



INSTITUT LUXEMBOURGEOIS  
DE RÉGULATION

---

## ATELIER

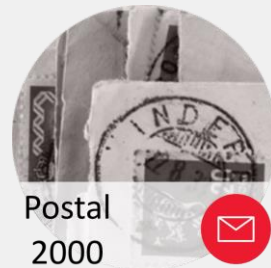
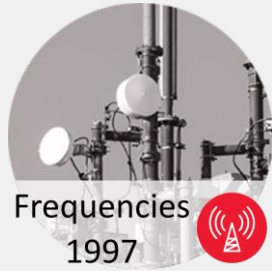
*présentation de méthodes de contrôle et de  
prévention de la sécurité des réseaux*

# Agenda

1. Présentation ILR
2. Cadre légal
3. Approche et expériences ILR



Service NISS



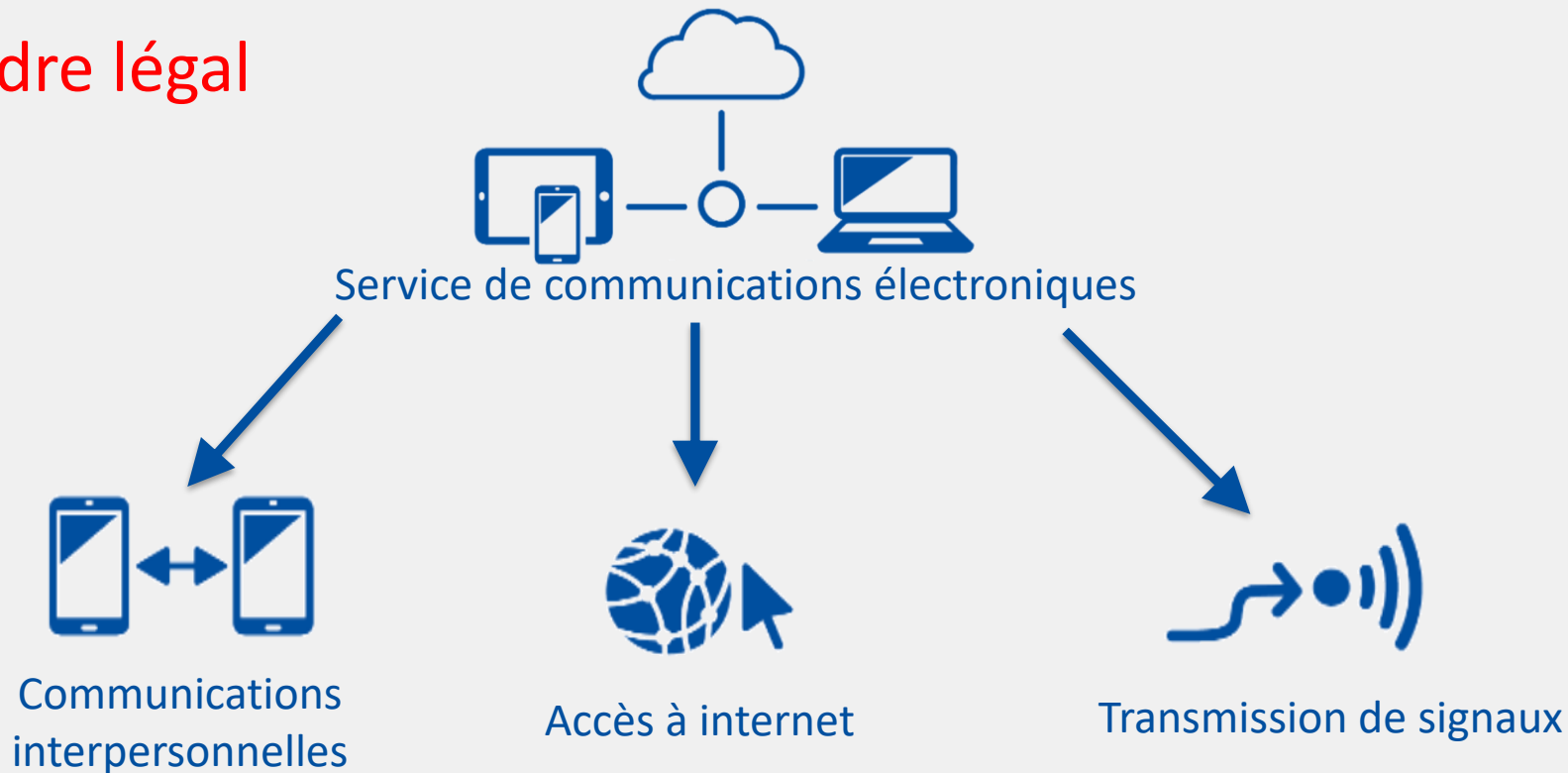
Et depuis  
2019 NISS:



# Cadre légal

Loi du 17 décembre 2021 sur les réseaux et les services de communications électroniques

# Cadre légal



# Cadre légal

## Obligations:

- Prendre les mesures techniques et organisationnelles
- Gérance des risques
- Notification des incidents

# Approche ILR

Depuis 2016 - collaboration avec LIST

Analyse de risque – outil basé sur MS Excel

Séminaires - Nomenclature commune

**Risque =  $f$ (menace, vulnérabilité, impact)**



Risk assessment

SERVICE	GROUP	THREAT	AFFECTED ASSET(S)	THREAT LEVEL	% OF AFFECTED CUSTOMERS	EXPECTED UNAVAILABILITY	IMPACT LEVEL	VULNERABILITY	ACTUAL VULNERABILITY LEVEL	RISK	COMMENT	TREATMENT	CONTROLS	NEW VULNERABILITY LEVEL	% OF AFFECTED CUSTOMERS	EXPECTED UNAVAILABILITY	IMPACT LEVEL	ESTIMATED RESIDUAL RISK
				1	5	5			0	0*				0	5	5		0
Fixed voice	Telco (INTERNATIONAL)	Fire	11 affected assets	1	5	5	Very high	Presence of flammable equipment and/or stuff	0	0*		Retention	A.11.2.1 , A.11.2.9	0	5	5	Very high	0*
								Lack or bad maintenance of the fire detection system					A.11.2.1 , A.11.2.2					
		Water damage	11 affected assets	1	5	5	Very high	Location in an area susceptible to flood	0	0*		Retention	A.11.1.4 , A.17.1.1 , A.17.1.2 , A.17.1.3 , A.17.2.1	0	5	5	Very high	0*
								Lack of facility maintenance					A.11.1.4 , A.17.1.1 , A.17.1.2 , A.17.1.3 , A.17.2.1					
													A.11.1.4 .					

# Approche ILR

Harmonisation est important !

Liste commune:

- des actifs
- menaces
- Vulnérabilités

Échelle d'impact

## Exemples:

### List and description of supporting assets

	Name	Ow	Type
1	CPE - Customer Premises Equipment (home access GW)		Hardware
2	DLU - Digital Line Unit		Hardware
3	DSLAM - Digital Subscriber Line Access Multiplexer		Hardware
4	FastLink		Hardware
5	GPON - Gigabit Passive Optical Network		Hardware
6	MSAN - MultiService Access Network		Hardware
7	NT - Network Terminal		Hardware
8	ONT - Optical Network Terminal		Hardware
9	PABX - Private Automatic Branch eXchange		Hardware
10	Data Center facilities		Hardware
11	Load balancer		Hardware
12	Router		Hardware
13	Server		Hardware
14	Storage		Hardware
15	Switch		Hardware

## Exemples:

### List and description of supporting assets

	Name	Own	Type
1	CPE - Customer Premises Equipment (home access GW)		Hardware
2	DLU - Digital Line Unit		Hardware
3	DSLAM - Digital Subscriber Line Access Multiplexer		Hardware
4	FastLink		Hardware
5	GPON - Gigabit Passive Optical Network		Hardware
6	MSAN - MultiService Access Network		Hardware
7	NT - Network Terminal		Hardware
8	ONT - Optical Network Terminal		Hardware
9	PABX - Private Automatic Branch eXchange		Hardware
10	Data Center facilities		Hardware
11	Load balancer		Hardware
12	Router		Hardware
13	Server		Hardware
14	Storage		Hardware
15	Switch		Hardware

THREAT	Mandatory
Fire	X
Water damage	X
Major accident	X
Destruction of equipment or media	X
Natural disaster	X
Power supply failure	X
Loss of essential services	X
Disturbance due to radiation	X
Theft of equipment	X
Data from untrustworthy sources	X
Equipment failure	X
Equipment malfunction	X
Software malfunction	X
Breach of information system maintainability	X
Unauthorised use of computers, data, services and applications	X
Corruption of data	X

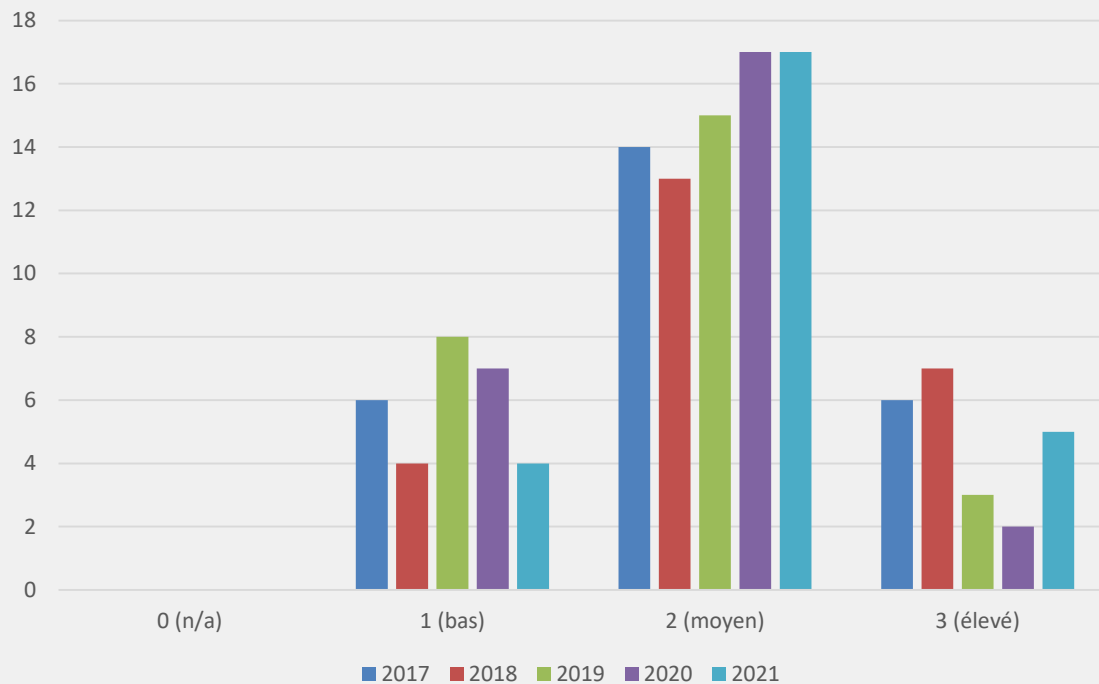
# Approche ILR

## Liste mesures de sécurité de l'ENISA

- Sécurité des ressources humaines
- Sécurité des systèmes et des ressources
- Gestion des opérations
- Gestion des incidents
- Gestion de la continuité de l'activité
- Surveillance, inspection et test
- Sensibilisation aux menaces.

## Exemple:

Niveau	Mesure de sécurité	Évidence
Bas	Fournir au personnel clé une formation et des documents pertinents sur la sécurité.	Le personnel clé a suivi des formations en matière de sécurité et ont des connaissances suffisantes en matière de sécurité (entretien).
Moyen	Mettre en place un programme de formation, s'assurer que le personnel clé possède des informations à jour en matière de sécurité.  Organiser des formations et des séances de sensibilisation du personnel sur des sujets de sécurité importants pour votre organisation.	Le personnel a participé à des sessions de sensibilisation à la sécurité.  Programme documenté de formation sur les compétences en matière de sécurité, y compris les objectifs pour les différents rôles et comment les atteindre (par exemple, par la formation, sensibilisation, etc.).
Élevé	Réviser et mettre à jour le programme de formation périodiquement, en tenant compte des changements et des incidents passés.  Tester les connaissances en matière de sécurité du personnel.	Mise à jour de la sensibilisation à la sécurité et programme de formation  Résultats des tests de sécurité du personnel. Commentaires d'examen ou journaux des modifications pour le programme.



# Approche ILR

Autres classifications possibles:

comparaison avec secteur, autres années

liste des mesures avec niveau haut/bas



# Approche ILR


## Notification Incident

formulaire disponible site Internet ILR

première notification endéans 24 heures

analyse après l'incident

## Step

✓	Introduction
!	Contact
✓	Preliminary notification 
▶	General notification information

## General notification information

### Impact level on essential service

Description and estimated level of impact on the essential service(s)



Date and time the incident was observed\*




Estimated date and time the incident started\*




Possible impact on other essential services of another body\*




Geographic scope of the impact\*



Support requested from GovCert or CIRCL

 Yes  No

 Previous Step

NEXT STEP 

# Projet Serima

Projet ensemble avec IBPT et CASES.lu

Plateforme unique

Analyses automatisées

Gérance des opérateurs

Multiple régulations

Analyse des risques

Tout déplier / Tout replier

Rechercher un actif...

test

- IT room
- réseau coeur
  - Datacenter
  - Building (+)
  - Building (+)

Bibliothèque d'actifs

Rechercher un actif...

Fundamentals

- Equipment
- Buildings & Premises
- Datacenter
- réseau coeur

test

test test

Risques de l'information Risques opérationnels

209 risques de l'information

Seuil de risque (sur le CID max)      Mots-clés

Type de traitement

Trier: Risque MAX Sens du tri: Décroissant

Actif	Impact			Menace		Vulnérabilité				Risque actuel			Traitement	Risque résiduel
	C	I	D	Libellé	Prob.	Libellé	Mesures en place	Qualif.	C	I	D			
Building (+)	2	3	1	Forging of rights	4	No procedures for checking authorisation of personnel entering the site or premises	lower risk	2	16	24	8	Réduction	12	
IT room	2	3	1	Theft or destruction of media, documents or equipment	2	The principle of least privilege is not applied		5	20		10	Réduction	12	
Building (+)	2	3	1	Error in use	2	Unfavourable work environment (rooms too small, lack of storage areas, etc.)		3	12	18	6	Accepté	18	
IT room	2	3	1	Theft or destruction of media, documents or equipment	3	Flaws in the physical access boundaries		3	18		9	Réduction	6	

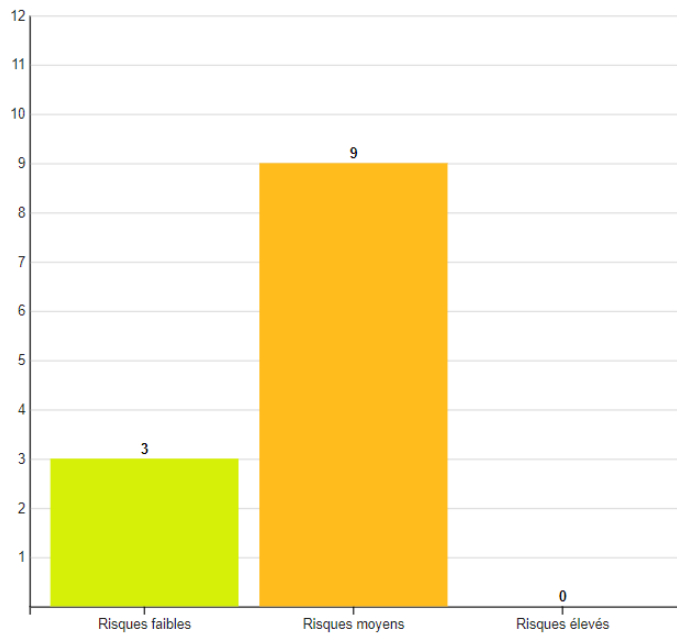
## Current risks

Display current risks by

Niveau

Chart type

Histogramme vertical



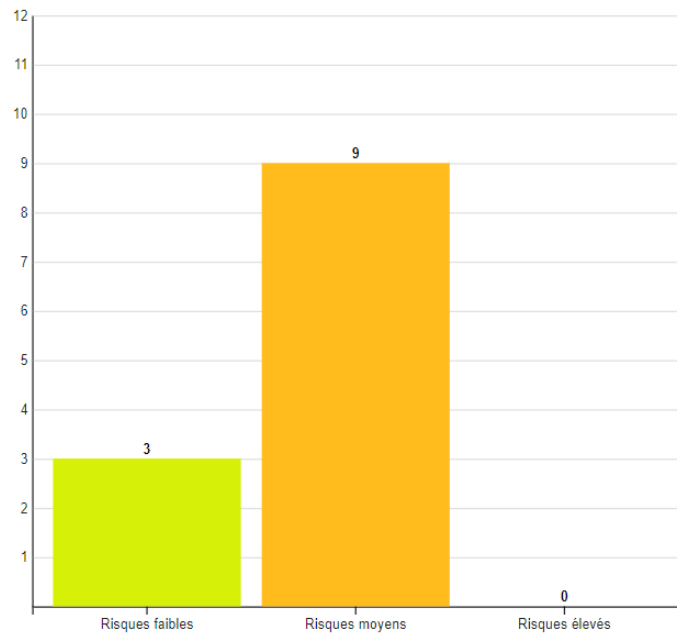
## Residual risks




























Display residual risks by

Niveau

Chart type

Histogramme vertical



Type d'actifs	Menaces	Vulnérabilités	Référentiels	Risques de l'information	Tags	Risques opérationnels	Ensemble de recommandations
NIS Directive	ISO 27002	NIST SP 800-53	NIST Core				 
Mesures 	<input type="text" value="Rechercher..."/>						Afficher tout 
<input type="checkbox"/> Code 	Libellé	Catégorie	Actions				
<input type="checkbox"/> 6.2.2	Teleworking	Organization of information security	 				
<input type="checkbox"/> 7.2.1	Management responsibilities	Human resource security	 				
<input type="checkbox"/> 9.2.1	User registration and deregistration	Access control	 				
<input type="checkbox"/> 9.2.2	User access provisioning	Access control	 				
<input type="checkbox"/> 9.2.4	Management of secret authentication information of users	Access control	 				
<input type="checkbox"/> 9.3.1	Use of secret authentication information	Access control	 				
<input type="checkbox"/> 9.4.1	Information access restriction	Access control	 				
<input type="checkbox"/> 9.4.3	Password management system	Access control	 				
<input type="checkbox"/> 11.1.1	Physical security perimeter	Physical and environmental security	 				
<input type="checkbox"/> 11.1.2	Physical entry controls	Physical and environmental security	 				
<input type="checkbox"/> 11.1.3	Securing offices, rooms and facilities	Physical and environmental security	 				



[www.monarc.lu](http://www.monarc.lu)

# Projet Serima

## Suite du développement

Dépendances

Vue globale sur l'écosystème

Notification d'incident lié à l'analyse de risque

Intégration de MISP





INSTITUT LUXEMBOURGEOIS  
DE RÉGULATION

---

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](http://www.ilr.lu)