

SERIMA - GUIDE UTILISATEUR

17, rue du Fossé Adresse postale L-2922 Luxembourg

T +352 28 228 228 F +352 28 228 229 info@ilr.lu

www.ilr.lu

Table des matières

1.	Intro	oducti	ion	3
2.	Envi	ronne	ement	3
2	.1.	Mot	de passe	3
2	.2.	Auth	nentification forte	3
3.	Pers	onnal	lisation de l'analyse de risques	3
3	.1.	Supp	pression de services - Détacher des actifs primaires	4
	3.1.2	1	Aperçu	4
	3.1.2	2.	Description	4
3	.2.	Perso	onnalisation – ajout d'assets	5
3	.3.	Perso	onnalisation – ajout de risques	5
4.	Réal	lisatio	on de l'analyse de risques	6
4	.1.	Confi	figurer les critères d'impact	6
	4.1.2	1	Aperçu	6
	4.1.2	2.	Description	6
5.	Crée	er un e	export JSON	7
5	.1.	Aper	rçu	7
5	.2.	Desc	cription	8
5	.3.	Prod	luction d'un export JSON avec un outil autre que SERIMA	9
6.	FAQ			10
6	.1.	Nami	ing convention	10
6	.2.	Traite	ement des risques	10
	6.2.2	1.	Risque non-traité	10
	6.2.2	2.	Risque refusé	11
7.	Supp	port		11



1. Introduction

Ce document a comme objectif de décrire comment procéder à des configurations spécifiques dans SERIMA dans le but de soutenir les opérateurs dans l'utilisation de l'outil.

Ce document sera adapté en fonction des évolutions et des besoins des parties prenantes.

2. Environnement

L'ILR met à disposition des opérateurs sous sa responsabilité un environnement SERIMA. Cet environnement s'appelle un « Front Office ». Celui-ci est associé à un administrateur chez l'opérateur, qui gère l'environnement et y donne accès à ses collègues au besoin.

2.1. Mot de passe

Un environnement, respectivement un compte, est associé à une adresse e-mail. Son propriétaire doit définir son propre mot de passe en sélectionnant « mot de passe oublié ». Ainsi, il reçoit un lien par e-mail lui permettant de définir le mot de passe. Attention, il est important avant de cliquer sur le lien de fermer toute fenêtre SERIMA / Monarc.

2.2. Authentification forte

Pour des raisons de sécurité, merci d'activer systématiquement l'authentification à deux 2 facteurs (2FA) en vous rendant dans votre profil.

3. Personnalisation de l'analyse de risques

L'ILR met à disposition de ses opérateurs une pré-configuration de SERIMA sur base de la librairie sectorielle définie conjointement. Cette pré-configuration contient tous les services respectivement services essentiels du secteur en question. Or, chaque opérateur n'offre pas forcément tous les services, respectivement services essentiels de son secteur. La première étape, après la création d'une analyse de risques sur base du modèle configuré par l'ILR, est de ne garder que les services, respectivement services essentiels prestés par l'opérateur. La méthode à suivre est décrite <u>ci-dessous</u>.

Par ailleurs, le modèle SERIMA correspond à la librairie sectorielle, qui peut être considérée comme « le plus petit dénominateur commun » entre tous les opérateurs d'un même secteur. Or chaque opérateur a ses spécificités, qu'il doit ajouter à l'analyse de risques. Chaque opérateur doit donc personnaliser son analyse de risques. Cette personnalisation consiste en :

- L'ajout des assets de support manquants
- L'ajout de risques spécifiques à l'opérateur.

3.1. Suppression de services - Détacher des actifs primaires

3.1.1. Aperçu

Pour supprimer un service, respectivement un service essentiel, il suffit de détacher l'asset primaire correspondant.

3.1.2. Description

- 1. Cliquer sur l'actif primaire concerné
- 2. Appuyer sur le menu
- 3. Cliquer sur « Détacher »
- 4. Cliquer sur « Détacher » encore une fois pour confirmer
- 5. L'actif primaire détaché est supprimé de l'analyse de risque

<u>Note</u>

• Quand vous détachez un actif primaire, alors tous les actifs de support liés à cet actif primaire seront supprimés

Exemple de la suppression du service « Market Communication » d'une analyse contenant 5 services.

Analyse des risques		^	ILR En Elec Sup M	arket conîmunic
	Tout déplier / Tout replier		Supply - Market communication	
Rechercher un actif Elec AR 1			Risques de l'information	Risques opération
+ ILR_En_Elec_Operatio + ILR_En_Elec_Operatio + ILR_En_Elec_Balancin + ILR_En_Elec_Supply_ LIR_En_Elec_Supply_	on_of_electricity_distribution_system on_of_electricity_transmission_system og_offer_and_demand of_electricity arket_communication 1		1 risques de l'information	Seuil de risque (sur le



II R



Seuls restent les 4 autres services non détachés.

Analyse des risques	^	Elec AR 1	
Tout déplier / Tout replier		Test monitoring	
Q Rechercher un actif		Risques de l'information	Risques
 Elec AR 1 + ILR_En_Elec_Operation_of_electricity_distribution_system + ILR_En_Elec_Operation_of_electricity_transmission_system + ILR_En_Elec_Balancing_offer_and_demand + ILR_En_Elec_Supply_of_electricity 	5	113 risques de l'information	Seuil de
		Actif	

3.2. Personnalisation – ajout d'assets

Pour personnaliser une analyse de risques, il peut être nécessaire d'y ajouter des assets. Ceux-ci peuvent être soit existants dans la base de connaissances, soit à créer. Pour plus d'informations, veuillez-vous référer au user-guide disponible sur <u>https://www.monarc.lu/documentation/</u>.

3.3. Personnalisation – ajout de risques

Pour ajouter un risque impactant un asset, il suffit 1) de sélectionner l'asset en question, 2) de cliquer sur « *Créer un risque spécifique »*.

Test	2 risques de l'in	orm	atio	Seuil de ris	que (sur l	e CID max) 🕘 💫 🗌 🗌 Mots-clés	Type de traitement 👻	Q 0	±	R	isque M/	XX 👻 Décr	oissant •
ILR_ITaining_Essential_Service_1 ILR_Training_Sub_Service_1	1	Imp	act	Menace		Vulněrabilité			Ris	que ac	ctuel	Talland	Risque
	Acti	C	D	Libellé	Prob.	Libellé	Mesures en place	Qualif.	с	1	D	traitement	résidue
ILR_Training_Fileserver	ILR_Training_Datacenter	2 3	4	Destruction de matériel ou de supports	-	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects		1.00				Non traité	- 24
···· ULR_Training_Internet	ILR_Training_Datacenter	2 3	4	Perte d'alimentation énergétique	2.50	Réseau électrique instable					•	Non traité	
Comparison of the second	ILR_Training_Datacenter + Créer un risqu	2 S	4 cifiqu	e 2	2.53	Réseau électrique instable	Page 1 👻	- Lignes pa	r page :	2	•	Non b	raité e 2

Pour plus d'information, veuillez-vous référer au user-guide disponible sur <u>https://www.monarc.lu/documentation/</u>.

II R

4. Réalisation de l'analyse de risques

Une fois l'analyse de risques personnalisée, l'évaluation des risques peut commencer. Pour rappel, d'après la norme ISO27005 un risque a trois composantes : une menace qui exploite une vulnérabilité pour résulter en un impact. Il est important de noter, dans le cadre de SERIMA, que la vulnérabilité est celle d'un asset de support, mais que l'impact à estimer est celui sur le service, respectivement le service essentiel.

4.1. Configurer les critères d'impact

4.1.1. Aperçu

Ce sous-chapitre vise à décrire brièvement comment procéder pour la configuration des critères d'impact dans SERIMA. La bonne pratique est de réaliser cette configuration au niveau du service respectivement du service essentiel. Cette configuration est alors propagée à tous les éléments contenus dans ce service. Puis, si et seulement si nécessaire, d'adapter cette configuration à un niveau plus bas dans la hiérarchie des assets, par exemple au niveau d'un asset de support.

4.1.2. Description

- 1. Sélectionner l'actif concerné (typiquement le service)
- 2. Appuyer sur le menu
- 3. Cliquer sur « Modifier les impacts »
- 4. Configurer le niveau des impacts
 - a. Ici, il est très important de configurer au moins la ou les colonnes correspondant aux critères d'impact de la librairie sectorielle. En d'autres mots, il n'est pas obligatoire (même si vous pouvez le faire) de configurer les colonnes correspondant à « *Réputation », « Opérationnel », « Légal », « Financier », « Personne »*. Par contre, il est obligatoire de configurer les colonnes suivantes, provenant de la librairie sectorielle.
- 5. Sauvegarder la configuration
- 6. Ligne par ligne, c'est la valeur « max » de l'impact qui est prise en compte pour le calcul du risque

Voici un exemple concret :

ſ	Analyse des risques	ILR_Training_Essential	Service_1 _{Confidentialité} : Hérité	Intégrité : Hérité	Disponibilité : Hérité	
	Tout déplier / Tout replier	Essential Service 1	•			
	Rechercher un actif	Risques de l'information	Risques opérationnels 2			
	+ ILR_Training_Essential_Service_1 1 + ILR_Training_Essential_Service_2	36 risques de	Seuil de risque (sur le CID max) 💿	Mots-clés	Type de traitement 💌 🔍 📀 🔮 Treer Risque MAX	-
	Bibliothèque d'actifs	Thiomaton		Sens du tri Décroissant ▼		

Analyse des risques	^	ILR_Training_Essential_S		Modifier les impacts	Ì
Tout déplier / Tout replier		Essential Service 1	-		
Rechercher un actif		Risques de l'information	Ŷ	Importer une analyse	
ntest			7	Exporter l'analyse	
+ ILR_Training_Essential_Service_1 + ILR_Training_Essential_Service_2		36 risques de	•	Contexte de l'actif	С
		l'information		Voir l'actif dans la bibliothèque	
Bibliothèque d'actifs	^		Ж	Détacher	
Bechercher un actif	n				

	Conséquences					4 (At	fficher les conséqu	ences m	asquées
	Réputation 💿	Opérationnel 🗿	Légal 🧿	Financier 🗿	Personne 🕥	Personnes impactées	0	Durée d'indisponibilité du service	0	Мах
Confidentialité	Non renseigné 👻	2	•	2	•	2				
Intégrité	Non renseigné 👻	Non renseigné 🔻	Non renseigné 👻	Non renseigné 👻	Non renseigné 🔻	3	*	3	•	3
Disponibilité	Non renseigné 👻	Non renseigné 🔻	Non renseigné 👻	Non renseigné 👻	Non renseigné 👻	4	*	4	•	4
					1			Annuler	Sa	5 uvegarder

Actif	Γ	Impac	t	Menace		Vu	Inérabilité		Ris	que ac	tuel	Traitament	Risque
Acui	с	1	D	Libellé	Prob.	Libellé	Mesures en place	Qualif.	с	1	D	natement	résiduel
ILR_Training_Datacenter 6	2	3	4	Destruction de matériel ou de supports	-	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects		-			-	Non traité	-
ILR_Training_Datacenter	2	3	4	Perte d'alimentation énergétique	-	Réseau électrique instable					-	Non traité	-
ILR_Training_DBMS_Database_Management_System	2	3	4	Usurpation de droits	-	Mauvaise gestion des mots de passe		-	-	-	-	Non traité	-

5. Créer un export JSON

5.1. Aperçu

ILR

Pour rappel, l'ILR n'a pas accès au contenu de votre environnement SERIMA. Il est donc nécessaire que vous exportiez votre analyse de risques au format JSON et que vous l'envoyiez de manière sécurisée à l'ILR. D'ailleurs, si vous ne disposez pas de moyens de communication sécurisés, l'ILR peut, sur demande, vous envoyer un lien OTX dont la validité est limitée dans le temps.

Ce sous-chapitre vise à décrire comment créer un export de l'analyse de risque sous le format JSON dans SERIMA.

5.2. Description

- 1. Cliquer sur l'analyse de risques
- 2. Appuyer sur le menu
- Sélectionner « Exporter toute l'analyse des risques » Exporter les évaluations : oui Mesures en place : oui Recommandations : oui
- 4. Appuyer sur le bouton « Exporter »
- 5. Un fichier JSON contenant l'analyse de risques est produit

<u>Note</u>

Vous avez la possibilité (non requis) de sécuriser votre fichier JSON avec un mot de passe. Dans ce cas, vous devrez également nous transmettre de manière sécurisée le mot de passe pour que nous puissions ouvrir le fichier.

Analyse des risques	Elec AR 1	2
Tout déplier / Tout replier	Test monitoring •	
Q Rechercher un actif	Risques de l'information	Ris
Elec AR 1 ILR_En_Elec_Operation_of_electricity_distribution_system ILR_En_Elec_Operation_of_electricity_transmission_system ILR_En_Elec_Balancing_offer_and_demand ILR_En_Elec_Supply_of_electricity	113 risques de l'information	Seu
	Actif	

Analyse des risques	^	Elec AR 1		Modifier l'analyse des risques
Tout déplier / Tout replier		Test monitoring		mounter ranaryse des risques
Q Rechercher un actif		Risques de l'infor	Ŷ	Importer une analyse de risques
★ Elec AR 1	-		~ 7	Exporter toute l'analyse des risques
HLR_En_Elec_Operation_of_electricity_distribution_system HLR_En_Elec_Operation_of_electricity_transmission_system HLR_En_Elec_Balancing_offer_and_demand HLR_En_Elec_Supply_of_electricity		113 risques de l'information	Î	Supprimer l'analyse



1 5		
Chiffrement		
Vous pouvez entrer un mo	t de passe pour protéger votre analyse inalisé	e des risques
Mot de passe		O
Sans mot de passe		
Options d'export		
Exporter avec les évaluations ? Oui		•
Options		
Étapes de la méth	ode Mesures en place	N
Interviews	Recommandations	43
Déclaration d'appl	icabilité	
Registres des activ	vités de traitement	4
	Annuler	Exporter

5.3. Production d'un export JSON avec un outil autre que SERIMA

Au cas où un opérateur souhaiterait utiliser un outil autre que SERIMA, il doit tout de même fournir un export au format JSON afin que l'ILR puisse, secteur par secteur, collecter toutes les informations dont il a besoin pour ses missions.

Les schémas JSON, ainsi que les données JSON, sont disponible sous : <u>https://objects.monarc.lu</u>. Des exemples d'objets composés sont également disponibles sous : <u>https://objects.monarc.lu/schema/21</u>.

La génération du fichier d'export d'une analyse de risques pouvant être complexe, car elle contient beaucoup de liens entre les différents éléments, il est conseillé de commencer par étudier un fichier provenant d'une analyse contenant très peu d'éléments.

ILR

ElecAR1.json

5

Par ailleurs, SERIMA étant un outil open source, chacun a accès à son code, peut s'en inspirer et peut même contribuer à le faire évoluer.

6. FAQ

6.1. Naming convention

- Dans un actif, p. ex. « ILR_En_Elec_Gen_Storage », quelles est la signification de « Gen » ?
 "Gen" (Generic) veut dire que ce sont des actifs de support génériques utilisés dans chaque librairie sectorielle. Ces actifs sont identiques pour tous les secteurs.
- Dans un actif, p. ex. « ILR_En_Elec_Spe_IT_Management », quelle est la signification de « Spe » ?
 "Spe" (Specific) veut dire que les actifs concernés sont des actifs de support spécifiques utilisés dans un secteur ou sous-secteur particulier.
- Quelle est la signification d'un risque « non-traité » ?
 Un risque "non-traité" veut dire qu'un traitement du risque n'a pas encore été sélectionné, c'est-àdire que le risque n'a pas encore été évalué, réduit, refusé, accepté ou partagé.
- Quelle est la signification d'un risque « refusé » Refuser un risque veut dire qu'un acteur évite de prendre le risque qui est en lien avec l'actif concerné.

Un risque "refusé" pourrait p. ex. conduire à la suppression de certaines activités qui sont liées au service essentiel en question, ou encore forcer les opérateurs à appliquer des changements importants relativement aux conditions opérationnelles de l'actif concerné pour poursuivre les activités affectées. Les actions à entreprendre dans le contexte d'un risque « refusé » dépendent de la nature du risque concerné.

6.2. Traitement des risques

6.2.1. Risque non-traité

L'ILR considère un risque comme étant non-traité si :

- Soit le risque n'est pas évalué (niveau de menace, niveau de vulnérabilité, impact manquant)
- Soit le traitement est resté sur non-traité

A l'inverse, un risque est considéré comme traité s'il est évalué et, que son traitement est un des éléments suivant (Réduction, Refusé, Accepté, Partagé) et que le plan de traitement contient les mesures liées à ce traitement.

6.2.2. Risque refusé

Refuser un risque veut dire que vous refusez de prendre le risque qui est en lien avec l'actif concerné. Attention, un risque "refusé" pourrait donc conduire à ne pas utiliser un actif nécessaire à la fourniture du service essentiel en question.

7. Support

Pour tout besoin de support, veuillez contacter serima@ilr.lu ou +352 28 228 380.

