approach relates the return on capital provided by a transaction, or business, to the riskiness of the investment. For the business to prosper, as the risk of the investment (and its capital requirement) rises, so must expected returns. To win management approval, an investment must achieve a minimum expected return – the hurdle rate – on the capital required to support the investment.

RAROC analysis reveals how much capital is required by each business line, product, or customer and how these requirements create the total return on capital produced by the firm. Further, RAROC provides an economic basis from which to measure all the relevant risk types and risk positions consistently. Finally, because RAROC promotes consistent and reasonable risk-adjusted performance measures, it provides managers with the information that they need to make the trade-off between risk and reward more efficiently.[60]

RAROC was made possible by the development of sophisticated risk measurement tools. These tools offered banks the practical capability to assign economic capital and measure performance on a risk-adjusted basis.

The numerator of the RAROC calculation for a portfolio of loans is the expected net return of that portfolio; that is, total revenue from the portfolio less its total costs. Revenue includes interest received from the borrowers. Costs include expected credit losses from defaults on borrower payment obligations, interest paid to investors, and relevant operating expenses to manage the portfolio over its life.

The denominator of the RAROC equation is the economic capital required to support the portfolio.[61]

$$RAROC = \frac{Expected\ Risk\ Adjusted\ Return}{Capital}$$

RAROC was first suggested as a tool for capital allocation, on an *ex-ante* basis. When used this way, management requires RAROC to exceed a hurdle rate (in this example 13%) to approve the portfolio. Hence, expected losses should be determined in the numerator of the RAROC equation.

After the portfolio has been closed, RAROC is sometimes used for performance evaluation, and in such a case, it is calculated on an *ex-post* basis, with realized losses used in the numerator rather than expected losses.

RAROC can be interpreted as the annual expected rate on equity capital needed to support the loan portfolio. The hurdle rate is the minimum RAROC management requires to approve a proposed loan portfolio.

[60] Refer to Durante et al: Designing and Validating your RAROC Framework (see References).

[61] This example is based upon a stand-alone calculation for a portfolio of loans. We can also look at this on an incremental basis for any loan we add to the portfolio.

RAROC Example: A Loan Portfolio Deal Analyzed in Three Scenarios

The example that follows analyzes the RAROC of a long-term $100 million loan portfolio consisting of 100 loans, each of $1,000,000. The bank has raised $92.5 million from new investors and has used $7.5 million of its own assets to fund this portfolio.

Each of these loans has an annual coupon of 9%.[62] Borrowers repay the principal at the end of the term of the loan.

In this example, the hurdle rate is 13%.

Scenarios Evaluated

To determine whether or how to do this deal, the bank's risk management team assesses the RAROC of three scenarios:

1. The loan portfolio by itself, ignoring the capital required to cover cyber risk.
2. The loan portfolio plus the capital required to cover the current state of cyber risk developed in the previous section.
3. The loan portfolio plus the capital required to cover the proposed state of cyber risk developed in the previous section.

The total expected risk-adjusted returns under each of the three analyzed scenarios are as shown in Table 13 through Table 16, using the following formula:[63]

$$Expected\ Risk\ Adjusted\ Return = Coupon\ Revenue - Investor\ Interest\ Expense - Operating\ Cost - Expected\ Credit\ Loss - Expected\ Cyber\ Loss$$

Portfolio Revenue

Revenue comes from one source: the 9% coupon on the $100 million portfolio: $9 million.

Portfolio Expenses

Annual expenses to operate the portfolio after it has been built are summarized below:

- Interest expense of 6% on the $92.5 million raised from investors: $5.55 million
- Operating expenses of $1.2 million per year in Scenario 1 and 2 that increase in Scenario 3 to $1.3 million to cover the additional cybersecurity controls
- Expected credit losses of 1% of the portfolio principal: $1 million

Expected losses due to cyber risk as shown in Table 12: $0.303 million in Scenario 2, and $0.152 million in Scenario 3.

[62] For ease of discussion, we will ignore considerations of the revenue on which the bank receives gains by investing their capital at the risk-free rate.
[63] The formula is a useful illustrative proxy to the actual variety of RAROC formula banks use to make risk-adjusted return calculations.

Calculating Reserves for Cyber Risk: Integrating Cyber Risk with Financial Risk

Capital Requirements

The capital required to cover the risk associated with this proposed loan portfolio deal has two components:

- The economic capital against the portfolio is estimated to be $7.2 million[64] (i.e., 7.2 % of the loan)
- The cyber risk capital requirement as presented in Table 12: $2.43 million in Scenario 2, and $1.43 million in Scenario 3

Analysis

Table 13 summarizes how cyber risk considerations affect expected cyber losses and economic capital requirements for three scenarios with the economic capital either being equal to the VaR or CVaR.

	Expected Cyber Loss ($)	**Economic Capital at a 99th Percentile VaR ($)**	**Economic Capital at a 99th Percentile CVaR ($)**
Ignoring Cyber Risk	N/A	N/A	N/A
Incorporating Current Cyber Risk	303,000	2,427,000	2,827,000
Incorporating Proposed Cyber Risk	152,000	1,428,000	1,863,000

Table 13: Summary of Cyber Risk Considerations

Table 14 provides the total expected return for each of the three scenarios.

Evaluation	**Expected Coupon Revenue ($)**	**Investor Interest Expense ($)**	**Operating Cost ($)**	**Expected Credit Loss ($)**	**Expected Cyber Loss ($)**	**Total Expected Return[65] ($)**
Portfolio Only	9 million	5.55 million	1.2 million	1 million	N/A	1.25 million
Portfolio with Cyber Risk	9 million	5.55 million	1.2 million	1 million	0.30 million	0.95 million
Portfolio with Mitigated Cyber Risk	9 million	5.55 million	1.3 million	1 million	0.15 million	1.0 million

Table 14: Total Expected Return of $100 Million Loan Portfolio With and Without Considering Cyber Risk

[64] Assume a 15% correlation between the 100 loans for purposes of calculating the risk.

[65] Assume the risk-free rate is zero.

Calculating Reserves for Cyber Risk: Integrating Cyber Risk with Financial Risk

The Go (do the deal), No-Go (don't do the deal) decision is based upon the example bank's minimum acceptable RAROC, economic capital measured as the VaR, and the hurdle rate of 13%, as shown in Table 15.

Evaluation	Total Expected Return ($)	Financial Risk Economic Capital ($)	Cyber Risk Economic Capital ($)	Total Economic Capital[66] ($)	RAROC (%)	Go, No-Go (>= 13%?)
Portfolio Only	1.25 million	7.2 million	N/A	7.2 million	17.4	Go
Portfolio with Cyber Risk	0.95 million	7.2 million	2.43 million	7.60 million[67]	12.5	No-Go
Portfolio with Mitigated Cyber Risk	1.0 million	7.2 million	1.43 million	7.34 million[68]	13.6	Go

Table 15: Go, No-Go RAROC Investment Decision Based on VaR

That same analysis and decision, but based upon an economic capital requirement based on CVaR, is shown in Table 16.

Evaluation	Total Expected Return ($)	Financial Risk Economic Capital ($)	Cyber Risk Economic Capital ($)	Total Economic Capital[69] ($)	RAROC (%)	Go, No-Go (>= 13%?)
Portfolio Only	1.25 million	7.2 million	N/A	7.2 million	17.4	Go
Portfolio with Cyber Risk	0.95 million	7.2 million	2.83 million	7.74 million[70]	12.3[71]	No-Go

[66] If financial risk (loss) is assumed to be statistically independent of cyber risk (loss), then the total capital requirements based upon the respective VaRs are approximately the square root of the sum of the squares of the respective capital requirements. However, that assumption of independence may not be strictly true and, if not, there is a correlation between zero and one between financial risk and cyber risk. In the extreme where financial risk and cyber risk are perfectly correlated, the Total Economic Capital would be the simple sum of Cyber Risk Economic Capital and Financial Risk Economic Capital.

[67] The range of Total Economic Capital is from $7.60 million to $9.71 million, depending upon the correlation between financial risk and cyber risk.

[68] The range of Total Economic Capital is from $7.34 million to $8.64 million depending upon the correlation between financial risk and cyber risk. With a sufficiently high correlation, the Portfolio with Mitigated Cyber Risk still would fail the Go, No-Go hurdle rate.

[69] If financial risk (loss) is assumed to be statistically independent of cyber risk (loss), then the total capital requirements based upon the respective VaRs are approximately the square root of the sum of the squares of the respective capital requirements. However, that assumption of independence may not be strictly true and, if not, there is a correlation between zero and one between financial risk and cyber risk. In the extreme where financial risk and cyber risk are perfectly correlated, the Total Economic Capital would be the simple sum of Cyber Risk Economic Capital and Financial Risk Economic Capital.

[70] The range of Total Economic Capital is from $7.74 million to $9.95 million depending upon the correlation between financial risk and cyber risk.

[71] Observe that even though the RAROC based upon CVaR-based economic capital is higher than the RAROC based upon VaR, it does not change the Go, No-Go decision.

Calculating Reserves for Cyber Risk: Integrating Cyber Risk with Financial Risk

Evaluation	Total Expected Return ($)	Financial Risk Economic Capital ($)	Cyber Risk Economic Capital ($)	Total Economic Capital[69] ($)	RAROC (%)	Go, No-Go (>= 13%?)
Portfolio with Mitigated Cyber Risk	1.0 million	7.2 million	1.86 million	7.44 million[72]	13.4	Go

Table 16: Go, No-Go RAROC Investment Decision Based cn CVaR

RAROC is a key metric used to inform financial decision-making. Reducing cyber risk and its associated economic and regulatory capital burden opens up additional transparent business opportunities for the bank because cyber risks and their associated capital requirements are included in that calculus. Evaluating the effects upon regulatory and economic capital from cyber risk management and cybersecurity programs provides a direct business value metric of cybersecurity programs.

As FIs have to incorporate cyber risk into their business risk and capital calculations, some business opportunities will not pass management's RAROC hurdle rate. The difference between including cyber risk and ignoring it can be dramatic, such as the RAROC of the portfolio only compared to the RAROC of the portfolio with cyber risk. As FIs measure and apply capital against this operational risk, they may be surprised by the effect cyber risk has on the business. These effects may be further amplified by financial technology and outsourcing.

[72] The range of Total Economic Capital is from $7.44 million to $8.95 million, depending upon the correlation between financial risk and cyber risk. With sufficient correlation between financial risk and cyber risk, the Portfolio with Mitigated Cyber Risk still would fail the Go, No-Go hurdle rate.

Measuring Return on Security Investment (ROSI)

The reduction of cyber risk as measured in economic terms is the true measure of a cybersecurity program's value. The greater the risk reduction, the greater the value of the program. This represents a sea change in cybersecurity management. Cybersecurity controls by themselves are no longer the goal: effective cyber risk management is. CISOs and other senior managers see cybersecurity controls as being the means to the end of effective cyber risk management, with the value of those controls measured by the remaining cyber risk. The less risk, the more valuable the controls.

Within the broad IT community, Return on Security Investment (ROSI)[73] is measured by estimating the amount of average Annual Loss Exposure (ALE) that security investment reduces. Measured over many security mitigation alternatives, the average annual losses avoided[74] or reduced are the benefits of those alternatives that can be evaluated against their useful lifetime capital and operational costs.

For example, an alternative that plausibly reduces (avoids) average annual losses of $151,000 (= 303,000 – 152,000; see Table 13) per year for each of three years accrues total net benefits to the organization of just over $450,000. To develop a cost-benefit analysis, that saving can be compared against the alternative's annualized cost of $100,000 for acquisition, deployment, maintenance, and retirement costs over the three-year life of the program.

Typically, ROSI, measured in percent per year, can be expressed by this formula:

$$ROSI = \frac{(ALE_{Current\,State} - ALE_{Proposed}) - (Annualized\,Cost\,of\,Control)}{Annualized\,Cost\,of\,Control}$$

in this example:

$$ROSI = \frac{(\$151{,}000) - (100{,}000)}{100000} = 51\%$$

As explored in the previous section, however, the benefits of additional security control alternatives can be evaluated beyond loss reduction. With scarce regulatory and economic capital, FIs can value the opportunity cost of allocating capital to cyber risk as opposed to allocating capital in the pursuit of financial business (investment) opportunity. Capturing cyber risk based on VaR and CVaR opens up new ways of quantifying the value of cyber security. ROSI shows the average costs and benefits of cybersecurity but not the effect of security controls on VaR and CVaR.

[73] Refer to the European Network and Information Security Agency: Introduction to Return on Security Investment (see References) for an introduction to ROSI.

[74] Average annual losses avoided are the difference between the ALE of the Current state before new controls are added and the ALE of that proposed future state.

Comparing RAROC and ROSI – An Example

The previous sections quantified a cyber risk, analyzed a proposed mitigation, and analyzed through RAROC analysis how new cyber risk controls can affect the viability of a financial transaction. Suppose, however, that management has several alternatives to consider in mitigating cyber risk to make that transaction viable through RAROC, each with its own ROSI and RAROC. Table 17 presents five scenarios:

- Scenario 1: The Current state as the unmitigated state in Risk-Adjusted Return on Capital (RAROC) (on page 33)
- Scenario 2: The Mitigation 1 alternative as developed in Risk-Adjusted Return on Capital (RAROC) (on page 33)
- Scenarios 3, 4, and 5: Mitigations 2, 3, and 4, which are not detailed here,[75] but are presented as alternatives to Mitigation 1 with their summary effects, as documented in Table 17

Each of these alternatives has a risk reduction benefit as measured by average loss, 99th percentile tail loss, VaR, and economic capital. Through those measures, each mitigation alternative has a ROSI and RAROC that depend upon the alternative's annualized cost.

Cyber Risk Measures ($)					
	Current	**Mitigation 1**	**Mitigation 2**	**Mitigation 3**	**Mitigation 4**
Average Loss/Year ($)	303,000	152,000	243,000	106,000	125,000
99th Percentile Loss ($)	2,730,000	1,580,000	1,812,000	1,505,000	1,539,000
VaR, Economic Capital ($)	2,427,000	1,428,000	1,569,000	1,394,000	1,414,000
RAROC (%)	12.5	13.4	13.0	12.9	13.6
ROSI (%)	N/A	51	20	-1.5	42
Annualized Cost of New Controls	0	+100,000	+50,000	+200,000	+125,000

Table 17: Example Cyber Risk Mitigations and their RAROC and ROSI

[75] In the following table, the risk reduction effects of Mitigations 2, 3, and 4 were modeled as changes to the SLEF in the Current state.

	Mitigation		
SLEF Parameter	**2**	**3**	**4**
Min	15%	2%	3%
Most Likely	20%	5%	7%
Max	40%	10%	15%

Mitigation 1 – the example in Risk-Adjusted Return on Capital (RAROC) (on page 33) – has the highest ROSI and also has sufficient RAROC to approve the transaction. Mitigation 3 has sufficient RAROC but a much lower ROSI, while Mitigation 4 has the highest RAROC but a lower ROSI. The risk reduction benefits of Mitigation 3 on average are below the annualized cost, and as that annualized cost is an expense to be captured in RAROC, the RAROC also falls.

This example is an introduction to the valuation of cybersecurity controls through their effect upon risk reduction. There is much more that could be written on the relationship between ROSI metrics and RAROC approaches, but that is beyond the scope of this document.

Conclusion

Similarities Between Cyber Risk and Financial Risks

As presented in this document, cyber risk can be expressed in the same economic terms as other risks, allowing a bank's risk management team to look at total risk holistically. Although the risk models and assumptions used in modeling market risk, credit risk, and cyber risk differ, the nexus of commonality is that they all express risk as a probable frequency of loss and a probable magnitude of loss. Losses are expressed in economic terms and as a distribution, from which a VaR can be calculated. Figure 5 below highlights this key conclusion.

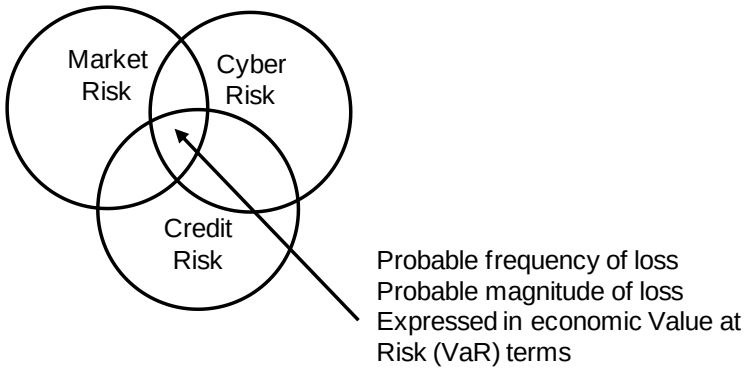


Figure 6: Similarities Between Market, Credit, and Cyber Risk Metrics

Focusing on similarities across these risks allows all stakeholders within an FI to govern and manage cyber risk as an enterprise risk:

- The board and senior management can meet their regulatory and fiduciary duties of treating cyber risk as an enterprise risk
- Reserves can be calculated for operational cyber risk, so the institution can comply with international banking regulation
- CROs and cyber risk managers can communicate and help each other understand how cyber risk affects the risk posture of an FI, bridging the knowledge, communication, and disciplinary gaps between general management, risk management, and cyber risk management
- Cybersecurity professionals can value their security programs in common risk reduction terms that show how cybersecurity and risk professionals understand the business of the institution and their contribution to it

Implications to Financial Risk Management

Most FIs have one set of rules to measure market risk, a second set of rules to measure credit risk, and a third set of rules to measure operational risk. Leading banks integrate these methodologies. Our goal in this

document is to integrate cyber risk with financial risk to obtain a more complete measure of an institution's risk and required regulatory and economic capital to cover unexpected losses. An integrated goal-congruent risk management process that puts all the elements together opens the door to optimal firm-wide management of risk. "Integrated" refers to the need to include cyber risk measures to avoid a fragmented approach to risk management – risk management is only as strong as the weakest link.

Developing an integrated risk measurement model that includes cyber risk will have important implications from both a risk transparency and a regulatory capital perspective. For example, if simply adding a market risk VaR plus a cyber risk VaR plus a credit risk VaR results in a total VaR (rather than developing an integrated model), then the amount of risk and associated required capital would be overstated. Summing these VaRs essentially requires the assumption that all these risks are perfectly correlated. In the example presented in this document, we assumed that cyber risk VaR was independent of credit risk VaR. However, there may be some interactions and correlations that are worth capturing between financial risk and cyber risk, which would lead to a more integrated and comprehensive FI risk model.

The banking industry, rather than the regulators, sponsored the original market VaR methodology. In particular, The JPMorgan™ RiskMetrics product release[76] pushed the industry forward. Industry has also sponsored the new wave of credit VaR methodologies, such as CreditMetrics. All this suggests that, in time, the banking industry will sponsor some form of generally accepted cyber risk VaR methodology. The methodologies described in this document provide a good start.

We will see increased price discovery for cyber risk, which will facilitate what individuals, businesses, and the public sector are willing to pay to avoid and mitigate cyber Loss Events. How cyber losses should be valued is an open and rapidly changing question. The shock of SolariGate exemplifies how the cyber risk valuation can change without notice.

Moreover, a major challenge for banks is to produce comprehensible and practical approaches to cyber risk that will prove acceptable to the regulatory community. Ideally, the integrated risk model of the future will encompass market risk VaR, credit risk VaR, and cyber risk VaR and will be used to calculate both regulatory capital and economic capital.

Implications for Cybersecurity/Cyber Risk Management

Many cybersecurity professionals, bank executives, and bank risk officers believe that cyber risk is too intangible to be measured and integrated with the bank's other risks, but analysts using MCS can quantify cyber risk and integrate that risk with the bank's other risks. Regulators and bank management can calculate reserves for cyber risk just as any other credit, market, or operational risk.

By calculating cyber risk through a VaR-based approach, management can value information security programs by the cyber risk they reduce and the business implications of that reduction. The reserves needed for cyber risk have a business opportunity cost. When a cybersecurity control program reduces cyber VaR, regulatory and economic capital can be put to other business purposes. CISOs and CROs can clearly demonstrate to management and their board of directors the business value of that program.

[76] Refer to: https://en.wikipedia.org/wiki/RiskMetrics.

In 2014, the National Association of Corporate Directors (NACD) published Cyber-Risk Oversight, Director's Handbook Series 2014 (see References) that guided board directors: *"… to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue*". In subsequent years, other governance advisory bodies have amplified that concept, with the Organization of American States (OSA) and the Internet Security Alliance (ISA) collaborating in their Cyber-Risk Oversight Handbook for Corporate Board (see References), saying: "*Guidelines from the National Association for Corporate Directors (NACD) advise that boards should view cyber-risks from an enterprise-wide standpoint and understand the potential legal impacts. They should discuss cyber risk and preparedness with management and consider cyber threats in the context of the organization's overall tolerance for risk.*"

For an FI's board to understand cyber risk as an enterprise-wide risk and perform its risk management oversight responsibility, cyber risk must be measured in the same terms as other enterprise risks such as market risk and credit; that is, in economic terms. Only then can directors and management make informed decisions on how to manage that risk in the context of the institution.

Quantifying cyber risk gives management and boards the information they need to make an informed decision whether to accept, transfer, or further mitigate the risk remaining after applying approved controls. By integrating cyber risk with financial and other operational risk, decision-makers have the information needed to make effective Go, No-Go business decisions.

Coming Up in the Second White Paper

This first White Paper focuses on quantifying cyber risk in financial terms so that risk managers within an FI can aggregate cyber risk with market risk, credit risk, and other operational risks to obtain a complete risk picture for prudential risk management and compliance.

The purpose of the second White Paper is to give an overview of the risk associated with modeling cyber risk – in other words, the risk associated with the model and analysis process. Regulators and FI management need to be confident that the risk models they use are relevant and correct. That confidence is built through the process of model vetting.

A cyber risk model must be vetted before it can be used to inform economic and regulatory capital requirements. The second White Paper presents an overview of how a quantitative cyber risk model could be analyzed as fit-for-purpose in an FI. We develop:

- How financial risk managers accept and vet models through the concept of parsimony
- Essential financial industry requirements on cyber risk analysis such as stress testing that are not as prevalent in other industries
- The organization of the cyber risk supply chain, the division of labor, and specialization in cyber risk analysis
- How the Open FAIR model is relevant and correct, as seen outside the financial industry
- How cyber risk practitioners view and argue the correctness of the Open FAIR model and analysis process
- How calculations are made in an Open FAIR MCS tool to give an example of how the Open FAIR risk factors can be combined to give accurate results consistent with the definitions of those factors

Calculating Reserves for Cyber Risk: Integrating Cyber Risk with Financial Risk

Throughout the second White Paper, we show the rigor of cyber risk analysis and compare that to the rigor and complexity of financial risk analysis. That comparison introduces financial risk managers to the Open FAIR theory and practice as input to assessing quantitative cyber risk analysis, as well as to comply with an FI's internal risk management policy and procedure and external regulatory requirements.

Glossary

Action

An act taken against an Asset by a Threat Agent. Requires first that contact occurs between the Asset and Threat Agent.

Asset

The information, information system, or information system component that is breached or impaired by the Threat Agent in a manner whereby its value is diminished or the act introduces liability to the Primary Stakeholder.

Banking Book

Refers to the activities in a bank, excluding the trading floor activities in a bank.

Competitive Advantage Loss or Cost

One of the six forms of loss, Competitive Advantage Losses are losses associated with diminished competitive advantage. Competitive Advantage Loss is specifically associated with assets that provide competitive differentiation between the organization and its competition. Examples include trade secrets, merger and acquisition plans, etc.

Conditional Value at Risk (CVaR)

Conditional VaR is an alternate risk measure that gives an indication of the magnitude of the potential losses in the tail. In particular, CVaR is the expected loss beyond VaR (i.e., the expected loss given that the loss exceeds the VaR).

Contact Event

Occurs when a Threat Agent establishes a physical or virtual (e.g., network) connection to an Asset.

Contact Frequency (CF)

The probable frequency, within a given timeframe, that a Threat Agent will come into contact with an Asset.

Control

Any person, policy, process, or technology that has the potential to reduce the Loss Event Frequency – Loss Prevention Controls – and/or Loss Magnitude – Loss Mitigation Controls.

Control Strength (CS)

The strength of a control as compared to a standard measure of force.

FAIR

Factor Analysis of Information Risk.

Fines and Judgments Losses or Costs

One of the six forms of loss, Fines and Judgments Losses or costs are those associated with legal or regulatory actions levied against an organization. Note that this includes bail for any organization members who are arrested.

Loss Event

Occurs when a Threat Agent's action (Threat Event) is successful in breaching or impairing an Asset.

Loss Event Frequency (LEF)

The probable frequency, within a given timeframe, that a Threat Agent will inflict harm upon an Asset.

Loss Flow

The structured decomposition of how losses materialize when a Loss Event occurs.

Loss Magnitude (LM)

The probable magnitude of loss resulting from a Loss Event. Losses are categorized into six forms of loss: Productivity, Replacement, Response, Competitive Advantage, Reputation, and Fines and Judgments.

Loss Scenario

The story of loss that forms a sentence from the perspective of the Primary Stakeholder.

Operational Risk

Regulators define Operational Risk as "the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events". The Basel III Capital Accords consider seven Level 1 Loss Event types. Cyber risk is an operational risk under Basel III and can influence several of these Level 1 Loss Event types.

Primary Stakeholder

The person or organization that owns or is accountable for an Asset.

Probability of Action (PoA)

The probability that a Threat Agent will act against an Asset once contact occurs.

Productivity Loss or Cost

One of the six forms of loss, Productivity Losses are losses associated with the reduction in an organization's ability to generate its primary value proposition (e.g., income, goods, services).

Regulatory Capital

Regulatory Capital is the minimum amount of capital imposed by the regulator.

Replacement Loss or Cost

One of the six forms of loss, Replacement Losses are those associated with the intrinsic value of an asset. Typically represented as the capital expense associated with replacing lost or damaged assets (e.g., rebuilding a facility, purchasing a replacement laptop).

Reputation Loss or Cost

One of the six forms of loss, Reputation Losses are those associated with an external perception that an organization's value proposition is reduced or leadership is incompetent, criminal, or unethical.

Resistance Strength (RS)

The strength of a Control as compared to the probable level of force (as embodied by the time, resources, and technological capability; measured as a percentile) that a Threat Agent is capable of applying against an Asset.

Response Loss or Cost

One of the six forms of loss, Response Losses are the expenses associated with managing a Loss Event (e.g., internal or external person-hours, logistical expenses).

Risk

The probable frequency and probable magnitude of future loss.

Risk Analysis

The process to comprehend the nature of risk and determine the level of risk. [Source: ISO Guide 73:2009]

Risk Assessment

The overall process of risk identification, risk analysis, and risk evaluation. [Source: ISO Guide 73:2009]

Risk Factors

The individual components that determine risk, including Loss Event Frequency, Loss Magnitude, Threat Event Frequency, etc.

Risk Management

Coordinated activities to direct and control an organization with regard to risk. [Source: ISO Guide 73:2009]

Secondary Stakeholder

Individuals or organizations that may be affected by events that occur to Assets outside of their control. For example, consumers are Secondary Stakeholders in a scenario where their personal private information may be inappropriately disclosed or stolen.

Threat

Anything that is capable of acting in a manner resulting in harm to an Asset and/or organization; for example, acts of God (weather, geological events, etc.), malicious actors, errors, failures.

Threat Agent

Any agent (e.g., object, substance, human, etc.) that is capable of acting against an Asset in a manner that can result in harm.

Threat Capability (TCap)

The probable level of force (as embodied by the time, resources, and technological capability) that a Threat Agent is capable of applying against an Asset.

Threat Community

A subset of the overall Threat Agent population that shares key characteristics.

Threat Event

Occurs when a Threat Agent acts against an Asset.

Threat Event Frequency (TEF)

The probable frequency, within a given timeframe, that a Threat Agent will act against an Asset.

Trading Book

Refers to the trading floor activities in a bank.

Value at Risk (VaR)

Value at Risk is defined as the worst loss that might be expected from holding a security or a portfolio over a given period of time (say a single day or 10 days) given a specified level of probability known as the confidence level.

Vulnerability (Vuln)

The probability that a Threat Event will become a Loss Event; the probability that Threat Capability is greater than Resistance Strength. (Synonym: Susceptibility)

Acronyms & Abbreviations

ALE	Annual Loss Exposure
CF	Contact Frequency
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CRO	Chief Risk Officer
CS	Control Strength
CVaR	Conditional Value at Risk
DNS	Domain Name Service
ERM	Enterprise Risk Management
FAIR	Factor Analysis of Information Risk
FI	Financial Institution
FinTech	Financial Technology
ISA	Internet Security Alliance
ISAC	Information Sharing and Analysis Center
ISP	Internet Service Provider
IT	Information Technology
LEF	Loss Event Frequency
LGD	Loss Given Default
LM	Loss Magnitude
MCS	Monte Carlo Simulation
NACD	National Association for Corporate Directors
NIST CSF	National Institute of Standards and Technology Cyber Security Framework
NRSRO	Nationally Recognized Statistical Ratings Organization
O-RA	The Open Group Standard for Risk Analysis
O-RT	The Open Group Standard for Risk Taxonomy
OSA	Organization of American States

OTC	Over-the-Counter
PD	Period
PERT	Program Evaluation and Review Technique
PII	Personally Identifiable Information
PoA	Probability of Action
RAROC	Risk-Adjusted Return on Capital
ROSI	Return on Security Investment
RS	Resistance Strength
SICI	Systemically Important Cloud Infrastructure
SIEM	Security Information and Event Management
SIFI	Systemically Important Financial Institution
SLEF	Secondary Loss Event Frequency
TCap	Threat Capability
TEF	Threat Event Frequency
VaR	Value at Risk
Vuln	Vulnerability

References

(Please note that the links below are good at the time of writing but cannot be guaranteed for the future.)

- Crouhy, M., Galai, D., Mark, R.: The Essentials of Risk Management, 2nd Edition, McGraw Hill, 2013
- Cybersecurity Ventures: Cybercrime to Cost the World $10.5 Trillion Annually by 2025; refer to: https://cybersecurityventures.com/annual-cybercrime-report-2019/
- Cyentia Institute: IRIS 20/20 XTREME: Analyzing the 100 Largest Cyber Loss Events of the Last Five Years; refer to: https://www.cyentia.com/wp-content/uploads/IRIS2020-Xtreme.pdf
- Demos: The Great Cyber Surrender: How Police and Governments Abandon Cybercrime Victims; refer to: https://demos.co.uk/project/the-great-cyber-surrender-how-police-and-governments-abandon-cybercrime-victims/
- Durante, D., An, Y., Mark, R.: Designing and Validating your RAROC Framework, The RMA Journal, 2013; refer to: https://www.rmahq.org/ProductDetail.aspx?productid=19292425
- European Network and Information Security Agency: Introduction to Return on Security Investment, December 2012; refer to: https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment
- IBM: Cost of a Data Breach Report 2020 Highlights; refer to: https://www.ibm.com/downloads/cas/QMXVZX6R

  For the full Cost of a Data Breach Report 2020, refer to: https://www.ibm.com/account/reg/us-en/signup?formid=urx-46542. (Note: An IBM login is required for access.)
- Insurance Business America: SolarWinds® Trojan Hack Estimated to Cost Cyber Insurers $90 Million; refer to: https://www.insurancebusinessmag.com/us/news/cyber/solarwinds-trojan-hack-estimated-to-cost-cyber-insurers-90-million-243638.aspx
- ISO Guide 73:2009, Risk Management – Vocabulary, November 2009; refer to https://www.iso.org/standard/44651.html
- Mark, R., Krishna, D.: How Risky is your Risk Information?, Journal of Risk Management In Financial Institutions, 1(4), 2008; refer to: https://www.ingentaconnect.com/content/hsp/jrmfi/2008/00000001/00000004/art00011
- Nan Tie, G., Mark, B.: Parsimony – A Model Risk Paper, PRMIA Institute, 2020; refer to: https://prmia.org/PRMIAInstitute/Resources/Papers/Parsimony_-_A_Model_Risk_Paper
- National Association of Corporate Directors (NACD): Cyber-Risk Oversight, Director's Handbook Series 2014; refer to: https://www.nacdonline.org/files/NACD%20Cyber-Risk%20Oversight%20Executive%20Summary.pdf
- National Institute of Standards and Technology (NIST): Cyber Security Framework (CSF); refer to: https://www.nist.gov/cyberframework

- Organization of American States (OAS) and the Internet Security Alliance (ISA): Cyber-Risk Oversight Handbook for Corporate Boards, 2020; refer to: https://www.oas.org/en/sms/cicte/docs/ENG-Cyber-Risk-Oversight-Handbook-for-Corporate-Boards.pdf
- Roll Call: Cleaning up SolarWinds® Hack May Cost as Much as $100 Billion; refer to: https://www.rollcall.com/2021/01/11/cleaning-up-solarwinds-hack-may-cost-as-much-as-100-billion/
- The Open FAIR™ Risk Analysis Tool (I181), published by The Open Group, January 2018; refer to: www.opengroup.org/library/i181
- The Open Group Standard for Risk Analysis (O-RA), Version 2.0 (C20A), published by The Open Group, November 2020; refer to: www.opengroup.org/library/c20a
- The Open Group Standard for Risk Taxonomy (O-RT), Version 3.0 (C20B), published by The Open Group, November 2020; refer to: www.opengroup.org/library/c20b
- Verizon: Data Breach Investigations Report 2020, Executive Summary; refer to: https://enterprise.verizon.com/resources/reports/dbir/
- Wall Street Journal: Suspected Russian Cyberattack Began with Ubiquitous Software Company; refer to: https://www.wsj.com/articles/suspected-russian-cyberattack-began-with-a-little-known-but-ubiquitous-software-company-11608036495?mod=tech_lead_pos6
- World Bank: Global Economic Prospects January 2021; refer to: https://www.worldbank.org/en/publication/global-economic-prospects
- World Bank: World Bank GDP (current US$) National Accounts Data, and OECD National Accounts Data Files; refer to: https://data.worldbank.org/indicator/NY.GDP.MKTP.CD
- ZDNet: Wawa's Massive Card Breach: 30 Million Customers' Details for Sale Online; refer to: https://www.zdnet.com/article/wawa-card-breach-may-rank-as-one-of-the-biggest-of-all-times/

Acknowledgements

The Open Group Security Forum acknowledges the contribution of the following people in the refinement and publication of this document:

- Christopher Carlson, CT Carlson LLC
- Dr. Jack Freund, Cyber Assessments, Inc.
- Eva Kuiper, Invited Expert
- Altaz Valani, Security Compass
- David Vose, Vose Software
- John Linford, Forum Director, Security & OTTF, The Open Group

The Open Group and the authors of this document gratefully acknowledge the feedback received at three presentations prior to publication made to The Open Group and the Society of Information Risk Analysts. All errors are the responsibility of the authors.

About the Authors

Dr. Robert (Bob) Mark

Dr. Bob Mark is a Managing Partner at Black Diamond Risk Enterprises. He serves on several boards, has led Treasury/Trading activities, and was a Chief Risk Officer at Tier 1 banks. He is the Founding Executive Director of the MFE Program at UCLA, he has co-authored three books on Risk Management, and holds an Applied Math PhD. Bob was awarded Financial Risk Manager of the Year by GARP, is a co-founder of PRMIA, has published extensively in leading business and finance journals, and is an Individual Contributor in The Open Group Security Forum.

Mike Jerbic

Mike Jerbic is the Founder and Managing Director of Trusted Systems Consulting Group specializing in cyber risk management. He is a retired lecturer in the Economics Department at San Jose State University, and serves as Chair of The Open Group Security Forum. Prior experience includes product development engineering and management at Hewlett Packard, and IT project management consulting. He has authored several articles and book chapters for the American Bar Association as a cyber risk and economics contributor.

About The Open Group

The Open Group is a global consortium that enables the achievement of business objectives through technology standards. Our diverse membership of more than 800 organizations includes customers, systems and solutions suppliers, tools vendors, integrators, academics, and consultants across multiple industries.

The mission of The Open Group is to drive the creation of Boundaryless Information Flow™ achieved by:

- Working with customers to capture, understand, and address current and emerging requirements, establish policies, and share best practices
- Working with suppliers, consortia, and standards bodies to develop consensus and facilitate interoperability, to evolve and integrate specifications and open source technologies
- Offering a comprehensive set of services to enhance the operational efficiency of consortia
- Developing and operating the industry's premier certification service and encouraging procurement of certified products

Further information on The Open Group is available at www.opengroup.org.