ICANN 58
COMMUNITY FORUM

COPENHAGEN
11–16 March 2017

ICANN

Towards Effective DNS Abuse Mitigation

GAC PSWG | ICANN 58 | 13 March 2017

Goals and Expected Outcomes of this Session

1 Discuss current trends and industry response to abuse of the DNS

2 Discuss ICANN's capabilities and practices

3 Identify steps towards an effective community response

Discussion Moderated by:

Cathrin Bauer-Bulst, GAC PSWG Co-Chair
Deputy Head of Unit, Fight Against Cybercrime
DG HOME, European Commission

Robert Flaim, GAC PSWG Member
Executive Office Liaison, Science and Technology Branch Executive Office
Federal Bureau of Investigation, United States

Agenda & Speakers

1. Introduction
2. Trends in Abuse and the Need for Mitigation
   - Presentation by Greg Aaron (APWG)
   - Q&A
3. Illustration of Possible Industry Response
   - Craig Schwartz (.BANK, .INSURANCE, Verified TLDs Consortium)
   - Q&A
4. Focus on ICANN's contribution
   - David Conrad (ICANN CTO)
   - Maguy Serad (ICANN Contractual Compliance)
   - Q&A
5. Closing Remarks

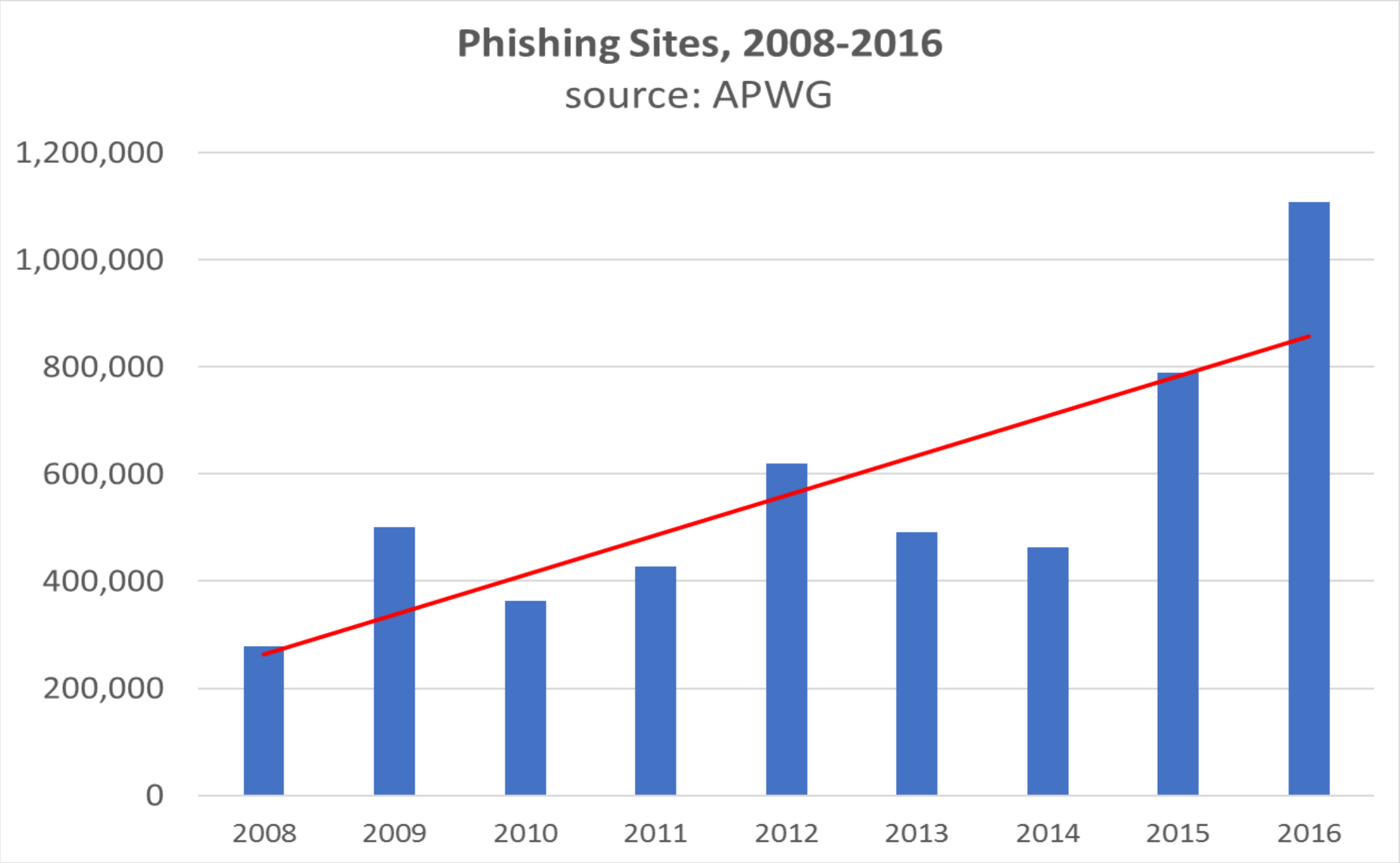
Effective DNS Abuse Mitigation: Why and How

- Anti-Phishing Working Group (www.apwg.org)
  - A not-for-profit research, educational, and industry association. It operates cybercrime data exchanges, publishes cybercrime statistics, and presents international cybercrime conferences. Members include companies, university researchers, law enforcement.
- Greg Aaron: APWG Senior Research Fellow
  - Also a professional cybercrime investigator, and member of ICANN SSAC

ICANN 58
COPENHAGEN
11–16 March 2017
COMMUNITY FORUM

APWG

Phishing Attacks (and malicious domain use) up



ICANN 58 COPENHAGEN 11–16 March 2017 COMMUNITY FORUM

Greg Aaron, 13 March 2017

APWG

Some Realities

- Cybercrime is more pervasive and more professional than ever.
- Abuse tends to concentrate in certain places, and moves over time:
  - Concentrations at certain registries (TLDs), registrars, hosting providers
  - Why? Often due to inattention, low price.
  - Cases where service providers are operated for criminal purposes (Registrars: Estdomains, AB Systems, etc.)
- Mitigation is mainly done by private parties, not law enforcement.
  - On the Internet, relationships are governed by contracts.
  - The reach of any law enforcement body is limited by jurisdiction, and is necessarily slow.
  - Those who operate Internet resources have the responsibility to do so responsibly.
- Criminals know the domain system, and don't play by the rules.

Example of Clustering

SURBL is a major reputation service that lists domains for malware, spam, and phishing. The top TLDs it lists are:

	TLD	Domains listed
1	.COM	479,231
2	.TOP	312,555
3	.SCIENCE	135,821
4	.NET	130,512
5	.BIZ	124,594
6	.US	92,402
7	.ORG	77,767
8	.GDN	70,889
9	.WIN	63,861
10	.INFO	62,983
11	.RACING	51,931
12	.LINK	36,884
13	.RU	33,665
14	.LOAN	26,766
15	.TRADE	23,411
16	.CLICK	23,113
17	.BID	22,765
18	.DOWNLOAD	20,793
19	.DATE	19,908
20	.XYZ	18,362

Source: http://www.surbl.org/tld , 8 March 2017

ICANN’s Role

- Mission: “Facilitate the openness, interoperability, resilience, security and/or stability of the DNS.” Public interest.
- ICANN accredits registrars and registry operators.
- In keeping with this mission and responsibility are ICANN policies, placed in contracts via community input.
  - WHOIS accuracy provisions (registrants, registrars)
  - Prohibitions against malicious use of domain names (registrants)
  - Anti-abuse monitoring, response, and reporting requirements (registries, registrars)
- ICANN’s contracts are enforceable.
- Suggestion: use those contractual tools to concentrate on the biggest, most harmful situations.

.BANK & .INSURANCE

Trusted. Verified. More Secure.

ICANN58 – 13 March 2017

fTLD
Registry Services, LLC

Registry Policies and Requirements

- Developed by Community-Based Working Groups, Advisory Council and approved by fTLD Management Team and Board of Directors
- Policies
  - **Registrant Eligibility**
  - **Names Selection**
  - **Acceptable Use / Anti-Abuse**
- Requirements
  - **Registrant verification prior to domain award**
  - **Robust Security Requirements**
  - **Prohibition of Privacy/Proxy Registrations**
- Security Requirements Monitoring

Registry Policies and Requirements (cont'd.)

- Registrant Verification: modeled after CA/Browser Forum Extended Validation SSL Certificates Guidelines
  - Entity eligibility
  - Confirmed phone number and mailing address
  - Registrant is a full-time employee and authorized (via phone call)
  - Domain name eligibility
- Security Requirements
  - Domains must be DNSSEC signed and have in-zone name servers to be in the zone and accessible to registrants
  - Transport Layer Security/strong cipher suites, authenticated email, multi-factor authentication, DNS Resource Records limitations
- Security Requirements Monitoring
  - Daily reporting to fTLD
  - Weekly notification to registrars/registrants about compliance issues

Operational Highlights

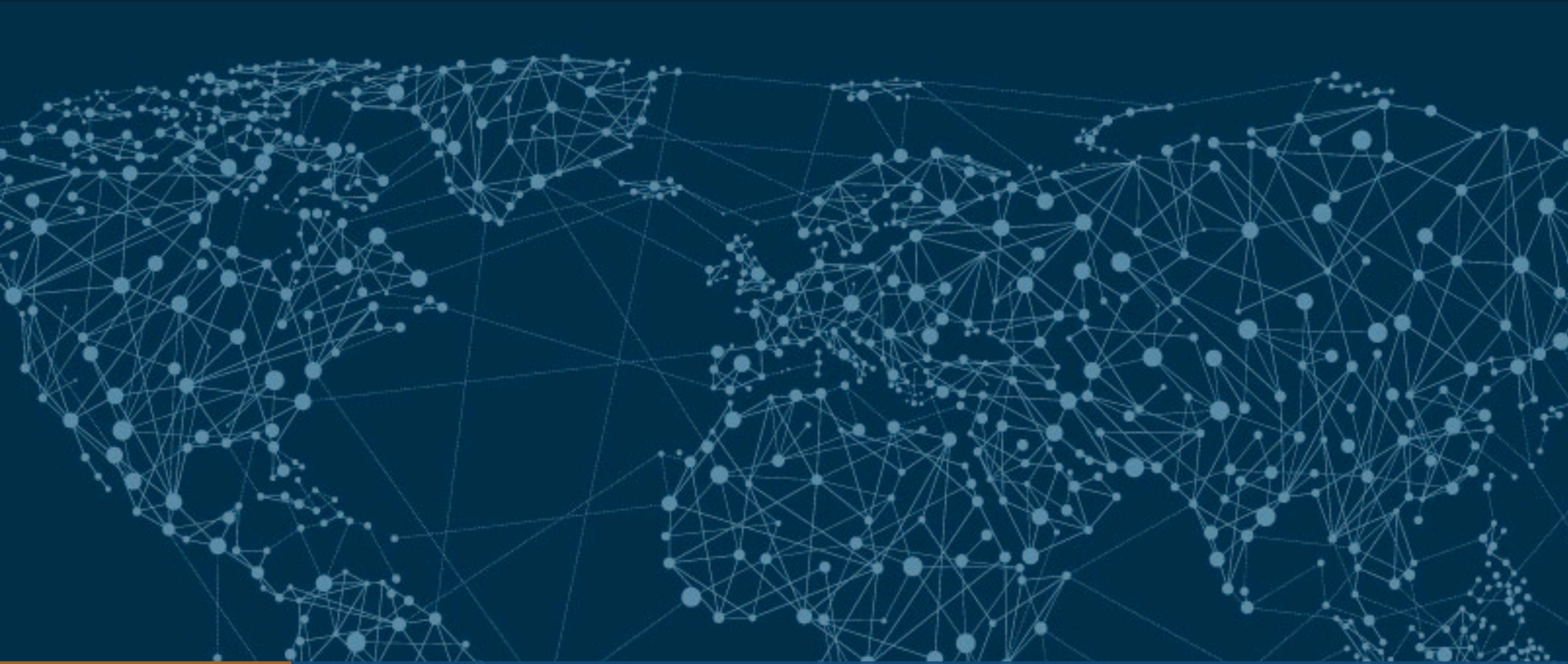
- Registration restrictions and verification are essential; public trust, safety and reputational risks are significant
- Providing resources to support activation is critical to adoption & use:
  - **Guides to Leveraging an fTLD Domain: https://www.ftld.com/guide/**
  - **Third-Party Provider Program: https://www.ftld.com/third-party-provider-program/**
- Verification, security requirements/monitoring and compliance activities contribute to high operating costs -> domain fees are high (another obstacle for bad actors)

Verified Top-Level Domains Consortium

- Advocates for enhancing public trust and online safety
- fTLD is a founding member along with .PHARMACY and .MED
- Nine members/15 gTLDs; four advisors
- Learn more at https://www.vTLD.domains/

Resources

- Craig Schwartz, craig@fTLD.com; +1 202 589 2532
- Registries Policies: https://www.ftld.com/policies/
- Security Requirements: https://www.ftld.com/enhanced-security/
- Verification Overviews: https://www.ftld.com/registrar-toolkit/
- .BANK: https://www.register.bank/
- .INSURANCE: https://www.register.insurance/



Security, Stability and Resiliency Team
Office of the CTO

David Conrad | ICANN 58 | March 2017

Agenda

Topics for discussion

- Handling of abuse, interactions with Contractual Compliance, contracted parties, others.
- Research project on public reporting of abuse.
- Identifier System Attack Mitigation Methodology.
- Improve state of abuse mitigation.

SSR Team’s interactions with Contractual Compliance, others

- The SSR Team and Contractual Compliance are investigating how SSR can further collaborate with Contractual Compliance by providing subject matter expertise.
- The SSR Team refers matters we have knowledge of to Contractual Compliance.
- The SSR Team regularly reaches out to contracted parties and the operational security community enabling informal collaboration in voluntary threat mitigation.

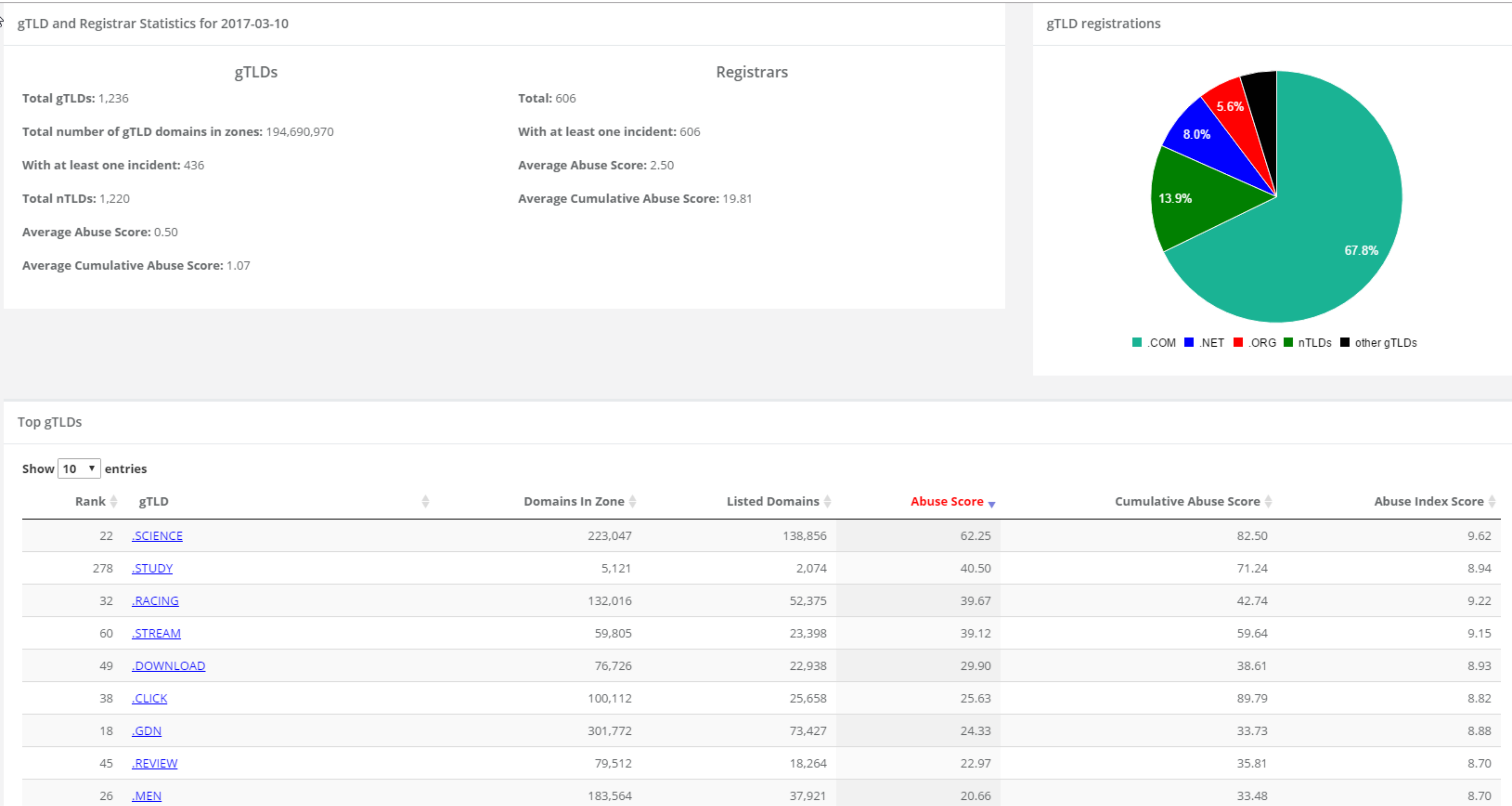
SSR Team – Anti-Abuse Research Project

- Hired a third party contractor to provide an abuse data analysis platform, currently in beta.

- Multiple data feeds focused on activity including the abuse types mentioned in the relevant GAC Communiqués.

- Investigating how we can make results available.

Abuse Data Analysis Platform (not yet production)



gTLD and Registrar Statistics for 2017-03-10

gTLDs

Total gTLDs: 1,236

Total number of gTLD domains in zones: 194,690,970

With at least one incident: 436

Total nTLDs: 1,220

Average Abuse Score: 0.50

Average Cumulative Abuse Score: 1.07

Registrars

Total: 606

With at least one incident: 606

Average Abuse Score: 2.50

Average Cumulative Abuse Score: 19.81

gTLD registrations

Top gTLDs

Show 10 ▾ entries

Rank	gTLD	Domains In Zone	Listed Domains	Abuse Score	Cumulative Abuse Score	Abuse Index Score
22	.SCIENCE	223,047	138,856	62.25	82.50	9.62
278	.STUDY	5,121	2,074	40.50	71.24	8.94
32	.RACING	132,016	52,375	39.67	42.74	9.22
60	.STREAM	59,805	23,398	39.12	59.64	9.15
49	.DOWNLOAD	76,726	22,938	29.90	38.61	8.93
38	.CLICK	100,112	25,658	25.63	89.79	8.82
18	.GDN	301,772	73,427	24.33	33.73	8.88
45	.REVIEW	79,512	18,264	22.97	35.81	8.70
26	.MEN	183,564	37,921	20.66	33.48	8.70

Identifier System Attack Mitigation Methodology

Addressing First Security, Stability & Resiliency Review Team (SSR-RT) Recommendation 12:

- An Identifier System Attack Mitigation Methodology be created

- ➢ Identify, prioritize, and periodically refresh a list of top attacks.
- ➢ Develop guidance on high-impact attacks and emerging high-risk vulnerabilities.
- ➢ Describe corresponding attack mitigation practices
- ➢ Encourage broader adoption of those practices via contracts, agreements, incentives, etc.

Available at https://www.icann.org/en/system/files/files/identifier-system-attack-mitigation-methodology-13feb17-en.pdf

Improve State of DNS Abuse Mitigation

Part of the SSR Team’s role:

- ➢ Produce impartial unbiased data and analytics to enable informed community policy development.
- ➢ Inform the ICANN organization’s various functions relating to DNS abuse matters.

OCTO’s Research and SSR teams are focused towards these goals.

Improve State of DNS Abuse Mitigation (cont'd)

More of the SSR Team's role:

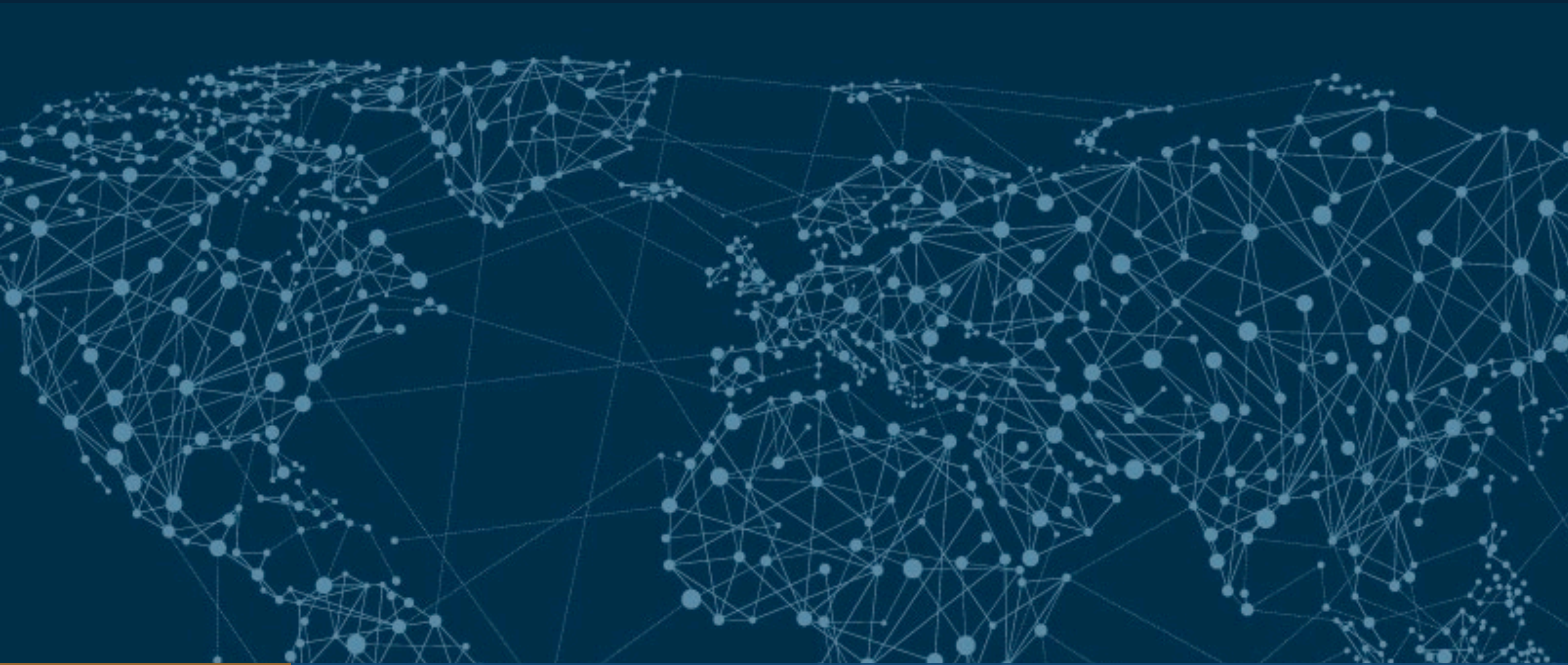
- Provide training and advice to Public Safety community to enable them to understand:

  1. The technical DNS environment;
  2. The ICANN policy development processes; and
  3. ICANN organizational processes and procedures.

Questions ?

The ICANN 58 presentations will be available at:

- The ICANN 58 Schedule page



Cross-Community Session: Towards Effective DNS Abuse Mitigation: Prevention, Mitigation & Response

Contractual Compliance | ICANN 58 | 13 March 2017

Agenda

Request to discuss in more details

- How the ICANN SSR Team and Compliance department work together
- What specific actions have been taken against registrars
- How proactive monitoring is conducted, how often, who does it touch, if there are obstacles such as resources

Background – The PSWG requested additional information to support the Compliance response to Annex 1 GAC Hyderabad Communique. (slide 13)

How the ICANN SSR Team and Compliance department work together

- ICANN internal referrals to Compliance of compliance-related matters are generated from multiple departments, for example:
  - Finance on past due fees
  - Technical Services as a result of Service Level and other monitoring
  - SSR Team on DNS abuse
  - PTI customer service referrals
  - Global Support referrals
  - GDD Ops Compliance Checks

- All referrals follow the Contractual Compliance Approach & Process (slide 14)

- Responses from contracted parties are reviewed by Compliance and as needed with the appropriate department

- SSR acts as ICANN’s main interface to the Operational Security communities and as such regularly communicates abuse issues with Compliance & active coordination between the departments

What specific actions have been taken against registrars

Enforcement actions taken against Registrars in 2016:

- 25 Registrars received a Notice of Breach
  - 4 Registrars were escalated to Suspension and then Termination
  - Suspension prohibits new registrations or inbound transfers

- Examples and trends on next slides

Actions taken to promote increased compliance by Registrars:

- Increased proactive monitoring

- Targeted outreach efforts

- Escalated Notices for previously remediated or repeat noncompliance

- On going audits – please refer to slides 19 – 21 for details

ICANN Enforcement in 2016

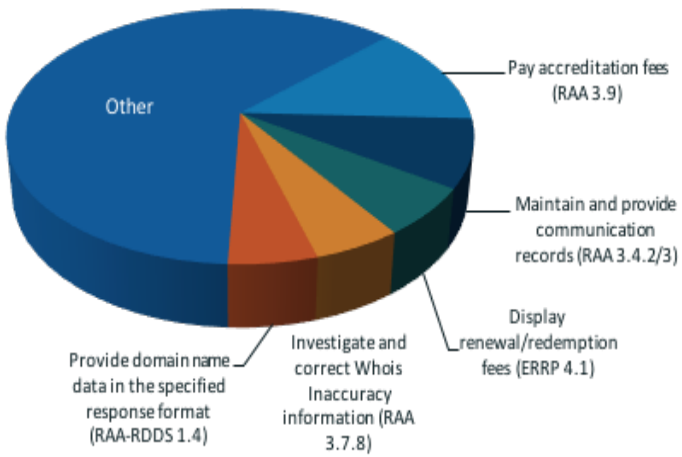
5% of enforcement reasons in 2016 for failure to cure Whois Inaccuracy issues; other issues were resolved.

For list of Registrars/Reasons of Enforcement: https://features.icann.org/compliance/enforcement-notices

For Enforcement Notices Page: https://www.icann.org/compliance/notices

Formal Notice Activity – Year 2016

Notice Reasons



Notices	Qty
Breach	25
Contract Non-Renewal	0
Suspension	4
Termination	4

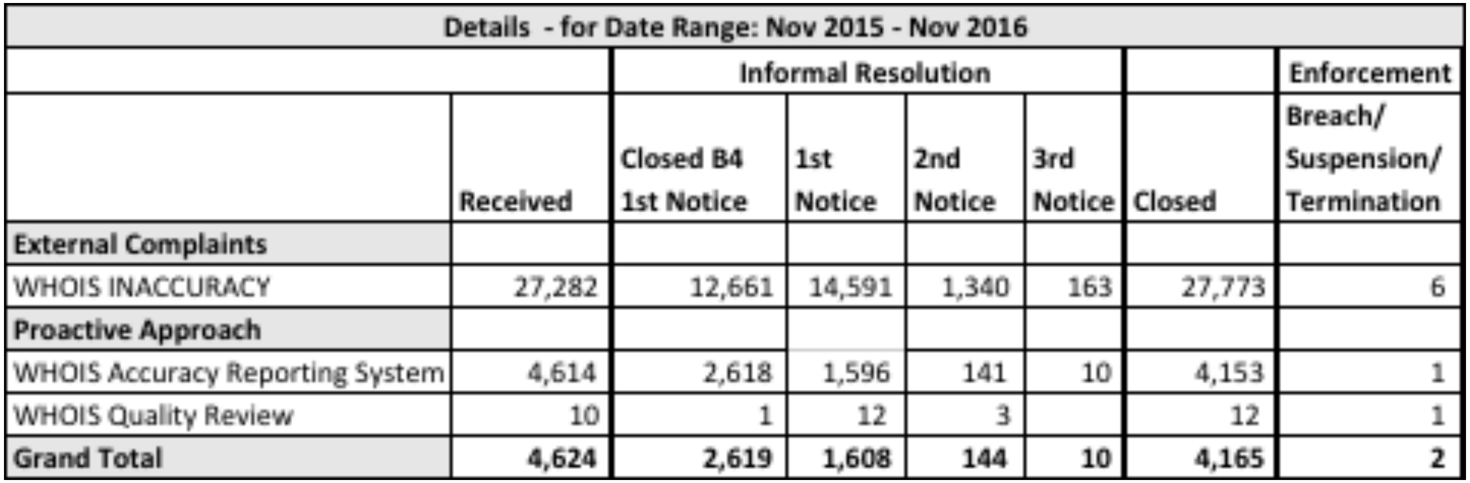
Breach Notice Reason*	Qty*
Failure Notice Reasons	119
• Cured	74
• Not Cured	45

*A singe Breach may contain multiple Notices Reasons.

Formal Notice Reasons	Percent
Pay accreditation fees (RAA 3.9)	13 %
Maintain and provide communication records (RAA 3.4.2/3)	9 %
Display renewal/redemption fees (ERRP 4.1)	6 %
Investigate and correct Whois Inaccuracy information (RAA 3.7.8)	**5 %**
Provide domain name data in the specified response format (RAA-RDDS 1.4)	5 %
Other	62 %

Source: 2016 Contractual Compliance Annual Report
Other Reasons – please refer to Appendix B of the report.

Response to Annex 1 GAC Communique WHOIS Inaccuracy Nov 2015 – Nov 2016



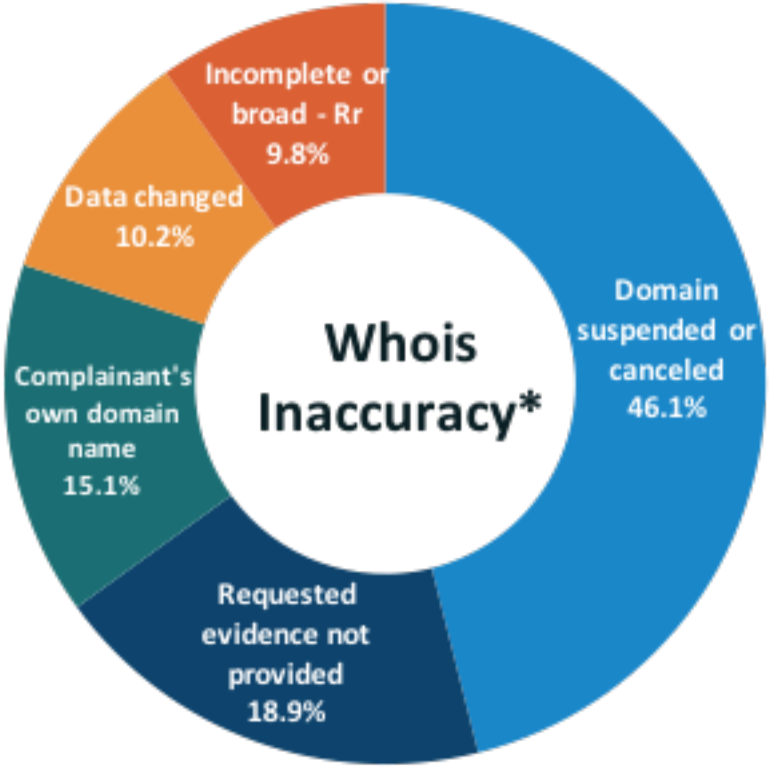
Details - for Date Range: Nov 2015 - Nov 2016							
		Informal Resolution					Enforcement
	Received	Closed B4 1st Notice	1st Notice	2nd Notice	3rd Notice	Closed	Breach/ Suspension/ Termination
External Complaints							
WHOIS INACCURACY	27,282	12,661	14,591	1,340	163	27,773	6
Proactive Approach							
WHOIS Accuracy Reporting System	4,614	2,618	1,596	141	10	4,153	1
WHOIS Quality Review	10	1	12	3		12	1
Grand Total	**4,624**	**2,619**	**1,608**	**144**	**10**	**4,165**	**2**

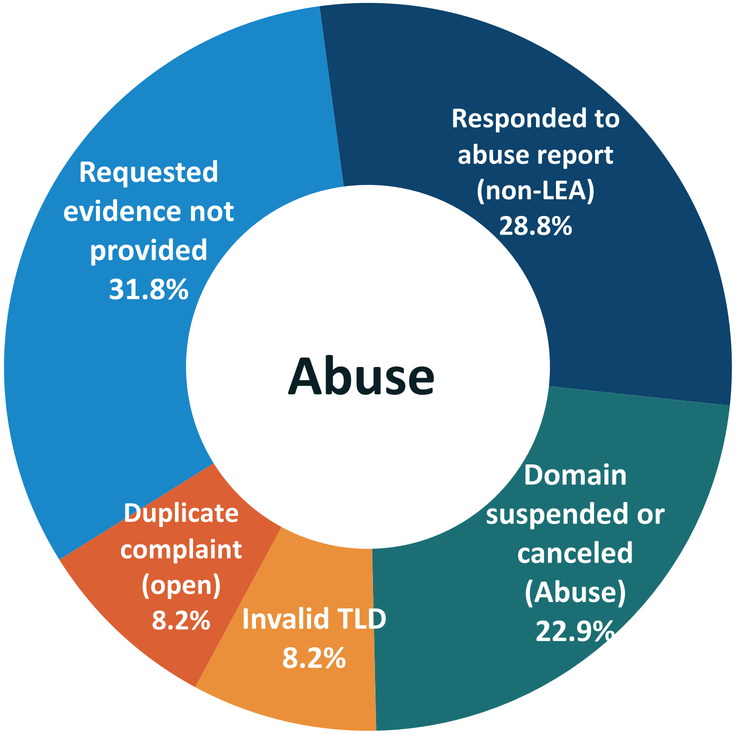
…Between November 2015 and November 2016, Whois inaccuracy complaints constituted approximately 70% of complaints processed by ICANN Contractual Compliance (**almost 32,000 complaints**).

- Different Types of Whois Inaccuracy efforts - External complaints and Internal monitoring type of complaints

- Complaints are resolved during the informal resolution process

Top Closure Reasons (Oct 2016 – Jan 2017)





Disclaimer: Due to rounding, percentages may not always appear to add up to 100%.

Closure reasons explain why a complaint is resolved or closed

How proactive monitoring is conducted, how often, who does it touch, if there are obstacles such as resources

Proactive monitoring is ICANN's effort to take initiative in identifying potential issues instead of waiting for issues to happen.

Proactive monitoring is conducted by way of:

- Automated tools that result in notifications to compliance
- Review of media and blogs
- Review of previously resolved issues (WHOIS Inaccuracy Quality Review)
- Review of registry Abuse contact data on their websites
- Review of registrar Abuse contact data on their websites and WHOIS data
- Sending emails to and calling registrar abuse contacts to verify

Frequency varies: real-time, daily and random efforts

Audits of contracted parties also proactively identify and address non-compliance

ICANN Proactive Monitoring & Outreach

Some efforts in 2016:

APAC Whois Verification Project – Goal is to test compliance with 2013 RAA requirements to verify and validate WHOIS information. Of 31 registrars from Asia Pacific region, 3 are in remediation to address non-compliance issues, 1 received Notice of Termination.

3rd Notice Continuous Improvement Project – Goal is to improve registrar compliance and resolution rate. Of 7 registrars, 3 had significant reduction in 3rd notice volume and 4 have had no subsequent 3rd notices.

Remediation Validation Project – Goal is to test and validate past remediation. Zero of 20 Registrars had new instances of non-compliance in areas where remediation was previously performed.

Updates are provided in Quarterly and Annual Reports at https://www.icann.org/resources/pages/compliance-reports-2016-04-15-en

Questions & Answers

Send compliance questions

To: compliance@icann.org

Subject line: ICANN 58 PSWG Session

The ICANN 58 presentations are available at:

- The ICANN Contractual Compliance Outreach page at this link https://www.icann.org/resources/compliance/outreach
- The ICANN 58 Schedule page
- ICANN's response to Annex 1 of the Hyderabad https://www.icann.org/en/system/files/correspondence/marby-to-schneider-08feb17-en.pdf

Appendix

Annex 1 To GAC Hyderabad Communique

Compliance response to GAC communique.

I. Implementation of 2013 RAA provisions and Registrar Accreditation

2. Enforcement by ICANN of WHOIS Verification, Validation and Accuracy Requirements
3. Diligence by ICANN in Relation to Registrars' Duty to Investigate Reports of Abuse
4. Awareness Efforts by ICANN on Registrars' Obligations: What efforts does ICANN undertake to ensure registrars are educated and aware of their contractual obligations?

III. DNS Abuse Investigation, reporting and mitigation performance

1. Abuse Investigations, Research, Reports
2. Multi-Jurisdictional Abuse Reporting

Note: Numbering above consistent with Annex 1 numbering

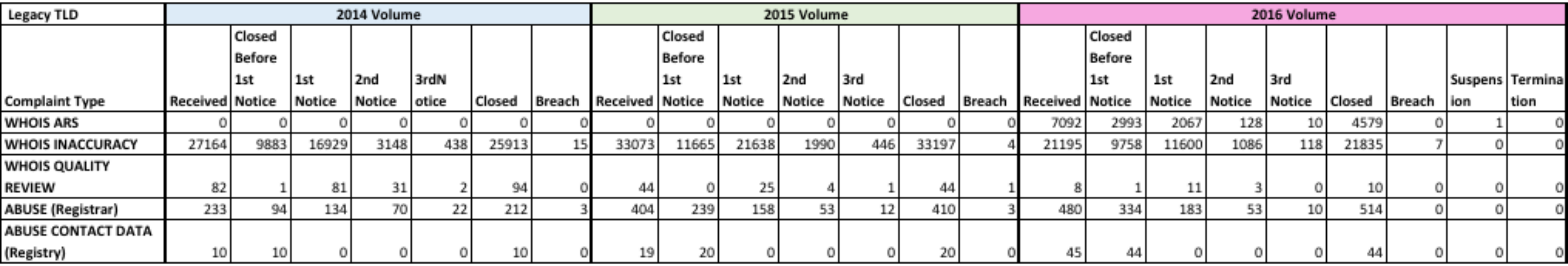
Contractual Compliance Approach & Process

- ICANN Contractual Compliance has a standard approach and process when dealing with compliance related matters

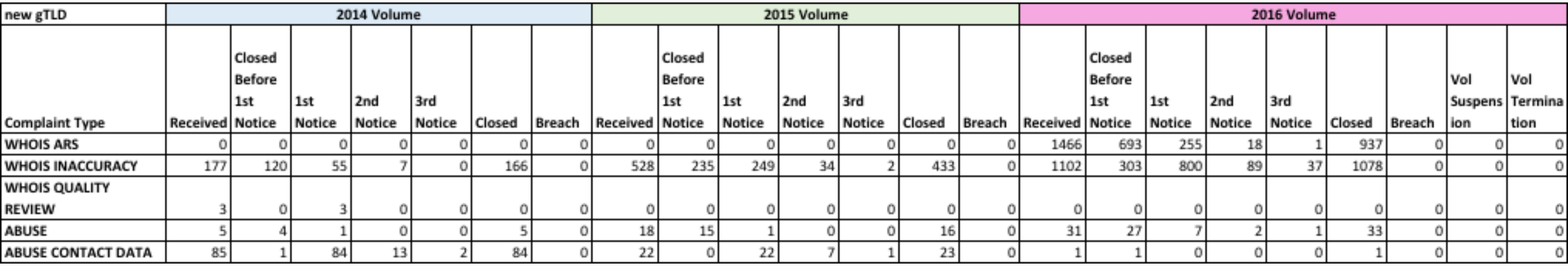
- General Guidance:
  - An Inquiry may be sent for information gathering
  - A Notice may be sent regarding an alleged area of noncompliance
  - An Escalated Notice applies to compliance matters that require immediate resolution or are a repeated matter of a recently cured breach.

- The Approach & Process can be found at - https://www.icann.org/resources/pages/approach-processes-2012-02-25-en

WHOIS Inaccuracy and Abuse Trends 2014 - 2016



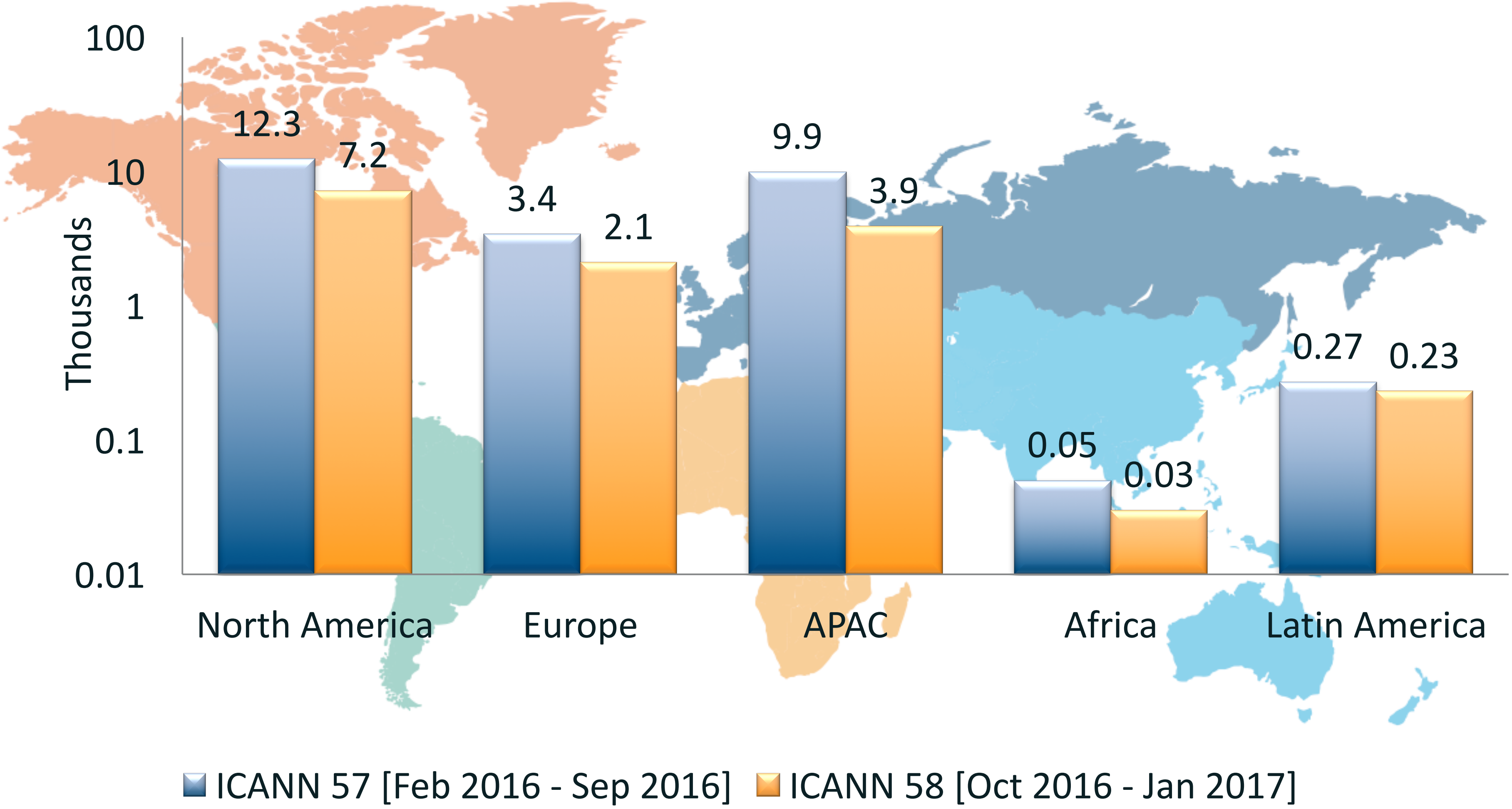
Legacy TLD	2014 Volume							2015 Volume							2016 Volume								
Complaint Type	Received	Closed Before 1st Notice	1st Notice	2nd Notice	3rdNotice	Closed	Breach	Received	Closed Before 1st Notice	1st Notice	2nd Notice	3rd Notice	Closed	Breach	Received	Closed Before 1st Notice	1st Notice	2nd Notice	3rd Notice	Closed	Breach	Suspension	Termination
WHOIS ARS	0	0	0	0	0	0	0	0	0	0	0	0	0	0	7092	2993	2067	128	10	4579	0	1	0
WHOIS INACCURACY	27164	9883	16929	3148	438	25913	15	33073	11665	21638	1990	446	33197	4	21195	9758	11600	1086	118	21835	7	0	0
WHOIS QUALITY REVIEW	82	1	81	31	2	94	0	44	0	25	4	1	44	1	8	1	11	3	0	10	0	0	0
ABUSE (Registrar)	233	94	134	70	22	212	3	404	239	158	53	12	410	3	480	334	183	53	10	514	0	0	0
ABUSE CONTACT DATA (Registry)	10	10	0	0	0	10	0	19	20	0	0	0	20	0	45	44	0	0	0	44	0	0	0



new gTLD	2014 Volume							2015 Volume							2016 Volume								
Complaint Type	Received	Closed Before 1st Notice	1st Notice	2nd Notice	3rd Notice	Closed	Breach	Received	Closed Before 1st Notice	1st Notice	2nd Notice	3rd Notice	Closed	Breach	Received	Closed Before 1st Notice	1st Notice	2nd Notice	3rd Notice	Closed	Breach	Vol Suspension	Vol Termination
WHOIS ARS	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1466	693	255	18	1	937	0	0	0
WHOIS INACCURACY	177	120	55	7	0	166	0	528	235	249	34	2	433	0	1102	303	800	89	37	1078	0	0	0
WHOIS QUALITY REVIEW	3	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ABUSE	5	4	1	0	0	5	0	18	15	1	0	0	16	0	31	27	7	2	1	33	0	0	0
ABUSE CONTACT DATA	85	1	84	13	2	84	0	22	0	22	7	1	23	0	1	1	0	0	0	1	0	0	0

- Volume of Compliance complaints since 2014
- The Contractual Compliance Approach & Process are published at https://www.icann.org/en/system/files/files/overall-03oct14-en.pdf

Global Complaint Trend ICANN 57 vs. ICANN 58



2013 RAA: Abuse Reports Requirements

Section 3.18.1

- Registrars must:
  - Take reasonable and prompt steps to investigate and
  - Respond appropriately to ANY reports of abuse
- Reasonable steps may include:
  - Contacting the RNH of the domain(s)
- "Appropriately" varies depending on facts and circumstances
- Court order is not required for registrar to investigate absent a specific local law or regulation provided to ICANN

VS

Section 3.18.2

- Registrar must have dedicated abuse email and phone number in WHOIS output
- Reports of Illegal Activity must be reviewed within 24 hours by an individual who is empowered to take necessary and appropriate actions
- Reports can be from any applicable jurisdiction once reporter is designated by registrar's local government as an authority

2013 RAA: Abuse Reports Complaint Processing

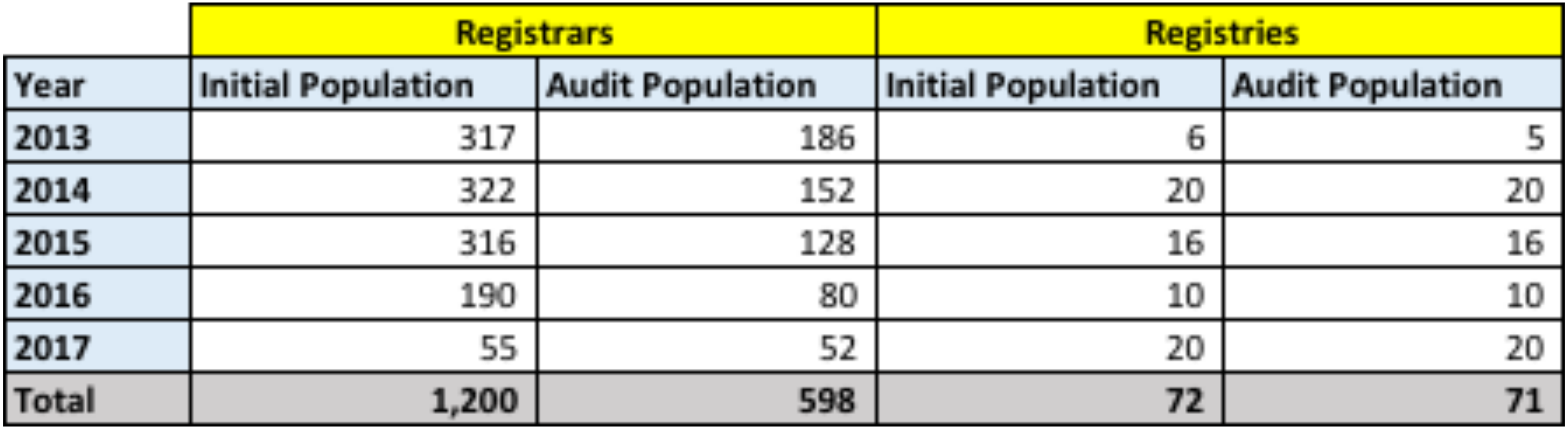
- ICANN confirms reporter sent abuse report to registrar abuse contact before sending complaint to registrar

- ICANN could request:
  - Steps taken to investigate and respond to abuse report
  - Time taken to respond to abuse report
  - Correspondence with complainant and registrant
  - Link to website's abuse contact email and handling procedure
  - Location of dedicated abuse email and telephone for law-enforcement reports
  - WHOIS abuse contacts, email and phone

- Examples of steps registrars took to investigate and respond to abuse reports:
  - Contacting registrant
  - Asking for and obtaining evidence or licenses
  - Providing hosting provider info to complainant
  - Performing WHOIS verification
  - Performing transfer upon request of registrant
  - Suspending domain

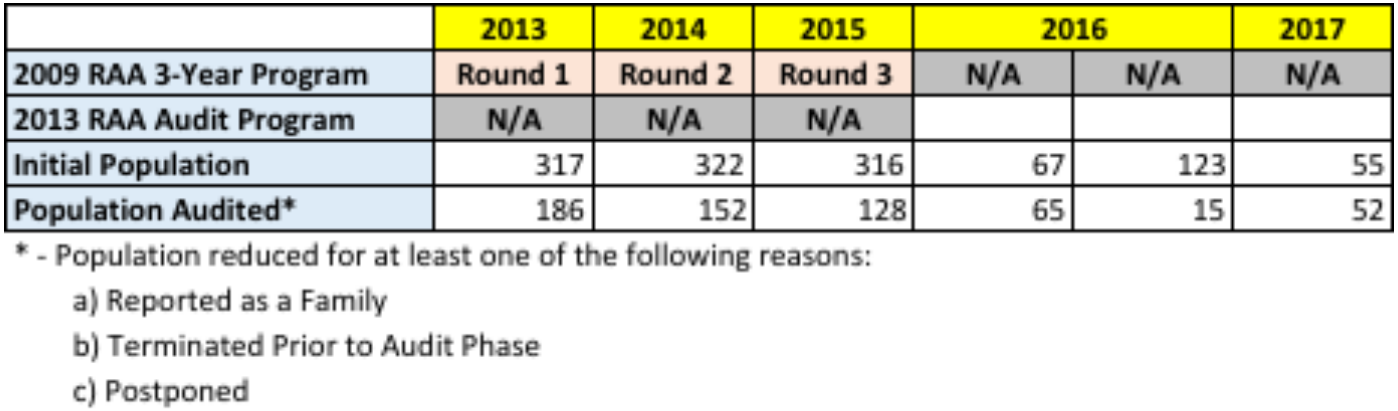
Contractual Compliance Audits

The table below provides a summary of the audits performed from 2013 to 2017



	Registrars		Registries	
Year	Initial Population	Audit Population	Initial Population	Audit Population
2013	317	186	6	5
2014	322	152	20	20
2015	316	128	16	16
2016	190	80	10	10
2017	55	52	20	20
Total	**1,200**	**598**	**72**	**71**

Contractual Compliance Registrar Audits & Top 5 Deficiencies



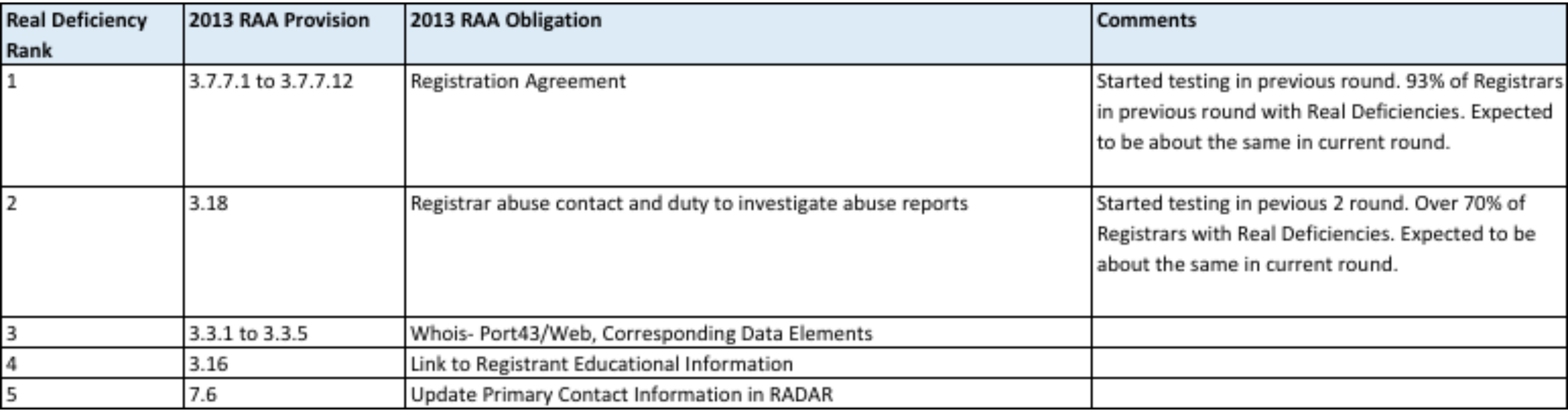
	2013	2014	2015	2016		2017
2009 RAA 3-Year Program	Round 1	Round 2	Round 3	N/A	N/A	N/A
2013 RAA Audit Program	N/A	N/A	N/A			
Initial Population	317	322	316	67	123	55
Population Audited*	186	152	128	65	15	52

* - Population reduced for at least one of the following reasons:

a) Reported as a Family

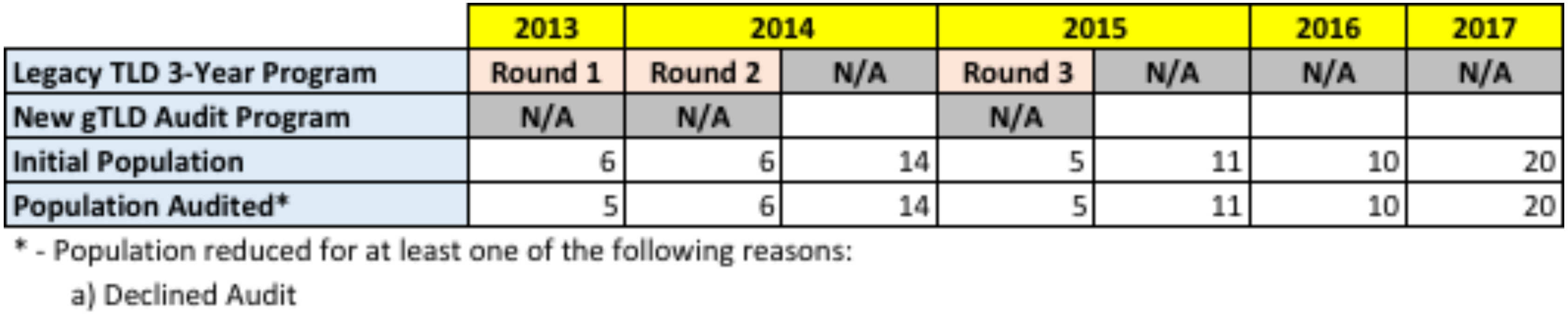
b) Terminated Prior to Audit Phase

c) Postponed



Real Deficiency Rank	2013 RAA Provision	2013 RAA Obligation	Comments
1	3.7.7.1 to 3.7.7.12	Registration Agreement	Started testing in previous round. 93% of Registrars in previous round with Real Deficiencies. Expected to be about the same in current round.
2	3.18	Registrar abuse contact and duty to investigate abuse reports	Started testing in pevious 2 round. Over 70% of Registrars with Real Deficiencies. Expected to be about the same in current round.
3	3.3.1 to 3.3.5	Whois- Port43/Web, Corresponding Data Elements	
4	3.16	Link to Registrant Educational Information	
5	7.6	Update Primary Contact Information in RADAR	

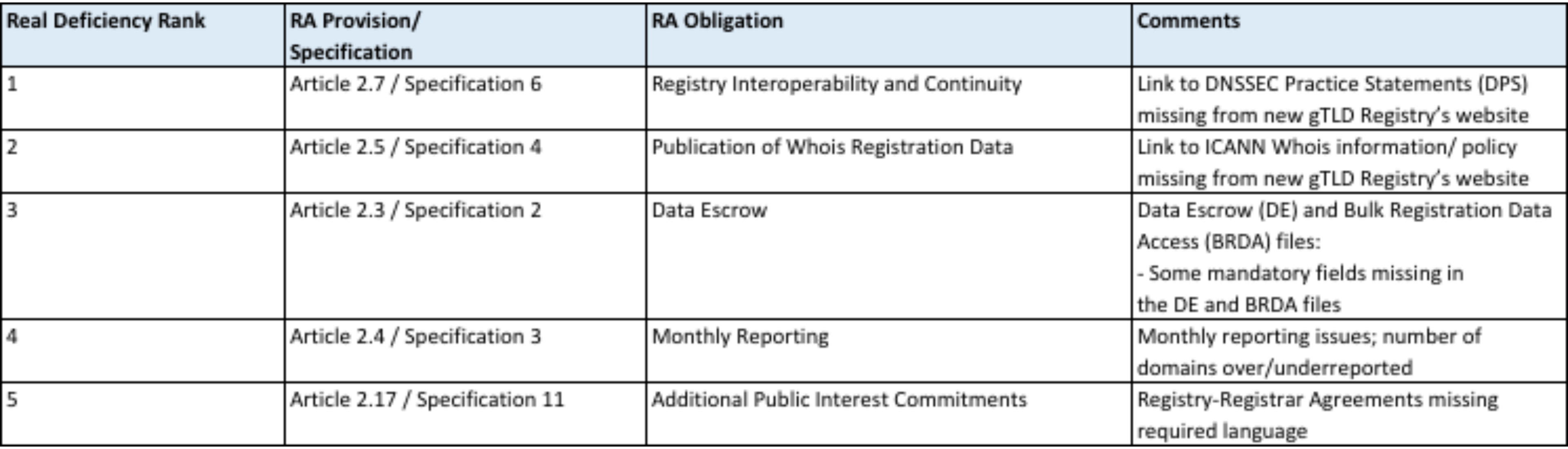
Contractual Compliance Registry Audits & Top 5 Deficiencies



	2013	2014		2015		2016	2017
Legacy TLD 3-Year Program	Round 1	Round 2	N/A	Round 3	N/A	N/A	N/A
New gTLD Audit Program	N/A	N/A		N/A			
Initial Population	6	6	14	5	11	10	20
Population Audited*	5	6	14	5	11	10	20

* - Population reduced for at least one of the following reasons:

a) Declined Audit



Real Deficiency Rank	**RA Provision/ Specification**	**RA Obligation**	**Comments**
1	Article 2.7 / Specification 6	Registry Interoperability and Continuity	Link to DNSSEC Practice Statements (DPS) missing from new gTLD Registry's website
2	Article 2.5 / Specification 4	Publication of Whois Registration Data	Link to ICANN Whois information/ policy missing from new gTLD Registry's website
3	Article 2.3 / Specification 2	Data Escrow	Data Escrow (DE) and Bulk Registration Data Access (BRDA) files: - Some mandatory fields missing in the DE and BRDA files
4	Article 2.4 / Specification 3	Monthly Reporting	Monthly reporting issues; number of domains over/underreported
5	Article 2.17 / Specification 11	Additional Public Interest Commitments	Registry-Registrar Agreements missing required language