# The Conditional Risk matrix – Making better decisions. A Data Story.





support@mcflosim.ch

## Foreword

Decisions are crucial. Some are quite complex in nature. Monte Carlo simulations in conjunction with a conditional risk-map maintain an overview in such situations, thereby facilitating better decisions. In the following, we will show you how to effortlessly implement better decisions within Microsoft Excel<sup>™</sup> and the associated add-in MC FLO.

## Introduction

Just as the layout of the keyboard arrangement of a typewriter aimed to break the flow of typing as little as possible, the task of the risk matrix is to represent the dangers within a very short time. Nevertheless, in the early days of the risk matrix, neither the technique of Monte Carlo simulation nor Bayesian statistics were widely prevalent as decision-making tools under uncertainty, or it took too much time to calculate all the "risks" consistently, thereby aggregated. According to economists, the continued widespread use of the risk matrix is due to path dependencies.

Critiques of the risk matrix are numerous (see also our <u>blog post</u>)<sup>1</sup>, but the alternative quantitative representation using a tornado graph (which is based on a correlation analysis) is victim of the mentioned path dependency.

For those people who appreciate quantitative analysis, but still use risk matrices for communication, MC FLO in conjunction with Microsoft Excel<sup>™</sup> can do this without effort.

### **Objectives**

The aim of a quantitative analysis using Monte Carlo simulation and Bayesian statistics is to obtain an objectively justifiable decision recommendation, considering uncertainty. In the context of classic corporate planning, the primary goal ("objective") is to generate an economic profit, which is subsumed in the following <u>example</u> as the "Expected Profit Loss" or EBIT > 0.

The classical planning process often separates drivers: The expenses and revenues which the company can directly control, as quantities produced and labor costs, are quantified and accounted in the planning tools. Indirect artefacts that are not directly under control, such as cyber-attacks, are at best modelled as a scenario, at worst delegated as part of a risk analysis using a risk matrix, and thus excluded from **an integrated quantitative** analysis. It gets even worse – because inefficient – when the drivers are accounted in both corporate planning and risk analysis without inter-action.

Let's take a closer look at the following <u>planning problem</u>. The company operates under uncertainty and therefore prepares the revenue and expenses stream using random variables. We assume that both quantities were generated using driver models (on an annual basis).



#### **Picture 1: Uncertainty regarding expenses**



#### Picture 2: Uncertainty regarding revenue

For the following analysis, however, we will focus on the "risk" of a cyber-attack. To ensure consistency in the planning process with all other driver variables, the company additionally defined random variables concerning the number of cyber-attacks per month and the severity per cyber-attack. These values can be obtained through experience or, in the absence of own data, based on data from comparable companies. By combining severity with the number of cases per month, the possible expenditure per year can be inferred via the concept of convolution.



#### Picture 3: Distribution of number of cyber-attacks per month



#### Picture 4: Distribution of compound severity

The driver variables (such as number of attacks, severity) are usually not independent, the degree of dependency is expressed in the simplest case by a correlation measure <sup>2</sup>. Among other things, the model assumes that there is a negative correlation between the severity caused by cyber-attacks and the revenue. The structure of the correlation is described by a Clayton copula.

MC FLOsim support@mcflosim.ch



#### Picture 5: Modelling inter-relationships

Once the model has been set up and the simulation has been carried out, it is relevant for the decision-makers to determine which drivers have the highest impact on the objective (in this case EBIT, "Expected Profit Loss", with an estimated value of 2.4 MCHF).

This brings us to the conditional risk matrix. All drivers are placed in the known grid (probability of occurrence and severity) but - according to Bayes' theorem - **conditional probabilities and conditional severities regarding the impact on objectives** (target) are used. But first things first.

In the long run a target of EBIT >= 0 is mandatory, so drivers that induce an EBIT of < 0 are to be regarded as risky. The simulation reveals that in about 26% of all simulated cases an EBIT < 0 is obtained. This 26% threshold is the "value-at-risk" at EBIT = 0. With the built-in Bayes formulas in MC FLO a conditional risk-matrix using the traditional charting capabilities of Microsoft Excel<sup>TM</sup> can be built from scratch. On the x-axis of the conditional risk matrix the conditional probability on the target variable at the "value-at-risk" level is displayed. It answers the following question: "What is the probability that EBIT is < 0, **given** that the driver variable "a" surpasses the "value-at-risk" threshold?". The severity can be seen on the y-axis of the risk matrix. It answers the question: "What is the average loss of the target variable (EBIT < 0), **given** that the driver variable "a" surpasses the "value-at-risk" threshold?".

For the driver variable "Expected Costs Cyber Attack", the probability is approximately 94% based on Bayes' theorem. There is a 94% probability that EBIT will be < 0, **given** that the driver variable "Expected Costs Cyber Attack" has surpassed the "value-at-risk" threshold at 26%. In this case, EBIT will be around -4.2 MCHF.

onen discente unitable: v	Choose Wizard: *	C Register variables	Best-case: 0	9 Iterations: 50'000	Diff Stat	Show statistical par-	ameters it wantable		
ose discrete variação	2 mper correspon	Po receptioned	Model Hear-case.	5 Cite contentions	100 point		0 0000000000000000000000000000000000000	Individual analysis Clo	se and Other
ose time series: *	Model specification	Fit distribution	Worst-case: 0.	1 Visualize simulation Simulation	P× Reset	Subida	See Calc constations Correlations and sensitivities	of iteration * save	esuits
merted Costs Cyber	Attack v 1	· free sother	variables/H9+8FLO	simula output("Expected Co	sets Cuber Attack"	.)			
В	0	D E	F	G H	1 1	K L	M N O P	Q R S	T U
The Bayesian way - A s	tatistical sound approach to	update beliefes given new d	ata			Risk matrix			
							and the second		
Moder setting Variable name Param 1 Param 2 Param 3 Distribution Number of cyber attacks			100		Before observing the data				
Estimated Number Cyber Attacks 0.00 10 4;6 4.00		4.00		Expected Mean Expected Profit Loss: 2.4 MCHF; Min. Target: 0 MCHF, Level			CHF, Level =		
Likelihood Number Cyber Attacks 2.75 4		4 ;	31			(0.74292	0.25708)		
Distance Estimated No.	other Alteria			10		5.0			
Posterior Escinated ing	HIGH PROPOS	12000000 1600000	150000000 4	478225223		1 A A			
Expenses		3'500'000 4'000'00	3'800'000	3766'667		Q 4.9		Revenue *	
						E 4.8			
Estimated Severity		12 0.3		170/246		\$ 47			
						1			
CorrelationPrior			0.9	0.9		3 40			
CorrelationPost			0.9	0.9		§ 4.5			
SECONDERVISION DE						0.44			
Expected Costs Cyber Att	ack		1.00	8171310		8.00			
Posterior Expected Costs	Cyber Attack		1 29	0.158.828		8:43		Expe	ected Costs Cyber
Constitution and the		been a been	marke cash			\$ 42			Attack
Maas	400	Mean	R'1	71/211.47		2 41			
10% Percentile	2.00	10% Quantil	376	10/814 13		8	Expenses •		
90% Perzentile	6.00	90% Quantil	13'5	96'202.37		2 4.0	The second s		weather working to
Probability, that # attacks	>4 76%					S 0.00%	10.00% 20.00% 30.00% 40.00%	50.00% 60.00% 70.00%	80.00% 90.00% 10
							Conditio	Inal Probability	
Dota									
Month 1	6								
Month 2	2					After observing the da	ata		
Month 3	2		Madana -		A land constants				
Month 4	1		Variants With constation		1 With correlation	1	Expected Mean Expected Profit Loss: 2.	4 MCHF; Min. Target: 0 MC	HF, Level =
Jon			No correlation	2	1		(0.74292,	0.25708)	
Statistics posterior (Lates	t Estimate) 3.26					C 2.6	Revenue •		
	2.00					ĝ.,			
10% Percentile	4.00					2 × 2			
10% Percentile 90% Percentile			Posterior cyber attacks atta	es	100000000000	5			
10% Percentile 50% Perzentile Probability, that #attacks	5>4 69%		Mean		6'984'826.07	ag 2.6			
10% Percentile 90% Perzentile Probability, that # attacks	5>4 69%				2701731.26	2	Expenses ·		
10% Percentile 90% Perzentile Probability, that # attacks	5>4 69%	and Particular	10% Quantil		a statement show that				
10% Percentile 90% Perzentile Probability, that # attacks Budget (simulated)	s>4 69% Ex-ante L	atest Estimate	10% Quantil 90% Quantil		11'599'197.35	g 2.5			
10% Percentile 50% Perzentile Probability, that # attacks Budget (simulated) Revenue	Ex-ante L	atest Estimate 14/335/627	10% Quantil 90% Quantil		11'599'197.35	2.5			
10% Percentile 90% Dezentile Probability, that # attacks Budget (simulated) Revenue Non cyber related expe	5>4 69% Ex-ante L 14'335'627 mes 3767'031	atest Estimate 14'335'627 3'76'7031	10% Quantil 90% Quantil Applying Bayes' rule		11'599/197.35	0345g wo 2.5			
10% Percentile 90% Percentile Probability, that # attacks Budget (simulated) Revenue Non cyber related exper- Cyber attack related exp	Ex-ante L 14'335'627 mes 3767'031 prms 8'1212'11	atest Estimate 14/335/627 3/76/7031 6/98/92/6	10% Quanti 90% Quanti Applying Bayes' rule Probability (ex-ante), that P	rofit > 0	11'599'197.35 74%	Coadrog us Again	Durriny_Post	rrior_Expe	
10% Percentile 90% Perzentile Probability, that # attacks Budget (simulated) Revenue Non cyber related expe Cyber attack related exp Expected Profit Loss	Ex-ante L 14'335'027 mes 8'76'7031 penses 8'171'211 2'397'385 C	etest Estimate 14/335/627 3/76/7031 6/984/326 8/588/770	10% Quantii 90% Quantii Applying Bayes' rule Probability (ex-ante), that P Probability (Latent Listmate	rofit > 0 5. Orat Smoth > 0	11'599'197.35 74%	rtoedrij vo Aguening 2.5 2.5	Dummy_Post cted_Costs_C	rrior_Expe yber_Atta ●	
10% Percentile 90% Percentile Probability, that Kattacko Budget (simulated) Revenue Non cyber related expe Cyber attack related exp Expected Profit Loss	Ex-ente         L           Ex-ente         L           14*335627         1767031           penses         8*171211           2397385         95% credible interval           95% credible interval         550% credible interval	atest Estimate 14/335627 17/27031 6/94/8205 2/583/770	10% Quantil 90% Quantil Applying Bayes' rule Probability (searce), that P Probability (searce), that P Probability (searce), that P	rofit > 0 ), that Profit > 0 rofit > 0; given number of attacks > 4	11'599'197.35 74% 85% 75%	23 25 25 25 25	Dummy, Post cted_Costs_C ck	rrior_Expe yber_Atta ●	
10% Percentile 50% Percentile Probability, that # attack Budget (simulated) Revenue Non cyber related expe Cyber attack related exp Cyber attack related exp Cyber attack related exp Dower Linner	Exercite         L           14*335627         14*335627           penses         17/2731           27327935         2737735           95% credible interval ef/set9502         6*389592           9*38*952         9*38*952	etest Estimate 14'335'027 3'76'7031 6'984'826 <b>3'583'770</b> -4'328'157 9'009'423	10% Coantil 90% Coantil Applying Bayes' rule Probability (ex-ante), that P Probability (catent tatimate Probability (catest tatimate Probability (catest Estimate	rofit > 0 (; that Shofit > 0 offit > 0; given number of attacks > 4 ); that Shofit > 0; given number of attacks >	11'599'197.35 74% 85% 4 85%	02-25 2.5 2.5 2.5 2.5 2.5	Durreny, Post cted_Costs_C ck	nfor_Dope yber_Atta ●	
10% Percentle 90% Percentle Probability, that # attack Budget (simulated) Renewa Non cyber related expe Cyber related expe Cyber attack related exp Cyber attack related exp Lower Upper	Ex-ante         D           14135567         L           1413567031         2767031           penses         17171031           2307385         2737385           95% czeółbie interval #589592         95%626592           9149508         9149508	etest Estimate 14'335'027 37'07'031 6'984'326 <b>3'585'770</b> 4'328'157 9'009'423	30% Quanti 30% Quanti Applying Rayes' rule Probability (or ante), that P Probability (catest Litimate Probability (Latest Estimate	rofit.>0 (f) (fnaf Yrofit.>U rofit.>0; g)ven number of attacks.>4 (j, that Profit.>0; given number of attacks.>	11599197.35 74% 85% 4 85%	2.5 2.5 2.5 2.5 2.5 2.5 0.00%	Dummy, Post cted_Costs_C dt 10.00% 20.00% 30.00% 40.00% 5 Condition	rfor Dipe yber Atta * a.com 60.com 70.com a ul Probability	10.00% 96.00% 100

Picture 6: Conditional risk matrix before observing new data

As can be seen, the variable "Expected Costs Cyber Attack" is the decisive driver variable, and not the expenses from the operating business. Also critical is the revenue stream, which follows from the modelled dependence between revenue and cyber-attack severity.





Given the results from the conditional risk matrix, the company can now derive measures and, for example, consider a variant that would increase investment in the IT infrastructure in combination

6

with a decreased expectation of the number of cyber-attacks. After all, the company can accept the risks described above and follow a "wait-and-see" strategy.

Despite the advantages of a simulation over mere point estimates and the coherent presentation of the outcome in the conditional risk matrix, every model must measure itself against reality and learn from it. This is where the Bayesian view of statistics helps decision-makers to refine their beliefs. To put it simply, let's assume that the uncertainty on sales and expense, the severities in the event of a cyber-attack as well as the assumed correlations are unchanged compared to the status before the data was measured, however, the number of cyber-attacks has to be adapted on the basis of the observed new data (see cells C28:C31).

If it is assumed that every cyber-attack follows a Poisson distribution. The posterior distribution of the cyber-attacks weights the initial beliefs – using Bayes' theorem - with the new data to obtain a new forecast for the end of the year ("Latest Estimate"). While the assumed number of cyber-attacks per month was 4 before the new data was measured, this drops to about 3 attacks per month based on the measured data from January-April. As the observed data is now part of the forecast, uncertainty decreases.

Ultimately, the probability of measuring EBIT < 0 at the end of the year has fallen to around 15%, resulting in a new estimated EBIT of 3.6 MCHF per EoY. As a result, the driver variables take an adjusted position in the conditional risk matrix. Given the new observed data, the conditional risk matrix can show the relevant driver variables and thus guide the decision makers.

With each new data set, the prediction can be refined and adjusted consistently. It is therefore the instrument that puts the combination of initial beliefs and data on a scientific basis.



		Information		Simulation	¢× Reset	Statistics	Correlations and sensitivities		Results		
	V I X	$\checkmark f_x \checkmark$									
В	С	D E F	G	н	I J	K L I	M N O P	Q R S	Т	U	
The Bayesian wa	- A statistical sound approach to u	pdate beliefes given new data				Risk matrix					
Model settion	Variable name Par	1 Param 2 Param 3 Distribution				Bafora obsenders the data					
Number of cyber-a	tacks		buttbutton			before observing the data					
Estimated Number Cyber Attacks		0.00 10 4;6 4.00				Expected Mean Expected Profit Loss: 2.4 MCHF; Min. Target: 0 MCHF			t: 0 MCHF, Leve	I =	
Likelihood Numa	er Cyber Attacks lized	2.75 4	3				(0.75936,0	.24064)			
Posterior Estima	ed Number Attacks		3.0			3.8					
Revenue		12'000'000 16'000'000 15'000'	000 14'333'333			Ξ.,			Depected Costs Cyb	er	
Expenses		3'500'000 4'000'000 3'800'	3'766'667			W 5.7			ALLBER		
						특 3.7					
Estimated Severity		12 0.30	170'246			6					
		🔜 MC FLO						×			
CorrelationPrior							dan Da				
CorrelationPost							Charttype 🔄 Store	results			
Expected Costs Cyl	er Attack	Output variables (5) Input variables (1)	<ol> <li>Correlation variables (-</li> </ol>	3) Summary							
Posterior Expected	Costs Cyber Attack	Outputs									
		Expected_Costs_Cyber	8000 -				Expected_Profit_Loss_o				
Statistics prior		Expected_Profit_Loss		0/027	2050.40		— c_Expected_Profit_Loss_o				
Mean	4.00	Likelihood_Normalized	8'154'059.88	x==0.037	930.19	1 2 3 4 1	Posterior_Expected_Profit_Loss_o				
10% Percentile	2.00	Posterior_Expected_Co	3'605'639.73			//	<ul> <li>c_Posterior_Expected_Profit_Loss_c</li> </ul>				
90% Perzentile	6.00	Posterior_Expected_Prc	2'538'057.10			-0.8		0.00% 70.0	00% 80.00%	90.00% 100	
Probability, that #	ttacks > 4 75%	Dummy Estimated Nar	6000-					Ity	0011 0010011		
		Dummy_Estimated_Nur						ity			
Data		Dummy_Esumated_Sev									
Month 1	6	Dummy Posterior Estin				-0.6					
Month 2	2	Dummy Posterior Estin				After observing the data					
Month 3	2	Dummy Posterior Exce	4000-								
Month 4	1	Estimated Number Ox	4000		Z has correspond	Expe		Min. Target:	0 MCHF, Level	-	
sum	11	Estimated Seventy				-0.4		24064)			
Statistics nosterior	(Latest Estimate)	Expenses				-0.4					
Mean	3.26	Likelihood_Number_Cyt									
10% Percentile	2.00	Revenue	0000								
90% Perzentile	4.00	Posterior_Estimated_NL	2000-								
Probability, that #	ttacks > 4 69%	Posterior cyb	er attacks attacs			-0.2					
		Mean			1000 100 100						
		10% Cluentil			1111	2 A A					
Budget (simulate	d) Ex-ante Lat	est Estimate 90% Quantil				Reven					
Revenue	14'336'080	14'336'080	0 -			0					
Non cyber relate	expenses 3'766'142	3'766'142 Applying Bay	State So	105 92	10						
Cyber attack rela	ed expenses 8'176'290	6'562'273 Probability (e	938	13	New 700 884						
Expected Profit L	oss 2'393'648	s'907'665 Probability (L	24	୍ କ୍ଷ୍କ	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	2.0					
	95% credible interval	Probability (e	x-ante), that Profit > 0; giv	en number of attacks > 4							
Lower	-7'197'798	-2'4 Probability (									
Upper	8'631'809	8 216 198				2 0.00% 10.0	00% 20.00% 30.00% 40.00% 50	00% 60.00% 70.00	055 80.0056 9	0.00% 100.0	
						8	Conditions	Reabability			

<sup>1</sup> See also <u>The Risk Matrix Approach: Strengths and Limitations (garp.org)</u>

<sup>2</sup> To determine the correlation, the (linear) Pearson correlation coefficient can be used, alternatively the (non-linear) Spearman Rank correlation coefficient. Copulas are used to describe the structure of dependency, such as the Gauss Copula or those named Clayton, Frank, Gumbel and others. A completely On the other hand, *transinformation*, which draws on entropy, is not yet sufficiently anchored.

Remark: the calculations were carried out on Microsoft Excel for Office and with the Monte Carlo Add-In MC FLO. MC FLO is available in German, English and Spanish.

Training video of MC FLO and Bayesian analysis: <u>https://youtu.be/dNz9YTqyK14</u>

Please let us know if you have any questions.

www.mcflosim.ch LinkedIn: <u>https://www.linkedin.com/company/14018968/</u>

