Quick Start

NC3 Luxembourg

Version 2024-11-25

Table of Contents

1. Introduction	1
1.1. Purpose	1
1.2. Other documents	1
1.3. Syntax used in the document.	1
1.4. Syntax used in MONARC	1
2. Creating the first risk analysis.	2
3. Description of the main view	3
4. Simplified risk analysis	4
4.1. Risk identification (default modelling)	4
4.2. Edit impacts and consequences.	5
4.3. Risk assessment	7
4.4. Risk treatment	7
4.5. Risk treatment plan management	3

Chapter 1. Introduction

1.1. Purpose

The purpose of this document is to help you get started quickly with MONARC. The Quick Start Guide outlines the tool's main features and shows the essential steps for addressing risks using the default settings.

1.2. Other documents



- Method Guide: Provides the complete documentation of the method.
- Technical Guide: Provides the complete technical documentation of the tool.

1.3. Syntax used in the document



H

All numbers displayed in white on an orange background are used in print-screen views to provide additional explanations. Explanations are always after the view with the corresponding numbering. **i.e.** 1.

Reference MONARC Reference

1.4. Syntax used in MONARC



The three-dot menu icon brings brings up the menu items.



Create/add something in context (assets, recommendations, etc.).



Most fields of MONARC display additional information when the pointer stay unmoved for some time.



Export any table (.csv) or graphic (.png).

Chapter 2. Creating the first risk analysis

After clicking on Create a risk analysis,

MONARC		
MyPrint [EN] [Created: Ruslan Baldan, 19/04/2022 14:38]	Create a risk analysis	×
+ Create a risk analysis	Source Source Existing risk analysis	
Copyright 2012-2023 NC3 MONARC v. 2.13.1	Select a risks model *	
	Description	
	Language "	
	Name Description	
	Cancel	Create

the following pop-up appears:

	Cre	ate a risk analys	sis			×
0	S Selec Blar	ource List of risks models C tt a risks model * nk model) Existing risk analysis			•
2		escription Language *				Ţ
4		Name - My Risk Analysis Description My first test risk analysis	s			-
	-				Cancel	Create

1. Select List of risks models

- 2. There are at least two choices. Select Modelling NC3. Modelling NC3 is the default template made available by the MONARC editor. It provides sufficient knowledge bases to start a risk analysis. This option should be used by default to start a new risk analysis.
- 3. Select your preferred language for this new analysis. (FR/EN/DE/NL)
- 4. Give a name for your risk analysis, for example, *My analysis*.
- 5. Optional field, which allows you to describe your analysis in more detail.

Chapter 3. Description of the main view

	Home > MyPrint [EN]				(2						4	* =	ж З	Ð
	0	2			-	3—	_	0	0					-0	D
MyPrint [EN] [Created: Ruslan Baidan, 1904/2022 14:38]	Risk analysis	MyPrint	[EN	ŋ		:									
+ Create a risk analysis	Expand all / Wrap all Q Search an asset	Informatio	n ris	ks		Operation	al risks								I
Copyright 2012-2023 NC3 MONARC v. 2:13.1	MyPrint [EN] + IoT + Printing department + Computer graphics department + GDPR legal obligations	163 informati risks	ion			Risk threshol	d (on max	(CIA) (CIA)	C C Keywords Sot Sort dw MAX risk V Desce	ction nding 👻	Kind o	if treatm	ent 💌	۹	I
•	Assets library		1	mpa	ct	Threa	at		Vulnerability		C	arrent ri	sk	-	
	Q Search an asset	Asset	с	1	۸	Label	Prob.	Label	Existing controls	Qualif.	с	1	Α	Treatment	
	+ Fundamentals + EBIOS	User workstations	1	3	2	Forging of rights	3	Authorisation management is flawed	No access control	5	15			Reduction	
		Printing operators	1	2	3	Error in use	3	Users are not made aware of information security	The person in place does not want training. He is retiring soon.	4	12	24	36	Accepted	

- 1. Risk Analyses panel: Create and select a risk analysis. Once the analysis is selected, the left column can be retracted to optimize the horizontal space by clicking on the icon
- 2. Navigation panel: User administration and account management.
- 3. Access to steps of the method by clicking on numbers 1 to 4.
- 4. Contextual working areas of analysis.

Chapter 4. Simplified risk analysis

4.1. Risk identification (default modelling)

It is necessary to use the assets of the library and place them in the analysis. If the risk analysis does not contain any assets, follow the instructions below, otherwise go to the next chapter.

By default, MONARC suggests a structure where primary assets (business assets) are placed at the root of the analysis, with supporting assets organized beneath them. In order to simplify this step, two groups of assets have been created:

- Front-Office: This asset group identifies common risks associated with a 'Human Resources' department from the user's perspective, including risks related to office spaces, computers, applications, and physical and environmental factors.
- Back-Office: This asset group identifies cross-functional risks within the organization, specifically those related to IT and general organizational functions.

\equiv Home $ ightarrow$ My Analysis				🌣 🔺 🗰 🖻
0	-0	•	0	
Risk analysis Expand all / Wrap all	My Analysis Risks analysis			
Q Search an asset	Information risks Operational risks			
My Analysis	0 information risks	Risk threshold (on max CIA)	Kind of treatment 👻 Q 🕣 🛃 MAX risk 🔻	Sort direction Descending v
Assets library	There are no nows for one incentive, or your meric recorrect no resource.		Page: Rows per page: 20 1 - 0	l of 0 < >
Search an asset				
Fundamentals Dramas Vasets Department Boo China Boo Chin				

Click on the + or the - to expand or wrap all categories of the library.

- 1. In the category Primary assets, click on Department and then, by holding down the left mouse button, move the asset to the analysis area just above (Drag and Drop).
- 2. In the category Model Structure find the assets Front Office and Back Office and then, by holding down the left mouse button, move the asset to the asset Department, which is now in the analysis area.

Risk analysis	My Analy My Analysis	ysis - for	S dem	nons	tration purpose	5	•	
Q Search an asset	Informatio	n ris	ks		Operational	risks		
 My Analysis Department Front Office Service office Employees 	84 4 informati risks	on			Risk threshold (r	on max C	(A) (O) (A) (A) (A) (A) (A) (A) (A) (A) (A) (A	Sort MAX risk
 User workstations + Specific software 	• •	Ir	mpa	ct	Threat			Vulnerability
3 - Back Office	Asset	с	I.	А	Label	Prob.	Label	Existing controls
Building Troom	Administrator workstations	-	-	-	Forging of rights	-	Authorisation management is flawed	
Administrator workstations	Administrator workstations	-			Forging of rights		User authentication is not ensured	
+ Backup management	Administrator workstations	-			Forging of rights	-	The user workstation is not monitored	
Software development	Administrator workstations			-	Retrieval of recycled or discarded media	-	Presence of residual data unknown to the user of reallocated or discarded equipment	

- 1. The risk analysis now offers a model for *Department*.
- 2. The *Front Office* now offers a default identification of the risks on the users' side.
- 3. The *Back Office* now offers a default identification of the risks, for IT and organization.
- 4. The total number of risks in this model is 84 (in this case).



The Identified risks are those commonly encountered and considered significant by default, though they are not intended to be exhaustive.

4.2. Edit impacts and consequences

The goal is to define the impacts and consequences on primary assets that may result from a risk occurring within the model. In this analysis, the primary asset is the *Department*.

≡ Home > My Analysis											٠	÷	₩ Ð
0	_2				(3)			-0-				-0
Risk analysis				Co	Depai Departm nfidentiality erited	rtment lient as ar : I	t 2 n entity that regr ntegrity : Inh	oup persons erited Ava	۲ پ	Edit impa	acts)	
My Analysis	Informatio	n ris	ks		Operational	risks			7	Export a	nalysis		
Front Office Service office Benployees User workstations + Specific software	84 informati risks	on			Risk thresho	ld (on ma atment	× CIA)	Sort	• •	Asset co See asso Detach	ntext et in the lib	rary	
- Back Office	Arrest	Ir	npad	ct	Threat			Vulne	ability				urrent ri
IT room	Asset	с	I.	A	Label	Prob.	Label	Exist	ing con	trols	Qualif.	с	1
System administrator Administrator workstations	Administrator workstations	•			Forging of rights		Authorisation management is flawed						
workstations													

- 1. Click on the primary asset Department.
- 2. Click on the icon 📋 to display the context menu of the asset.
- 3. Click on Edit impacts.

The pop-up below appears.

Edit impacts						×
	Consequences			(Show hidden conse	quences
	Reputation 🔘	Operational 🔘	Legal 🔘	Financial 🔘	Personal 💿	Max
Confidentiality	2 👻	0 -	2 👻	Unknown 👻	3 👻	3
Integrity	Unknown 👻	Unknown 👻	Unknown 👻	Strong impact, hardly bears Information leaks seriously - Confidential information I - Bank secrecy	ible. harm organization's interest eaks.	t. Example:
Availability	Unknown 👻	Unknown 👻	Unknown 👻	- Sensitive personal data - Security incident		

1. Consultation of impact scales is done through the menu at the top right of the screen.



By leaving the pointer unmoved over the numbers, the meaning of this number appears after one second.

When one of the criteria **C** (confidentiality), **I** (integrity) or **A** (availability) is allocated, there is a need to ask: what are the consequences on the company, and more particularly on its ROLFP, i.e. its **R**eputation, its **O**peration, its **L**egal, its Finances or the impact on the **P**erson (in the sense of personal data).

Save

Cancel

In the case of the above figure, the 3 (out of 5) impact on confidentiality, is explained by the maximum value ROLFP regarding confidentiality. Example, 3 is the consequence for the person in case of disclosure of his personal file.

4.3. Risk assessment

Risk analysis	🜐 Bu	ildin	g	:	Con	fidentiality : Inherit	ed Integrity : Inherited		Av	/ailab	ility : I	nherited				
Expand all / Wrap all Q Search an asset	Risk threshold (on max CIA)									of treatment 👻 🔍 📀 👲						
My Analysis Department Front Office Service office	5 info risks	rma	tion		•											
Employees User workstations	Asset	Impact		Threat	U		Vulnerability 6	0	Cu	Current ri		Treatment	Residual			
+ Specific software		с	A	Label	Prob.	Label	Existing controls	Qualif.	с	<u> </u>	A					
Back Office Building Differe	Building			Theft or destruction of media, documents or equipment		The principle of least privilege is not applied						Not treated				
System administrator Administrator workstations	Building			Theft or destruction of media, documents or equipment		Authorisation management is flawed						Not treated				

- 1. Click on a secondary asset, for example Building.
- 2. CIA Impact: It has been assigned to the *Department* and is inherited by default, so no further action is required.
- 3. Threat: *Theft or destruction of media, documents or equipment* is a physical threat that expresses fear of being robbed or destroyed materials.
- 4. Probability (Prob.): This is an estimate of the probability on a scale of 1 to 4 that the threat occurs. Take, for example, the case of a very large company where this threat is above average, so **3**.
- 5. Vulnerability: *The principle of least privilege is not applied*. The security principles focus on determining who has access rights and whether those rights align with the responsibilities of the individuals involved.
- 6. Existing controls: Describe, in a factual manner, the security controls in place regarding this vulnerability or, more broadly, the risk in question. Take, for example, a second unfavourable case, for example a hospital where the whole building is like a public area.
- 7. Qualification (Qualif.): Concerning the measure in place (point 6 above), the vulnerability qualification is therefore maximum of 5 out of 5.
- 8. Current Risk : All the parameters for calculating the risk are present, the current risk is therefore calculated based on the CIA values, which are directly dependent on the threat.



By leaving the pointer on most fields, a tooltip appears after 1 second.

4.4. Risk treatment

The risk treatment consists of proposing one of the 4 types of treatment, knowing that most of the time the treatment is to reduce the risk by allocating a control, or to accept a weak risk. To access the risk treatment table, click on Not treated in the *Treatment column*.

Building		Confidentiality : Inherited	Integrity : Inherited	Availability : Inherited
		с	I	A
Current risk				
Residual risk		•		
Asset	😳 De	partment > Back Office > Building		
Threat	Theft	or destruction of media, documents or equipmen	t	
Threat probability	÷			
Vulnerability	The p	rinciple of least privilege is not applied		
Vulnerability qualification	-			
Risk owner				
Risk context				
Existing controls				
Recommendations				
Search a recommendation 🕒				
Kind of treatment	=	Not treated 🔹 🙎		
Vulnerability reduction		3		
Security referentials	11.1.2	SO 27002 2 - Physical entry controls		
< Previo	ous		Back to the list	Next > 4

- 1. Create one or many recommendations.
- 2. Define the treatment type (according to ISO / IEC 27005).
- 3. Estimate the risk-reducing value in order to define the residual risk.
- 4. Save the treatment (or click 'Next' in case you do more than one risk treatment at once).

4.5. Risk treatment plan management

≡ Home ➤ My Analysi															* ±	₩ Ð
0		2	_	_			_3									_
Risk analysis	^	My Analy	sis		:		Ev	aluation	and treatment of	risks						
Expand all / Wrap all		RISKS analysis	5		•			7 Estimation	evaluation and risk treatme	nt						
Q Search an asset		Information	ı risk	6	Operational risks			Risk treatment plan management ①								
My Analysis		84 inform	otic		Risk threshold (on	max CIA) (Delit	verable: Final	report C Keywords	Kind	of treatme	ent 👻	Q	Ð		
-Service office -Service office - Service office - Service office - Service office	Risk t	creatment p	olar	i mai	nagement			Cort	Cad direction				×	<	Treatment	Target
- Building				Pecomr	nendation		Imp	Assat	Existing controls	Current ris	ek	Target	riek	Α		TISK
- HT room O System administrator Administrator	<u>↓</u> (Entry 4 Control all person	s in tr	ie entra	nce of the building		•••	Building	No access control	45		18		30	Reduction	18
workstations		Administrator workstations	3	2 2	Forging of rights		Authorisati manageme	ion ent is flawed			-	•			Not treated	
Backup managemen	nt	Administrator workstations	3	2 2	Forging of rights		User authen not ensure	entication is			-	-			Not treated	
T organization		Administrator workstations	3	2 2	Forging of rights	-	The user v is not mon	vorkstation itored			-	-	-	-	Not treated	•
I I L- Software developme	ent						-									

In that case, the risk treatment plan only consists of one risk, but once all risks are treated, all risks and information risk recommendations will be in the treatment plan.

- 1. The call of the pop-up is done by clicking on the 3rd step of the method (Evaluation and treatment of risks) and choosing the link Risk treatment plan management.
- You can order the recommendation positions by holding down the left mouse button on the icon
 and moving it.
- 3. Reset the positions in importance order (Imp.)
- 4. Edit recommendation

A final report of the risk analysis can be generated by clicking on the 3rd step of the method and choosing the link Deliverable: final report.



Deliverables are only relevant when the MONARC method has been fully processed and all information has been entered.