Cybersecurity assurance in Togo
The “PPP” model

Speaker: Palakiyem ASSIH
Head of CERT.tg
CTO Cyber Defense Africa (CDA)

Summary

- Challenges in Togo for an effective cybersecurity strategy
- Public Private partnership (“PPP”)
- Cybersecurity Assurance – the national cybersecurity rules

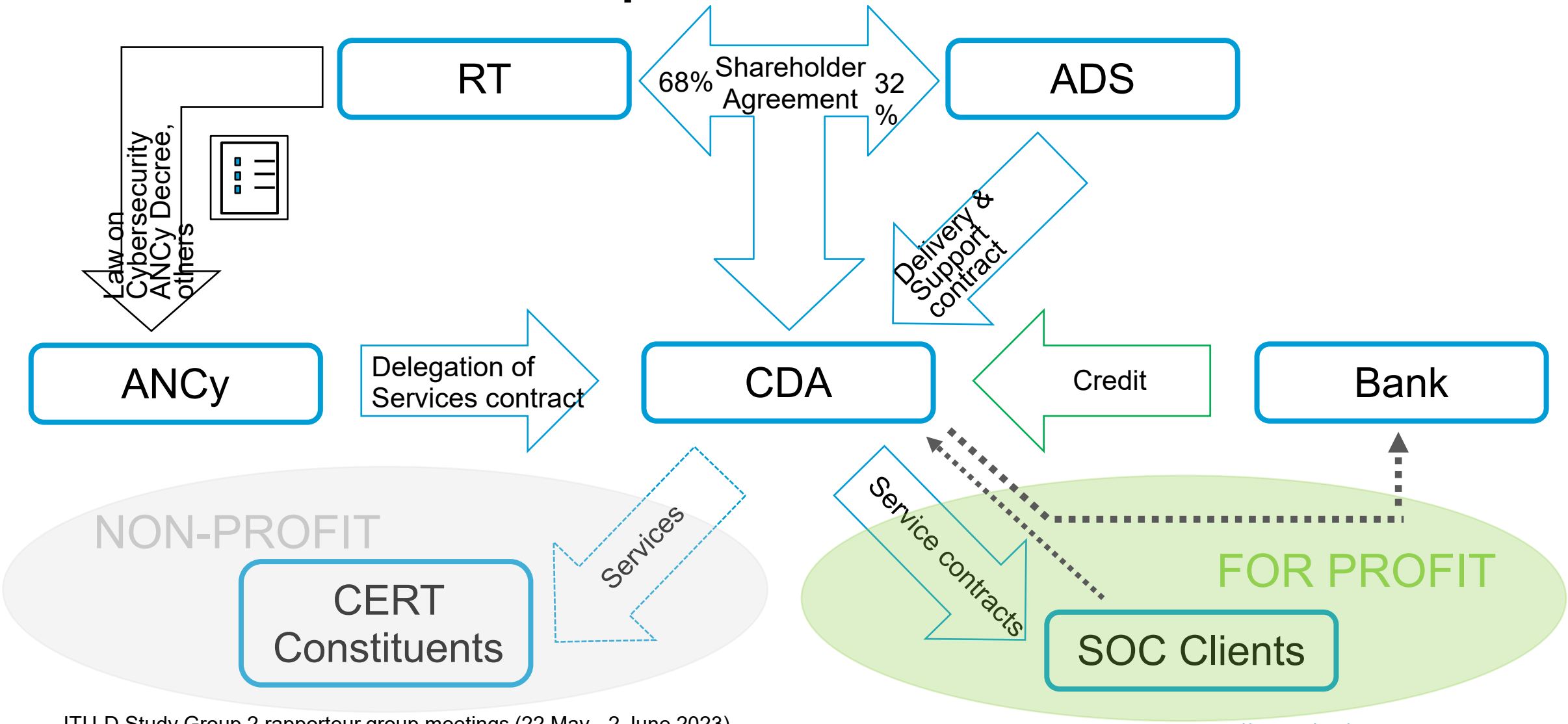
Challenges

- Togo development strategy based on digital
- Urgency to implement cybersecurity assurance for critical infrastructure, public institutions and citizens
- Limitation of fundings for the implementation of effective cybersecurity
- Limitation of human resources and technologies
- Increasingly sophisticated threats and expanding attack surface
- Lack of trust from the private sector, citizens and partners

Legal and regulatory framework

- June 2017: Law 2017-007 on electronical transactions
- December 2018: Law 2018-026 on Cybersecurity & Fight against Cybercrime
- February 2019: Decree 2019-022/PR creating National Cybersecurity Agency (ANCy)
- July 2019: Decree 2019-095/PR defining Essential Service Operators
- October 2019: Law 2019-014 on personal data protection
- **June 2022:** **Arreté N°2022-040/PMRT National Cybersecurity Rules.**

Public Private Partnership “PPP”



Cyber Defense Africa (CDA)

Public Private Partnership

Asseco Data Systems

- 1/3 of the capital
- Cybersecurity leader in Central & Eastern Europe
- 28.000+ employees
- 50+ countries
- Software & IT services
- System integrator
- Sectors : Public Administration (Civilian, Uniformed), Financial Services, Telecoms & Enterprise

Togolese Republic

- 2/3 of the capital
- Regional cybersecurity leader
- Political & security stability
- Ambitious development plan through digital & knowledge economy
- Legal & regulatory framework in place

Cybersecurity Assurance

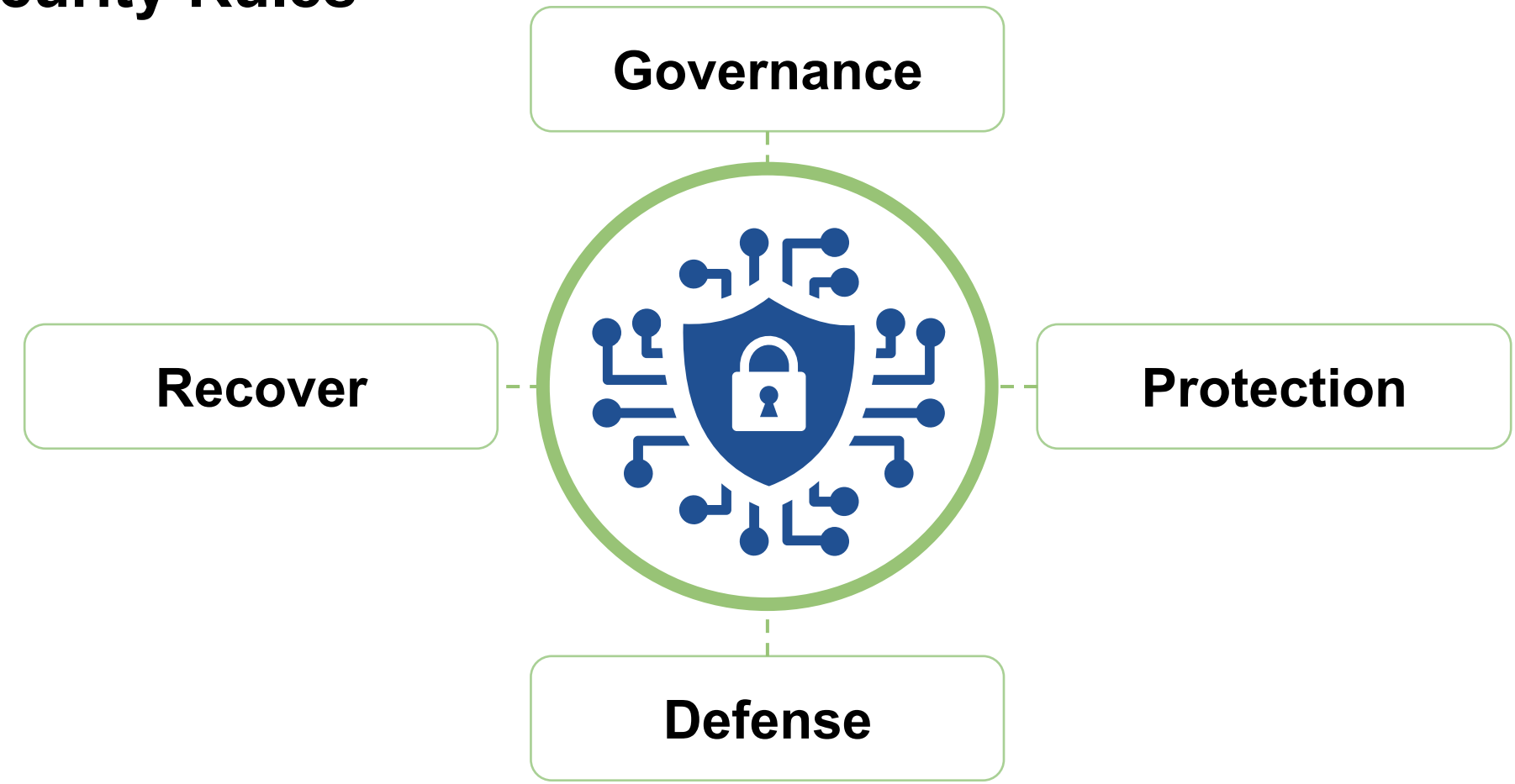
- National Cybersecurity Rules
- Signed by the Prime Minister on the 29th of June 2022
- Were provided for in article 3 and 6 of the law on cybersecurity and fight against cybercrime
- The National Cybersecurity Agency (ANCy) grants accreditations to operators of essential services who comply with the rules

National Cybersecurity Rules

- Based on industry standards and common best practices on national cyber security protections
- **ISO 270012013** – Information technology — Security techniques — Information security management systems — Requirements
- **PCI DSS** (Data Security Standards For Payment Card Industry
- **NIST 800-53 Revision 5** “Security and Privacy Controls for Federal Information Systems and Organizations »
- **CIS 20 Critical Controls**
- **SANS 20 Critical Controls**

National Cybersecurity Rules

- 4 domains
- 14 sub-domains
- 216 measures
  - Objective
  - Controls



National Cybersecurity Rules

1 Governance, Management and Leadership

- Cybersecurity Management and leadership
- Cybersecurity Strategy & policies
- Risk management
- Compliance Audit and Performance
- Human resource Security
- Supplier Relationships

2 Protection

- Access controls
- Asset Management
- Network and communications security
- Information Systems Acquisition, development and management
- Support and Operations security
- Environmental and Physical Security

3 Defense

- Security Operation Centers

4 Recover

- Business Continuity Management

National Cybersecurity Rules

Domaine	Réf.	Sous-domaine	Réf.	Contrôle	Réf	Sous-contrôles	Description	Conformité de L'OSE
Protection (P)	P2	Gestion des actifs	P2.1	Gérer les actifs	P2.1.1	Cartographie des actifs	L'OSE réalise l'inventaire des actifs pour son IE à la fois logiciel et matériel.	Conforme
					P2.1.2	Propriété des actifs	Tous les actifs doivent être attribués à un propriétaire spécifié avec des responsabilités de gestion pour chaque actif identifié.	Conforme
					P2.1.3	Utilisation acceptable des biens	L'OSE doit identifier les règles régissant l'utilisation des actifs informationnels. Ces règles doivent être identifiées, documentées et mises en œuvre.	Conforme
					P2.1.4	Restitution des actifs	L'OSE met en place un processus pour tous les utilisateurs, le personnel et les sous-traitants qui détiennent des actifs de l'OSE à retourner à la fin de leurs engagements. La restitution des ressources doit également être effectuée en cas de changement d'emploi ou lorsque l'employé cesse d'utiliser la ressource dans l'exercice de ses fonctions.	Non conforme

National Cybersecurity Rules

- Annual control carried out by CDA
  - On behalf of ANCy
- Assessment of the effectiveness and application of cybersecurity rules
- Compliance report sent to ANCy
  - Containing the findings on the measures applied
  - Recommendations
- Based on the report, ANCy decides if the ESO is compliant and can be granted the accreditation
- If not, ANCy can fine the ESO

National Cybersecurity Rules

TABLEAU DE BORD DE CONTRÔLE DES REGLES DE CYBERSECURITE DE L'OSE

CDA

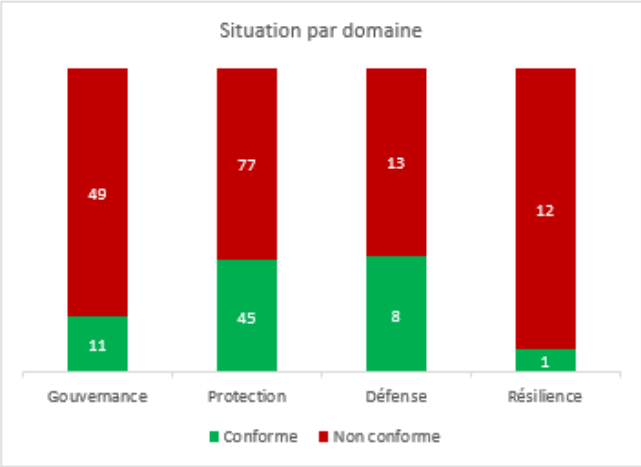
Nom de l'OSE :	OSE1
Numéro OSE :	N/A
Personne contact :	Nom RSSI
Période :	2022
Date :	22/09/2022

Evaluation finale

NON SATISFAISANT

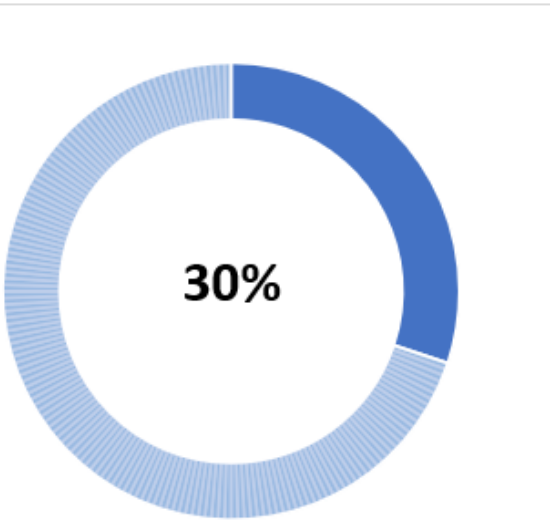
Conformité par domaine de règles de cybersécurité

Domaines	Conforme	Non Conforme	Total
Gouvernance (G)	11	49	60
Protection (P)	45	77	122
Défense (D)	8	13	21
Résilience (R)	1	12	13
TOTAL	65	151	216



Pourcentage de conformité aux règles de cybersécurité

30% CONFORME
70% NON CONFORME



Thank you !
N'labalè !
Akpé !

cda.tg
twitter.com/CDA_tg
info@cda.tg
22 53 59 83

cert.tg
twitter.com/cert_tg
contact@cert.tg
22 53 59 83