

EXECUTIVE SUMMARY

Various regulations such as EU GDPR, PCI-DSS, SOX, HIPAA and SSAE are being applied to your company or organization at the government or industry level.

RURA, which operates under strong regulation at the government level, is a regulation that is applied to companies and institutions operating public facilities in Rwanda, and according to Law N° 09/2013 of 01/03/2013, which governs RURA, it is applied as a mandatory to seven business areas as follows.

- Telecommunications, information technology, broadcasting and converging electronic technologies including the internet and any other audiovisual information and communication technology;
- 2. Postal services;
- 3. Renewable and non-renewable energy, industrial gases, pipelines and storage facilities;
- 4. Water;
- 5. Sanitation;
- 6. Transport of persons and goods; and
- 7. Other public utilities, if deemed necessary.



EXECUTIVE SUMMARY

As most government-level regulations operate in general with strong penalties, a thorough preliminary preparation is required, since a large amount of penalty will be imposed if the RURA regulation is violated.

In addition, RURA's information security regulations consist of detailed requirements that encompass not only technical security but also administrative security and physical security, therefore you have to organize and prepare an enterprise-wide T/F team.

Our consultants who have a thorough understanding of RURA regulations and have many years of experience in information security and various cases, can solve your troubles enough.

Once this project is completed, You will achieve the following goals:

- A good understanding of the information security experts for Audit Results
- Sufficient corrective action preparation and virtual simulation for Audit Results
- Implementing security document sets for managerial security required by Regulation
- Building cost effective security system for technological security required by Regulation
- Exhaustive advanced preparation for the all detailed requirements of Regulations



SERVICE STRATEGY

Our strategies to provide sufficient advanced preparation and corrective action for thorough regulatory response are as follows.

Professional Consultant T/F Team Composition

- Consists of consultants with years of experience dealing with various regulations in information security
- Consists of consultants who have a perfect understanding and experience for the regulation
- Consists of experts in the field of technical security for many years and experts in management and operational security

Rapid and Systematic Service Providing using by Pre-prepared Solution Portfolio

- Utilize pre-prepared standard templates and corrective actions for sectoral requirements such as Telecom, Broadcasting, and Information Technology
- Utilizes already prepared information security standard document set including appropriate information security policies, guidelines and procedures
- Use cost effective security solution portfolio already secured by technical security requirements of regulations



METHODOLOGY

The consulting methodology consists of 4 phases from Understanding to Certification Support. Depending on the scope of project, there are a little bit deference tasks and steps of each phase.

Requirements

- Requirement Gathering
- Project Scope Definition
- Detailed WBS Design

Assessment and Simulation

- Regulatory Audit Result Analysis
- Prioritizing Corrective Action
- Audit Result Virtual Simulation

Corrective Action Support

- Technical Security
 Implementation Support
- Administrative Security Implementation Support
- Security System Implementation Support

Final Simulation

- Final Readiness Simulation
- Wrap-up meeting

Deliverables

- Corrective Action Plan
- Phased Regulatory Compliance Virtual Simulation
- Establish Security System Required by the Regulation (optional)
- Information Security Policies and Procedures required by Regulation
- Information Security Education and Training required by Regulation



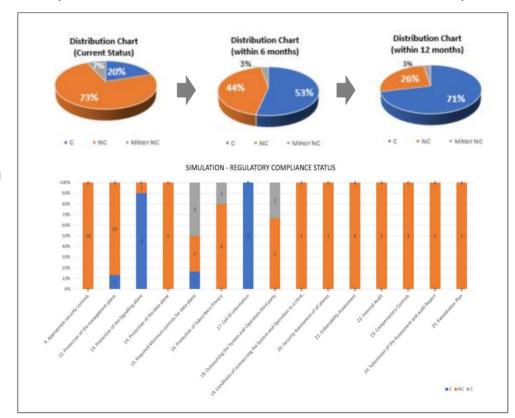
CASES-TELECOM

Simulation of Compliance Status for RURA's Telecom Network Security Requirements (15 Articles, 71 Requirements)

Prioritizing Corrective Action considering technical difficulty and budget

in the	anner.	Bill Facet (mentional desirations)	- Andrew	-	1-0-10 pt 100	Control to be Explanated	-	NAME OF TAXABLE PARTY.	Dar Ber	1 Steam
	ajtti	- The diffusion for extracts acres or extra con- crated in # folicitationers from:	1	1	-	Sufficients for between automotives should be operated stocky or new lone protected.	Feitzt	# 100 No leger	Sept 30, 2010.	Part Stated
	A1118	Theograph, and boys, Indeplication, is neclearized by some of paramet Malaysian organism cross or 275 felial and 45 MeV.	è	1	- 1	Designing will below indication in incremental in some of secure fields in impages once	Pará di	-	April 10 July	NO BLAND
- 9	ARTE	 or TE NOC (ground floor) a CDN street is closed for three it is need of an additional CDN comes between it following. is it is indicated and flooring. is it is indicated and flooring comes is not consided an out-indicate and larger come. 	3			CCTs remote discald by Enterlied . additionable to CTS halfs and P halfs.	F +14 CE	TE NOT WHEE	44 = 210	ton several
	41114	of exposment, had to be contract spaceaged. Serious and tention can raise it as a hadiso- tion door. The above to be name shown.	1			This does to site office of vigaries to to see the state of vigaries to the second of		P NOT Manager	Sec. 21, 210	ton quited
1	AMES	and to the magniferantial. "The first endpoint in a satisfaction is deligated and administrating endoughed during the Constitution under the Non-sectionary of the contribution of the co		4		f) The addinguistic concentry points tracked to the Enterpolar tracked to the Enterpolar to the EP count. g) Enterpolar that antisynature for maintain eligibilities (Local Toward Local accurated and placed to the UTL NOV IPT. cook.	m	-	401 III 2010	Tot delled
	******	The second secon		*		registers model to incommitted behavior of terry critical equipment in the second control of the properties of the properties for second control of the properties for second and properties for second and properties for second and placed to the 8 hOC out?		1	40 10 200	tio moted
rt	ARLES	Let Off when becausing added as at the suppression? - Turk the energetise (all, type—budgets) a qualitate that appropriation the energy equipment is encounted because its protection of profits. - It the John Look, the energy story is not profit to the John Look, the energy story.				to Advance your or strepping against final to enterestible behavior of may miss operate in the most cost of 38 Octor in Bulleton for natingation for mortist approximations, midd to promised and plained in the 38 Decem-	1,00	-	April 20, 2018	hor hones
10.	ANGE MILIT	 Consistion we discounter only A. VI. 21 year and to day 8 for a year employer X is transposed. View heat to be an appropriate in a transposed or transposed to the an appropriate product of the appropriate produc	A	4		Section and discount of offernation exists policy had do no descripted.	*	S Steele	96-5 (C.205)	OneW and by least or health.
	01538 01538	There is no only alread how assessment or against discard to a common officeal assessment of the common of th				e must be defined the policy for ther field policy proved quality and physical approximation	r	filmes	March 21: 2016	Code original
,	PE13.	Manager on it information bounds from the Districted officeration between Different is not empress.	×			CSC trust be properly) recognition that	armi.	(00)	100×10 30 30 10	feet the free
	4613	A fig. increasing contact points of authorities in tool part mentioped This last is perturbed, numbers of what or product illustrate prints	2			a file receiving contact party of particular trials for written and tage	2000VIII	the Manager	900 N 200	Test should
	46)1	graph of other banded search fromte and probabilities that be related and probabilities displayed the related - The burnes displayed shaked and your denter it as STS decline table helpston	Œ		1	FIG. COMMENT, Secretary Secretary Secretary and COST force for policies, but Justice of the developed association likes 6000 to sectority sectors.	chec	ene.	hip 14, 2010	tor assess

Step-by-step Regulatory Compliance Virtual Simulation (Current Status > within 6 months > within 12 months)





CASES-TELECOM

RURA regulatory requirements are largely divided into three categories, and service portfolios are provided according to requirements.

Article 9: Appropriate security controls Article 12: Protection of the management plane Article 13: Protection of the Signaling plane Article 14: Protection of the data plane Article 15 :Required Minimum controls for data plane Article 16: Protection of Subscribers Privacy Article 17 :Call ID information Article 18: Outsourcing the System and Operation third party Article 19: Conditions of outsourcing the System and Operation to a third party Article 20 :Security Assessment of all planes Article 21 :Vulnerability Assessment Article 22 :Internal Audit Article 23: Compensatory Controls Article 24 :Submission of the Assessment and audit Report Article 25 :Remediation Plan REGULATIONS Nº 001/R/TD-ICS/RURA/016 OF 06/05/2016 GOVERNING TELECOM NETWORK SECURITY IN RWANDA ADOPTED BY THE REGULATORY BOARD RWANDA UTILITIES REGULATORY AUTHORITY (RURA)

Information Security Policies

In Article 12, 19, 31;

- General Part Security Policies and Procedures
- Network Security Part Polices and Procedures
- Server Security Part Policies and Procedures
- Application Security Part Policies and Procedures
- and others

Establish Security System

- Network Layer: SIEM, Firewall, IPS/IDS, AAA system, Log Management, VPN, DDoS, NAC, etc.
- Server Layer: PMS, VPN, Spam Filter, Antimalware, anti-APT, etc.
- Application/Data: WAF, DLP, DBMS Firewall, Secure USB, DRM, SSO/EAM, HSM, OTP, etc.
- PC Layer: Anti-virus, etc

Education and Training

- Education for Security Vulnerability Test and Penetration Test
- Security Test Training for DRP, DDoS,
- Awareness education for general users

