KINDNS

KINDNS

A Framework to Improve Secured DNS Operations

Aug. 2023

Yazid AKANHO
ICANN’s Office of the CTO
Yazid.Akanho@icann.org

Agenda

1. KINDNS presentation
2. Demo
3. Q/R session

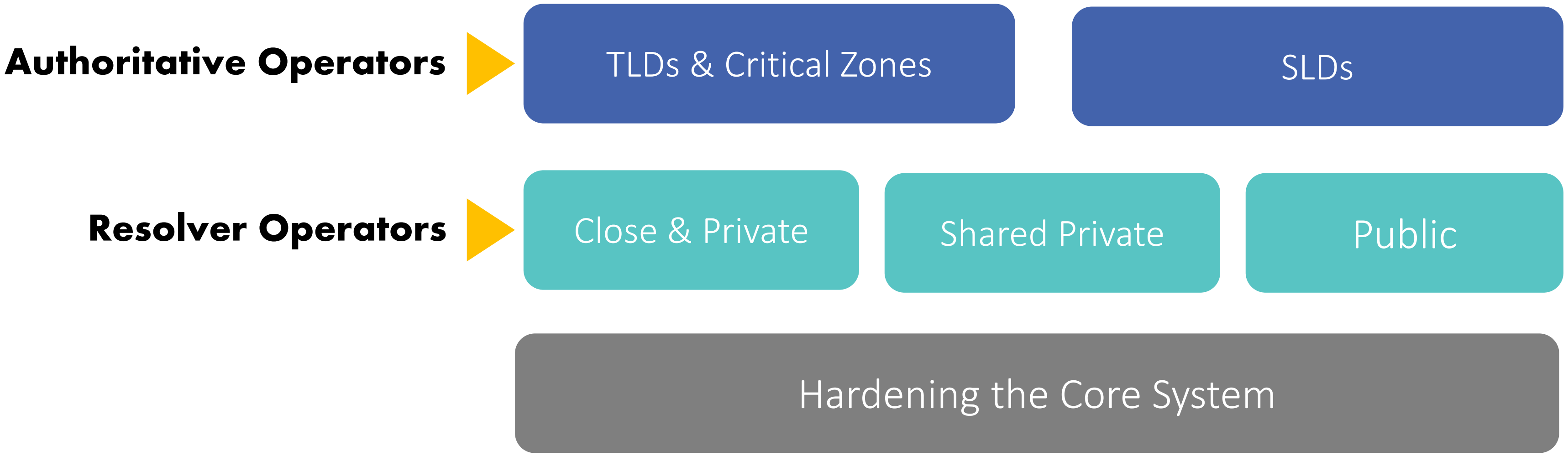
What Is It?

Knowledge-sharing and **I**nstantiating **N**orms for **D**NS
(Domain Name System) and **N**aming **S**ecurity

*A simple framework that can **help a wide variety of DNS operators**, from small to large, to follow both the **evolution of the DNS** protocol and the best practices that the industry identifies for better security and more effective DNS operations.*

*..... is pronounced "**kindness**"*

Targeted Operators



Authoritative Operators

TLDs & Critical Zones

SLDs

Resolver Operators

Close & Private

Shared Private

Public

Hardening the Core System

Each category has 6-8 practices that we encourage operators to implement.
See www.kindns.org, for more details.

Authoritative DNS Operators of Critical Zones

TLDs & Critical Zones

1. MUST be DNS Security Extensions (DNSSEC) signed and follow key management best practices.

2. Transfer between authoritative servers **MUST** be limited

3. Zone file integrity **MUST** be controlled

4. Authoritative and recursive nameservers **MUST run on separate infrastructure**

5. A minimum of two distinct nameservers **MUST** be used for any given zone

6. There **MUST** be diversity in the operational infrastructure: **Network, Geographical, Software**

7. The infrastructure that makes up your DNS infrastructure **MUST** be monitored

Authoritative DNS Operators of SLDs

SLDs

1. MUST be DNSSEC signed and follow key management best practices

2. Transfer between authoritative servers **MUST** be limited

3. Zone file integrity **MUST** be controlled

4. Authoritative and recursive nameservers **MUST run on separate infrastructure**

5. A minimum of two distinct nameservers **MUST** be used for any given zone

6. Authoritative servers for a given zone **MUST** run from diversified infrastructure

7. The infrastructure that makes up your DNS infrastructure **MUST** be monitored

Closed & Private Resolver Operators

Private resolvers are not publicly accessible and cannot be reached over the open internet. They are typically found in corporate networks or other restricted-access networks

Closed & Private resolvers

1. DNSSEC validation **MUST** be enabled

2. Access control list **(**ACL) statements **MUST** be used to restrict who may send recursive queries

3. QNAME minimization **MUST** be enabled

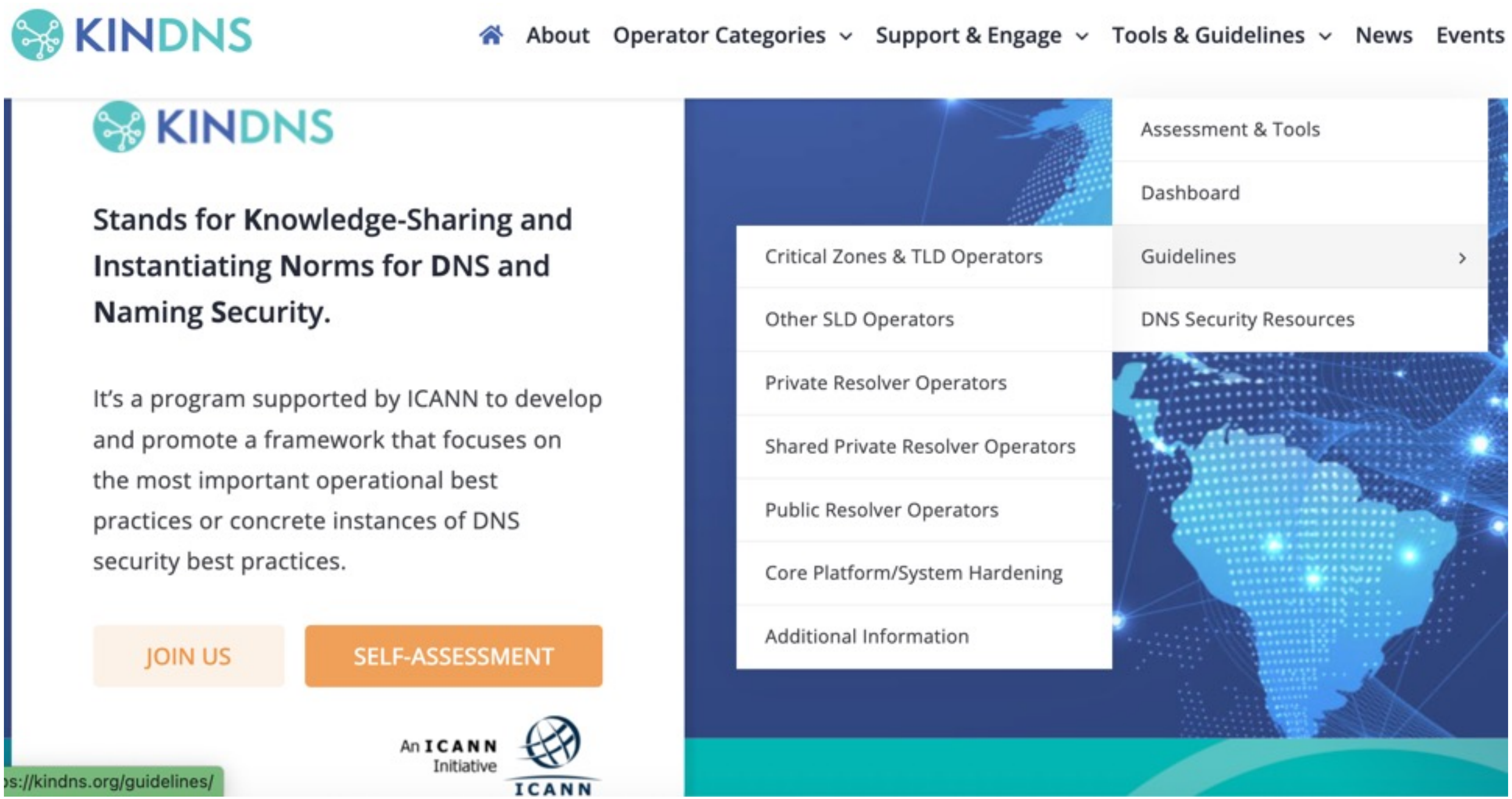
4. Authoritative and recursive nameservers **MUST** run on separate infrastructure

5. At least two distinct servers **MUST** be used for providing recursion services

6. Authoritative servers for a given zone **MUST** run from a diversified Infrastructure

7. The infrastructure that makes up your DNS infrastructure **MUST** be monitored

All practices are well documented there!



Stands for Knowledge-Sharing and Instantiating Norms for DNS and Naming Security.

It's a program supported by ICANN to develop and promote a framework that focuses on the most important operational best practices or concrete instances of DNS security best practices.

Self-assessment & Enrollment

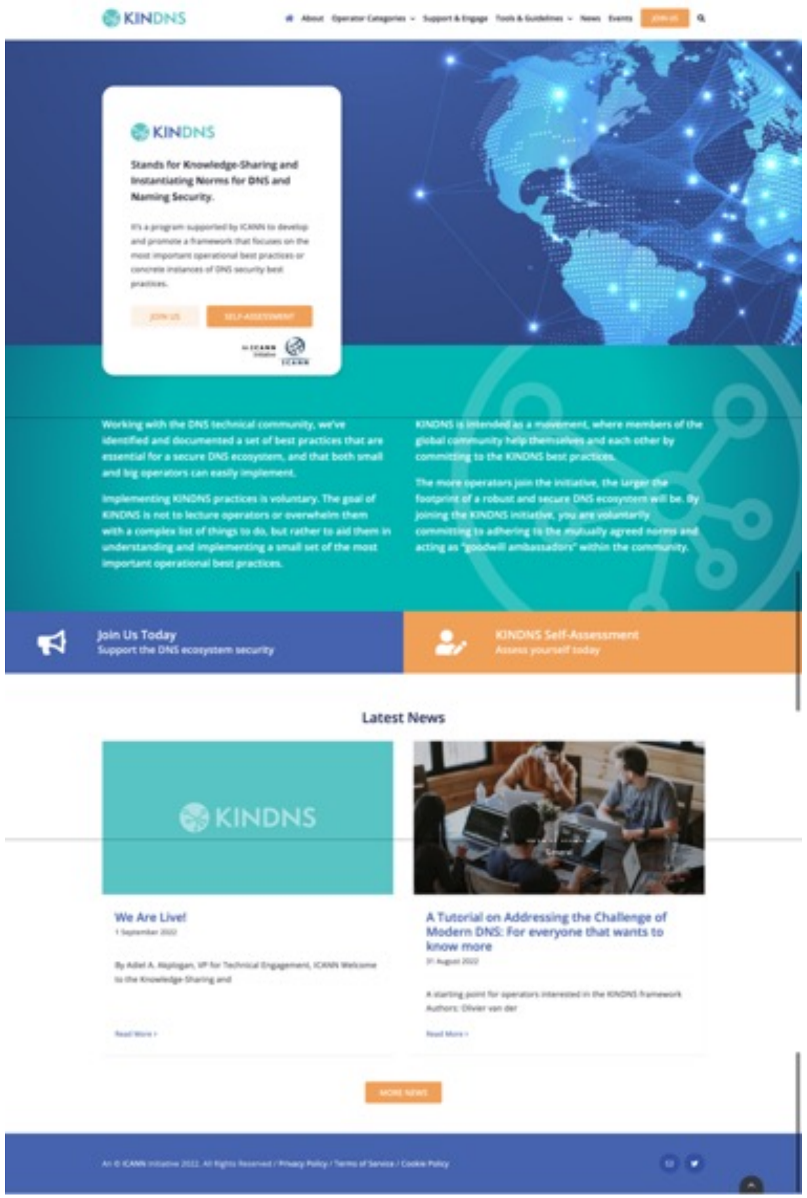
Operators in each category can self-assess their operational practices against KINDNS and use the report to correct/adjust unaligned practices.

- self-assessment is anonymous
- reports can be downloaded directly from the web site.

Operators can enroll as participant to one or many categories covered by KINDNS.

- Participation in the KINDNS initiative means voluntarily committing to implement/adhere to agreed practices.
- Participants become goodwill ambassadors and promote best practices.

Website – https://kindns.org/



KINDNS

Stands for Knowledge-Sharing and Instantiating Norms for DNS and Naming Security.

It's a program supported by ICANN to develop and promote a framework that focuses on the most important operational best practices or concrete instances of DNS security best practices.

Working with the DNS technical community, we've identified and documented a set of best practices that are essential for a secure DNS ecosystem, and that both small and big operators can easily implement.

Implementing KINDNS practices is voluntary. The goal of KINDNS is not to lecture operators or overwhelm them with a complex list of things to do, but rather to aid them in understanding and implementing a small set of the most important operational best practices.

KINDNS is intended as a movement, where members of the global community help themselves and each other by committing to the KINDNS best practices.

The more operators join the initiative, the larger the footprint of a robust and secure DNS ecosystem will be. By joining the KINDNS initiative, you are voluntarily committing to adhering to the mutually agreed norms and acting as "goodwill ambassadors" within the community.

Join Us Today
Support the DNS ecosystem security

KINDNS Self-Assessment
Assess yourself today

Latest News

We Are Live!
1 September 2022

By Adiel A. Akplogan, VP for Technical Engagement, ICANN Welcome to the Knowledge-Sharing and

A Tutorial on Addressing the Challenge of Modern DNS: For everyone that wants to know more
31 August 2022

A starting point for operators interested in the KINDNS framework Authors: Olivier van der

An © ICANN Initiative 2022. All Rights Reserved / Privacy Policy / Terms of Service / Cookie Policy

Self-Assessment Report

Self-Assessment Report

KINDNS

Completed on this 09 May 2022

KINDNS

Instantiating Norms for DNS and Naming Security) is
that focuses on the most important operational best
DNS security best practices.

Recursive Resolver Category. The first step in
rvice is determining how your server is being

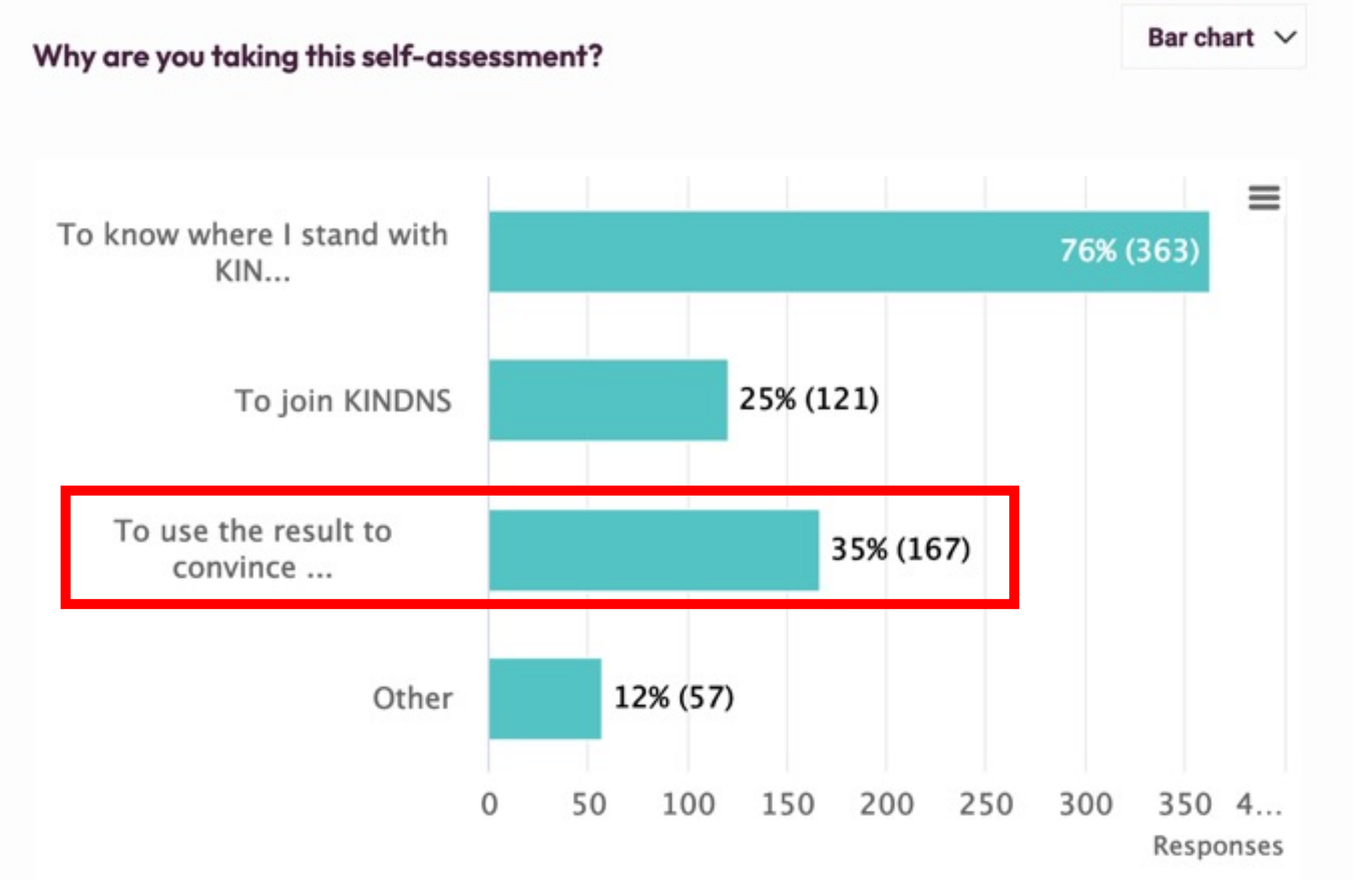
rivate?
er the open internet (public IP address, not

over the open internet (private IP address, or
ation)
d?
onds to, queries from any client
n of some sort to be used (for example, IP
e [DoT])

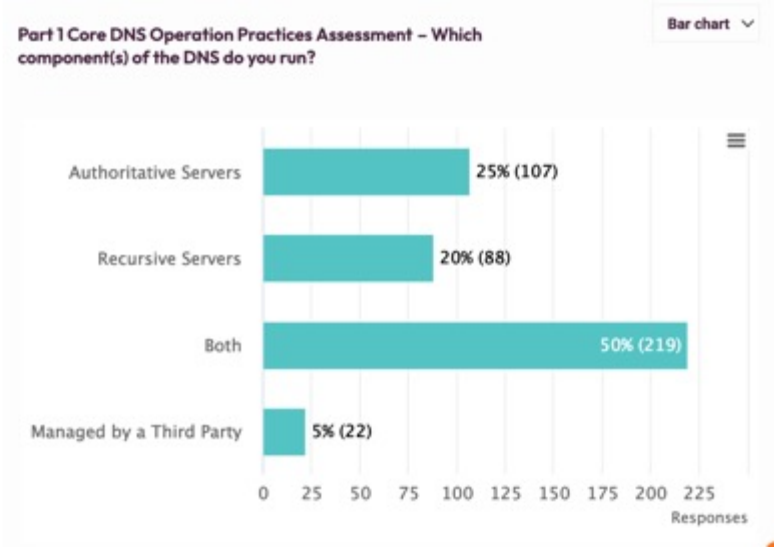
s practice, you may be operating one or
s and implementation guidelines for
es, reflecting the types of resolver

KINDNS

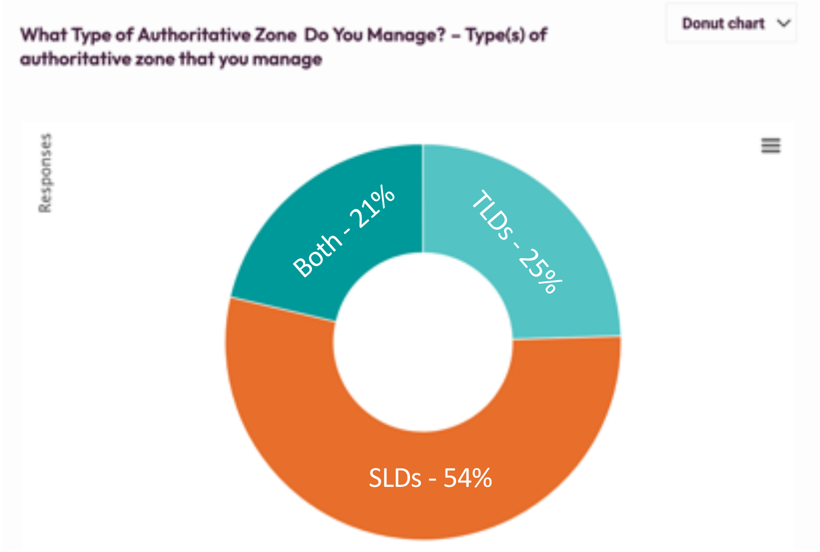
Early Observations



Why are you taking this self-assessment?

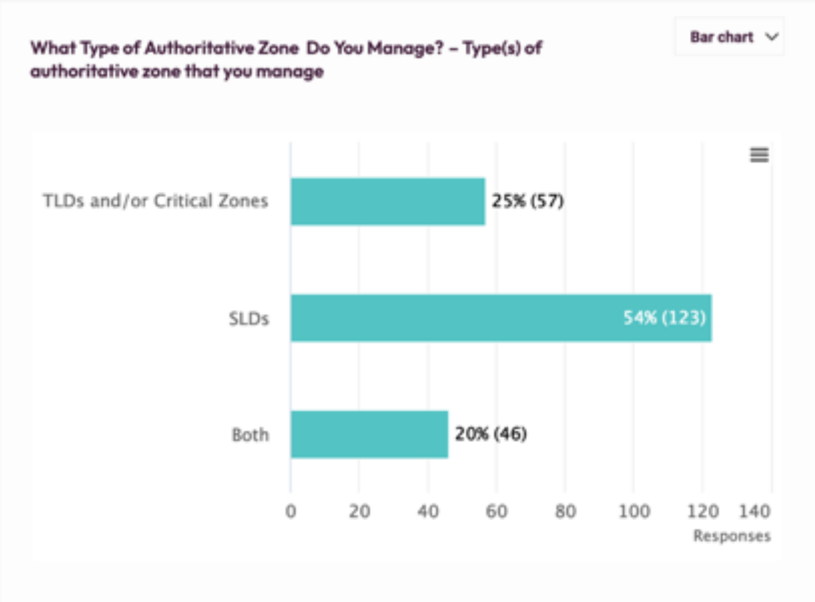


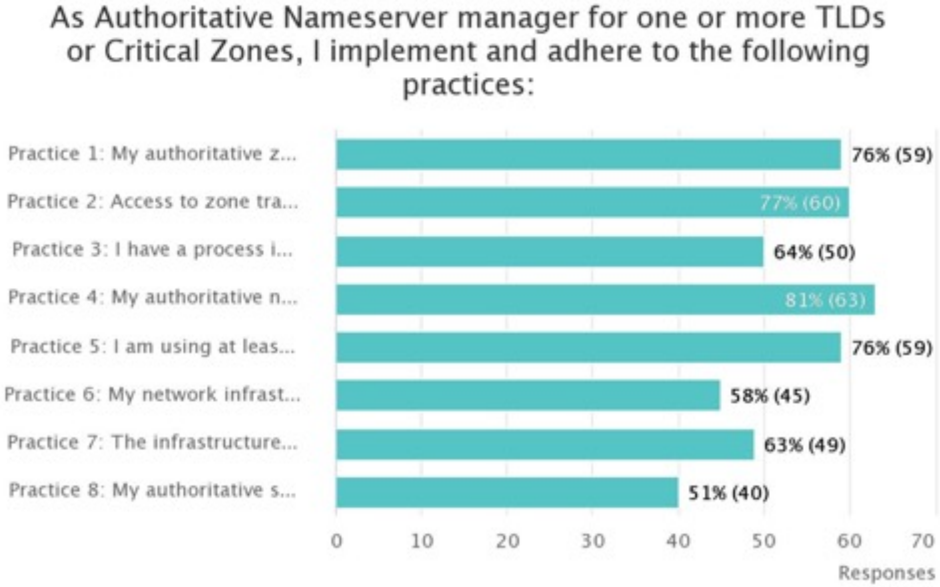
Part 1 Core DNS Operation Practices Assessment – Which component(s) of the DNS do you run?

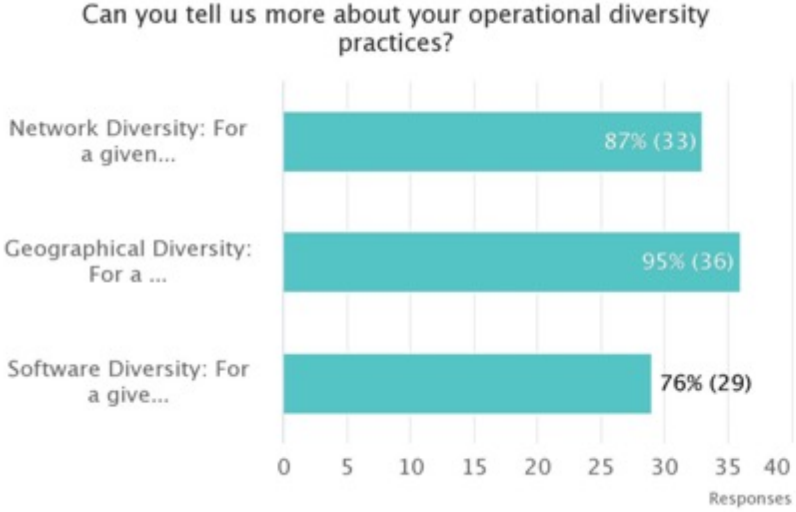


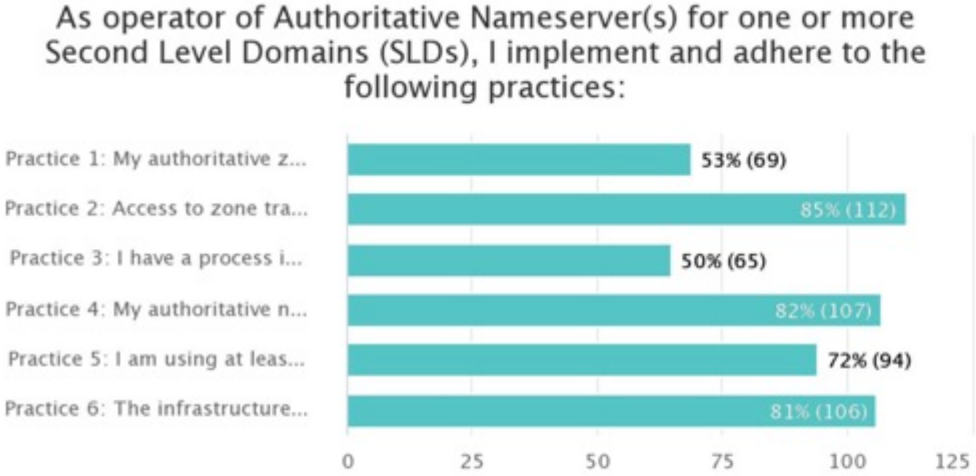
What Type of Authoritative Zone Do You Manage? – Type(s) of authoritative zone that you manage

Early Observations (con't)


What Type of Authoritative Zone Do You Manage? – Type(s) of authoritative zone that you manage


As Authoritative Nameserver manager for one or more TLDs or Critical Zones, I implement and adhere to the following practices:


Can you tell us more about your operational diversity practices?


As operator of Authoritative Nameserver(s) for one or more Second Level Domains (SLDs), I implement and adhere to the following practices:

KINDNS

Selecting BCPs

How do we identify them ?

- Draw from own operational experience
- Ask operators (NOG lists, communities)
- Review RFCs and other standards https://powerdns.org/dns-camel/
- Shortlist based on relevance, ease of implementation, and how widespread the adoption is

Ask operators to review the selection (kindns-discuss)

Debate and justify choices

Engaging the community

Operators must agree on the selected BCPs

kindns-discuss list launched in 2021

- Encouraged operators from all backgrounds to join
- When in doubt, we asked community for advice on what they consider to be a BCP or not
- Some things were debated – is DNSSEC validation a **MUST** nowadays ? (We think so ☺)
- Some practices weren't implemented widely enough, or too complicated (not low hanging fruit) for small operators
  - e.g. Anycast

Current Focus: Phase 2

Service Platform Hardening

Front-end

- Re-Activate the full **enrollment form**
- **Translate** the website and the tools into other languages
- **Evolve the Self-assessment** tool to technically measure/assess how operators implement the practices.
  - Two views: Internal & External
  - Ability to measure implementation by collecting anonymized data from the self-assessment tool.
  - Integrate a Zonemaster version for Authoritative servers

Back-end

- *Integrate the KINDNS server to ICANN E&I monitoring service*
- *Implement a ticketing system to better track interactions with the public.*
- *Improve the security fence around WordPress*
- *Deploy an integrated enrollment management tool (a WP plugin)*
- *Renew ICANN infosec assessment.*
- *Directly link self-assessment to enrollment*
- *Develop an integrated tool to simplify/automate Operator compliance assessment*

Current Focus: Phase 2 (con't)

Community Engagement

- **Community engagement**: continue to encourage operators to get onboard to **contribute and support** the framework:
  - *Direct 1:1 Engagements*
  - *Convince/Encourage more DNS operators to join*
  - *Workshops & webinars to raise awareness on KINDNS practices as part of our overall DNS ecosystem security awareness program.*
  - DNSAthons around secure DNS operations
  - Develop partnerships with programs such as MANRS and Pulse, internet.nl, etc.

- **Communication**: a more active communication plan to further promote KINDNS
  - Publish a series of DNS best practices dedicated blogs
  - Develop toolkits to help operators engage with internal decision-makers.

KINDNS v.2 - Discussion Points

1. **Adding Response Rate Limiting (RRL)** to Authoritative Servers' practice
   - ccTLD and critical Zone Operators
   - Other SLDs too?

2. **Addressing 'Split' responsibilities** for Authoritative servers' operation:
   - Zone file content is controlled by a third party. i.e root server operators and the root zone itself.

3. **Access reliability:** Reachability over IPv6, RPKI for the prefix used for the DNS servers.

4. **Community review team**: volunteers from the community to work with staff to help with assessing participating candidates or other aspect of KINDNS practice evolution.

5. **Metrics**: help measure the impact of KINDNS adoption on global DNS operations

Some external additional tools

1. **Zonemaster**: https://zonemaster.net/

   A program that tests a DNS zone configuration with different sanity checks configured in an engine and provides a zone health report.

2. **DNSviz**: https://dnsviz.net/

   Provides a visual analysis of the DNSSEC authentication chain for a domain name and its resolution path in the DNS namespace, and lists configuration errors detected by the tool.

3. **SuperTool**: https://mxtoolbox.com/SuperTool.aspx

   An integrated tool that can perform several kind of diagnostics on a domain name, IP address or host name. Documentation available at https://mxtoolbox.com/restapi.aspx

4. **Intodns**: https://intodns.com/

   Checks the health and configuration and provides DNS report and mail servers report.

Stay Informed and Contribute

Website	www.kindns.org
Twitter	https://twitter.com/4KINDNS
E-Mail	info@kindns.org
Mailing list	kindns-discuss@icann.org https://mm.icann.org/mailman/listinfo/kindns-discuss

Engage with ICANN

Thank You and Questions

Visit us at **icann.org**
Email: kindns-info@icann.org

- @icann
- facebook.com/icannorg
- youtube.com/icannnews
- flickr.com/icann
- linkedin/company/icann
- soundcloud/icann
- instagram.com/icannorg

To be KIND with DNS
An AFRINIC journey

Cedrick Adrien Mbeyet

cedrick.mbeyet@afrinic.net

DNS … a critical infrastructure

What is a Critical infrastructure?

- Not only hardware (ISP Backbone, transmission lines, routing equipment, etc.)

- But also Software services (DNS, Email, DB, Web hosting, etc.)

- Any interruption for a significant period of time will seriously impact Internet

Why is DNS a critical infrastructure?

- Without DNS,
  - No name resolution
  - Have to remember the full IP address
  - Hard to make multiple site coexist
  - Lots of spam will found their way

DNS @ AFRINIC

Reverse DNS

- Support the functioning of the ARPA Zone (in-addr.arpa and ip6.arpa) roles that the RIRs and IANA perform

- AFRINIC operate c.ip6-servers.arpa and c.in-addr-servers.arpa

- Run under **AS37181**

Africa Domain Secondary Program

- AfDSP runs under **AS 37177**
- Offer a secondary to TLDs (1st and 2nd)
  - Around 40 ccTLD
  - For 27 countries in Africa
- Separate ASN to not create confusion with operator filters

AfRSCP
Africa Root Server Copy Program

- Support the installation of DNS Root servers within Africa region
  - Hardware
  - Admin / contact
- Root operators we work with D, E, F, K, L and very soon M
- Increase DNS resilience in the region

AFRINIC Anycast program

- NS2 (reverse DNS) and CIP (ccTLD)
- We have nodes inside and outside our region
- Both virtual and physical
- Currently we operate from 8 addiitional locations
  - Physical: Tunisia, Rwanda
  - Virtual: Tanzania, Madagascar, Poland, SA (JNB, CPT, Durban)

Our journey to a more resilient DNS infrstructure…

10 years ago…

AfriNIC
The Internet Numbers Registry for Africa

2 datacenter collocation (1 active and 1 DR)

3 physical anycast node

1 virtual location

Up to 10h downtime over the year

Today…

Join the Africa dns Support Programme

AFRINIC

4 datacenter collocation (all active)

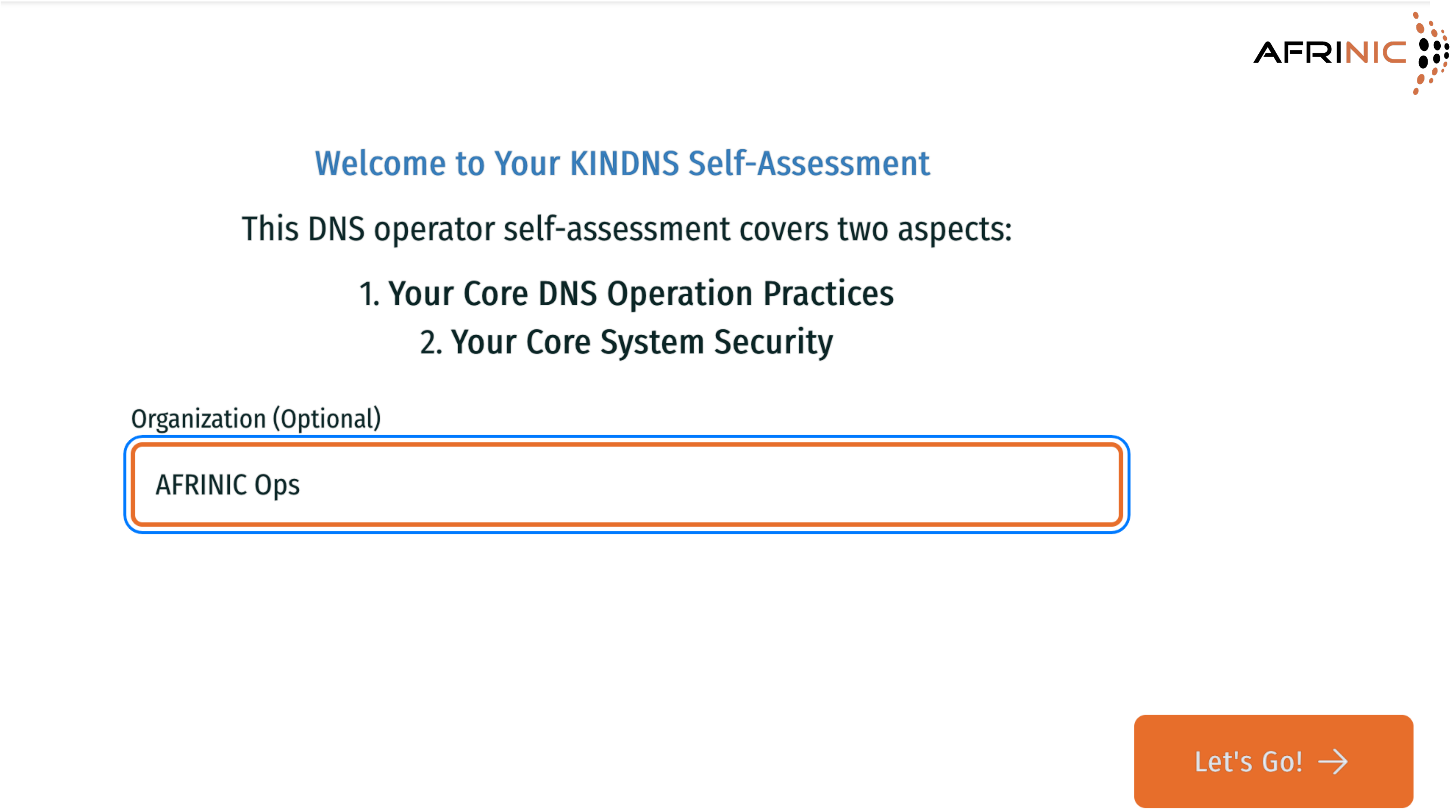
3 physical anycast node

5 virtual location (and counting)

At least 2 virtual nodes per location

99.99% uptime in 2022

KINDNS self assesment



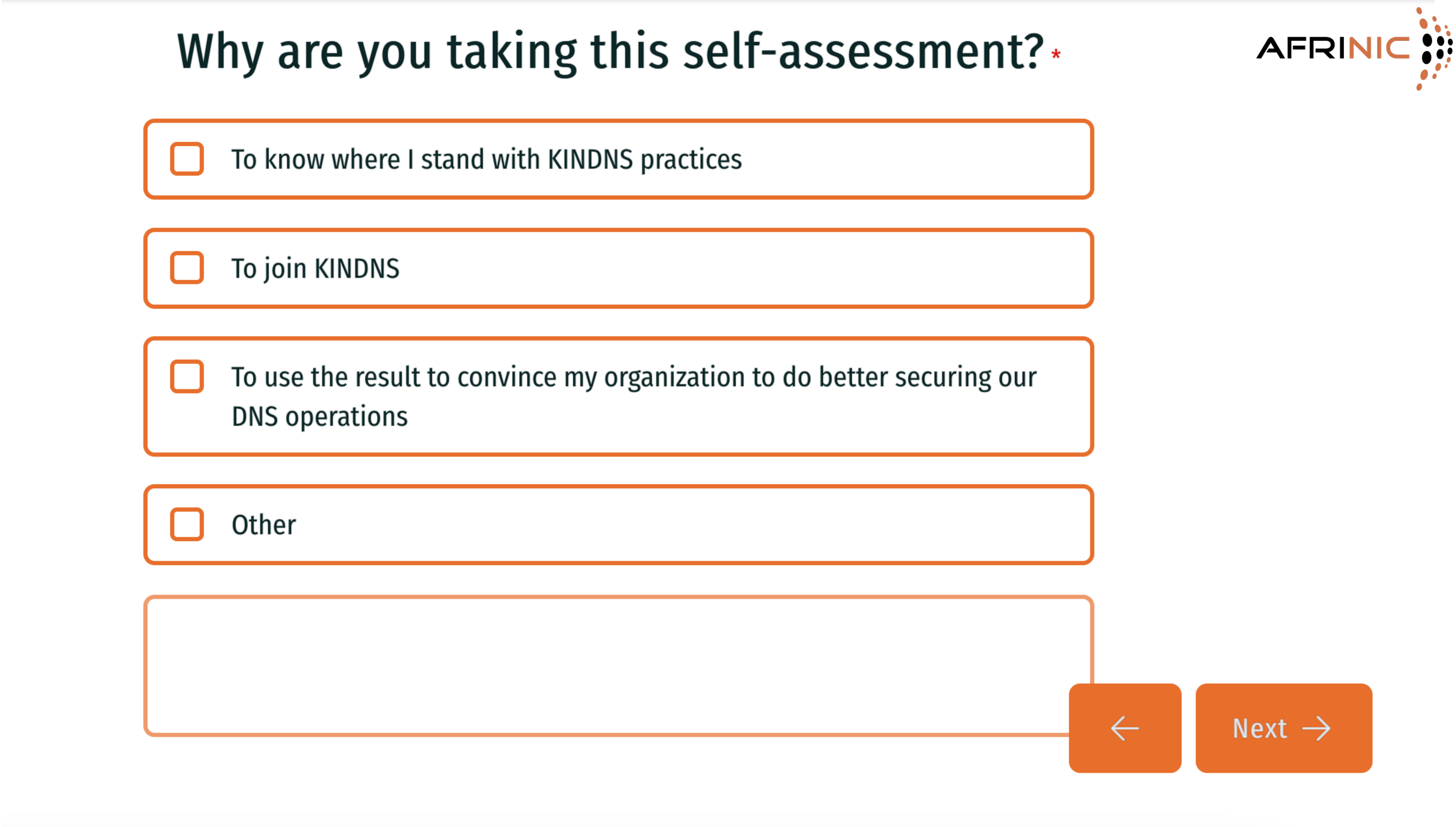
Welcome to Your KINDNS Self-Assessment

This DNS operator self-assessment covers two aspects:

1. Your Core DNS Operation Practices
2. Your Core System Security

Organization (Optional)

AFRINIC Ops



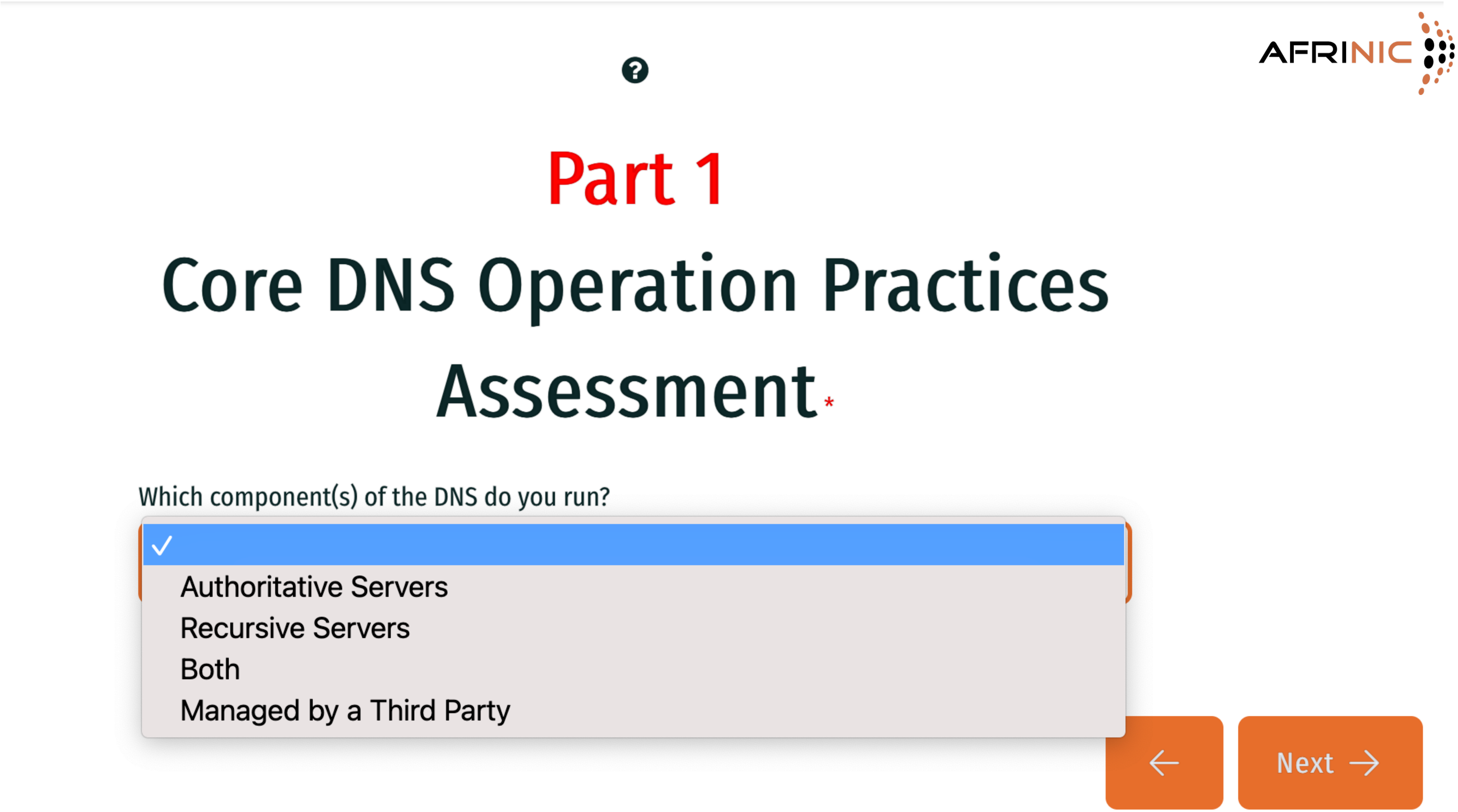
Why are you taking this self-assessment? *

□ To know where I stand with KINDNS practices

□ To join KINDNS

□ To use the result to convince my organization to do better securing our DNS operations

□ Other

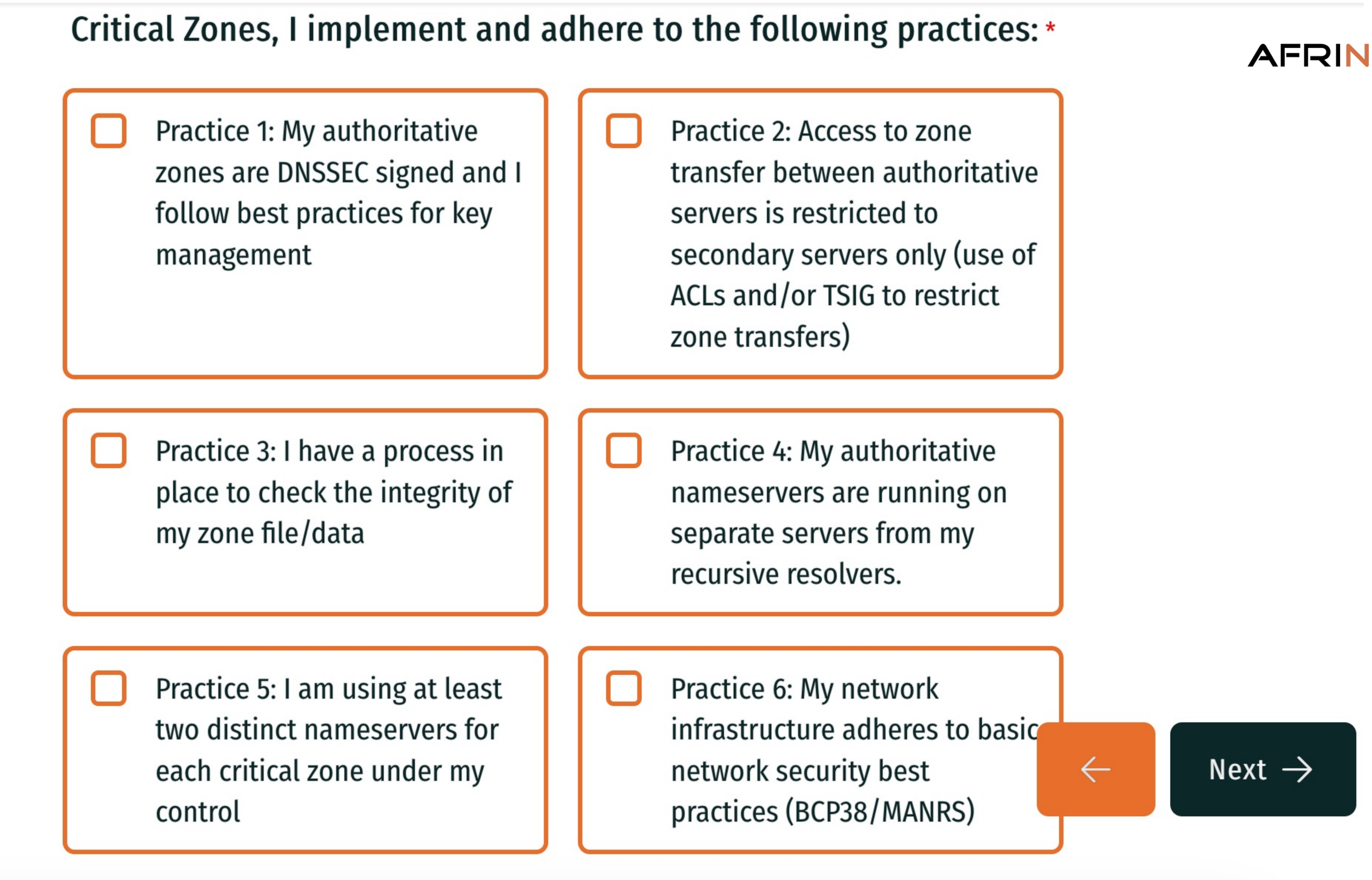


Part 1

Core DNS Operation Practices Assessment*

Which component(s) of the DNS do you run?

AFRINIC



Critical Zones, I implement and adhere to the following practices: *

□ Practice 1: My authoritative zones are DNSSEC signed and I follow best practices for key management

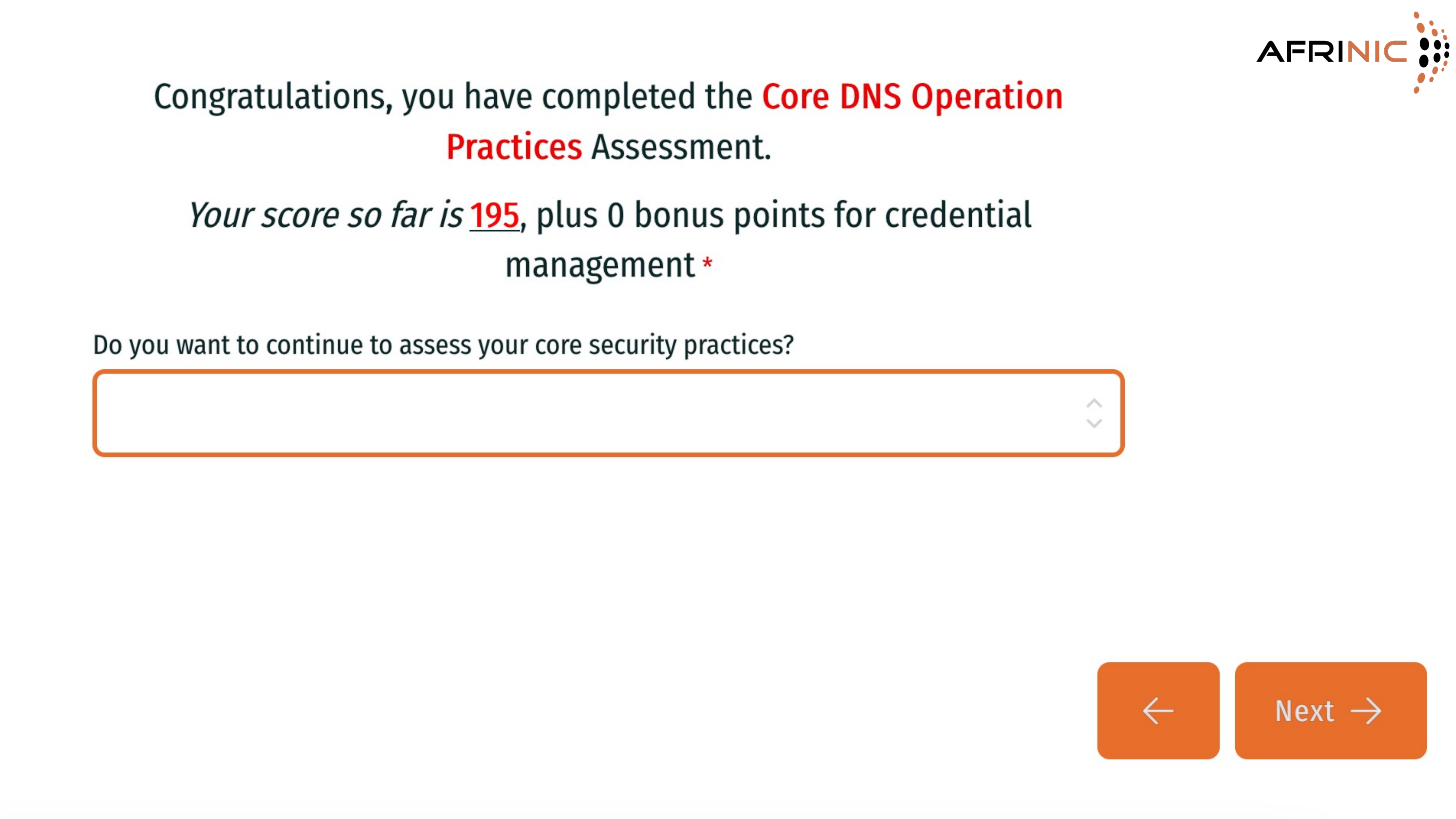
□ Practice 2: Access to zone transfer between authoritative servers is restricted to secondary servers only (use of ACLs and/or TSIG to restrict zone transfers)

□ Practice 3: I have a process in place to check the integrity of my zone file/data

□ Practice 4: My authoritative nameservers are running on separate servers from my recursive resolvers.

□ Practice 5: I am using at least two distinct nameservers for each critical zone under my control

□ Practice 6: My network infrastructure adheres to basic network security best practices (BCP38/MANRS)



Congratulations, you have completed the **Core DNS Operation Practices** Assessment.

Your score so far is 195, plus 0 bonus points for credential management *

Do you want to continue to assess your core security practices?

Part 2

Core System Security Practices

In addition to implementing best practices for DNS security, availability and resilience, as operators you must also pay careful attention to practices that help harden the platforms that host your DNS. There are three types of hardening practices that we are focusing on: network security, host security, and customers-facing portal and services security. On following screens, and for each of the hardening categories, please select the statements that match your operational practices.

← Next →

Network Security: *These best practices are aimed at preventing unauthorized network access to your DNS servers and ensuring your internal traffic does not leak onto other networks.*

Please select the statements that match your operational practices.

□ Practice 1: ACLs are implemented to restrict network traffic to your DNS servers (Authoritative or Resolver)

□ Practice 2: BCP38/MANRS egress filtering is implemented so that no network traffic can leave your network with a source IP address that is not assigned to you or your customers.

← Next →

Host and Service Security: *These practices are aimed at improving the security of the hosts running DNS services in order to reduce the likelihood of a host compromise, denial of service attack, or other attack.*

Please select the statements that match your operational practices.

□ Practice 3: The configuration of each of my DNS servers is locked down

□ Practice 4: User permissions and application access to my system resources are limited. File permissions and ownership restrictions are set so that users and services not directly associated with management of the DNS subsystem do not have read or write access to DNS service configuration, data files, and database subsystems.

□ Practice 5: System and service configuration files are versioned. For authoritative operators, zone files/data are also versioned.

← Next →

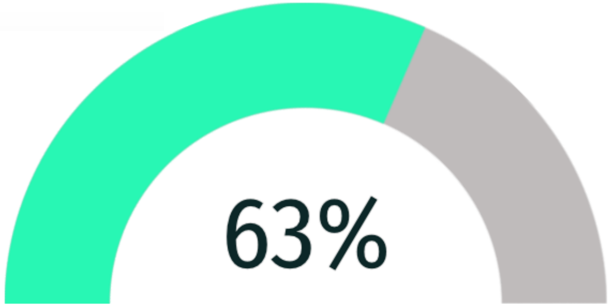
Thank you for completing the KINDNS assessment.

Your score for Authoritative (TLD+SLD) and Resolver Operator practices is 195 / 300

Your score for the Core System Security assessment is 60 / 100

You do not have bonus points for Credential Management. *Please pay attention to your credential management practices.*

Your Total Score for this assessment is 255 / 400



Downlo

Take the Sel

Thank You For Your Support and Attention.

Should you have any question in this regard,
please feel free to contact us

AFRINIC Ltd
11th Floor Standard Chartered Tower
19 Cybercity, Ebene | Mauritius
www.afrinic.net

AFRINIC Stakeholder Development Department
engagement@afrinic.net

t: +230 403 5100 | f:+230 466 6758