The purpose of this document is to carry out Task 8 of the RDS PDP WG Phase 1 work plan. As noted in that plan, the bulk of the WG’s work will involve recommending requirements for registration directory services.

Recognizing that the Board recommended that the EWG Final Report should be the starting point for this PDP and that EWG efforts, although not policy development, were very comprehensive with extensive and thorough consideration of public input, this document identifies ***possible*** requirements from the [EWG Final Report](https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf) along with ***possible*** requirements obtained from [additional Key Inputs](https://community.icann.org/display/gTLDRDS/Additional+Key+Inputs) such as the sources identified by [input-gathering sub-teams](https://community.icann.org/x/DDCAAw) on Data, Purpose and Privacy and in the [PDP Issue Report](http://whois.icann.org/sites/default/files/files/final-issue-report-next-generation-rds-07oct15-en.pdf), and ***possible*** requirements suggested by [SG/C/SO/AC Inputs](https://community.icann.org/x/pYxlAw) and [WG Members](https://community.icann.org/x/I4xlAw).

After all ***possible*** requirements are gathered into a comprehensive and inclusive list, which is compiled without debate on the merits of each of the ***possible*** requirements, the WG will design a very systematic approach to maximize efficiency in discussing and attempting to reach consensus on recommended requirements for registration directory services. These requirements will help the WG reach an informed decision about if and why a next-generation system is needed to replace today’s WHOIS system.

**Organization**

The ***possible*** requirements listed in this document are organized as follows:

1. ***Possible*** Requirements that map to one or more of the eleven (11) questions in the charter. Note that the same requirement may address multiple questions.
2. ***Possible*** Requirements that may not map to any question identified in the charter.
3. ***Possible*** Foundational Questions that must be answered based on all other requirements.

As stated above, all of the ***possible*** requirements in this document are derived from cited Key Input documents (listed in Annex A), supplemented by any additional ***possible*** requirements suggested by WG members or SGs, Cs, SOs and ACs during outreach.

After the WG confirms that this list of ***possible*** requirements is sufficiently complete to serve as the foundation for WG deliberation, the WG should continue through its work plan until reaching Task 12 where it will systematically consider each ***possible*** requirement individually with the goal of trying to reach as strong a consensus as possible as to whether the WG supports the possible requirement, including how it is worded.

The grouping of the requirements into the 11 charter questions should not be seen as fixed. The WG should feel free to move ***possible*** requirements under different questions and even to include a given requirement under more than one question if that seems useful, as long as the duplication is noted.

The order of the ***possible*** requirements within the various sections in this document is primarily based on the order in which the 11 questions are posed in the WG’s charter. The WG may decide to change the order to provide a more useful presentation but this should be done with full consideration of the reasons why the order was established in the framework. Due to interdependencies, WG deliberation will likely be iterative, especially on fundamental questions pertaining to purpose, data, and privacy.

**Notation**

***Possible*** requirements are numbered using the notation [QQ-D#-R#] for ease of use and scalability as this list evolves. Specifically, “QQ” identifies the associated question as follows:

**FQ** Foundational Questions: Questions to be answered based on all other requirements

**OQ** Other Questions: Questions that may not fit within the 11 charter questions

**UP** Users/Purposes: Who should have access to gTLD registration data and why?

**GA** Gated Access: What steps should be taken to control data access for each user/purpose?

**DA** Data Accuracy: What steps should be taken to improve data accuracy?

**DE** Data Elements: What data should be collected, stored, and disclosed?

**PR** Privacy: What steps are needed to protect data and privacy?

**CX** Coexistence: What steps should be taken to enable coexistence?

**CM** Compliance: What steps are needed to enforce these policies?

**SM** System Model: What system requirements must be satisfied by any implementation?

**CS** Cost: What costs will be incurred and how must they be covered?

**BE** Benefits: What benefits will be achieved and how will they be measured?

**RI** Risks: What risks do stakeholders face and how will they be reconciled?

This “QQ” will be followed by “D#” which identifies by number a key input document from Annex A.

Finally, “R#” sequentially numbers within each document all ***possible*** requirements. For example, [UP-D1-R3] is the third ***possible*** user/purpose requirement extracted from the EWG Final Report [D1], while [DE-D1-R4] is the fourth ***possible*** data element requirement taken from that same document.

***Possible*** requirements are not necessarily quoted verbatim from key input documents, but rather phrased as needed to describe a ***possible*** requirement for gTLD registration directory services or registration data. In particular, ***possible*** fundamental requirements should not be specific to today’s WHOIS system or a next-generation replacement, since the goal is to enable WG deliberation and consensus as the basis for answering foundational questions posed by the WG charter.

**Users/Purposes (UP)**

The following ***possible*** requirements address the charter question on Users and Purposes (UP): *Who should have access to gTLD registration data & why?*   
***Possible*** requirements for WG deliberation include:

**[UP-D1-R1]** –“ In support of ICANN’s mission to coordinate the global Internet’s system of unique identifiers, and to ensure the stable and secure operation of the Internet’s unique identifier system, information about gTLD domain names is necessary to promote trust and confidence in the Internet for all stakeholders.” (p. 16, Section IIb, Purpose)

**[UP-D1-R2]** – “gTLD registration data [must be] collected, validated and disclosed for permissible purposes only.” (p. 21, p. 31 Principle 6)

**[UP-D1-R3]** – gTLD registration directory services must “accommodate in some manner all identified permissible purposes”, including the following users and permissible purposes. (pp. 21-25, 27-29)

**[UP-D1-R4]** – Domain Name Control – “Creating, managing and monitoring a Registrant’s own domain name (DN), including creating the DN, updating information about the DN, transferring the DN, renewing the DN, deleting the DN, maintaining a DN portfolio, and detecting fraudulent use of the Registrant’s own contact information.”

**[UP-D1-R5]** – Personal Data Protection – “Identifying the accredited Privacy/Proxy Provider or Secure Protected Credential Approver associated with a DN and reporting abuse, requesting reveal, or otherwise contacting that Provider.”

**[UP-D1-R6]** – Technical Issue Resolution – “Working to resolve technical issues associated with domain name use, including email delivery issues, DNS resolution failures, and website functional issues, by contacting technical staff responsible for handling these issues.”

**[UP-D1-R7]** – Domain Name Certification – “Certification Authority (CA) issuing an X.509 certificate to a subject identified by a domain name needing to confirm that the DN is registered to the certificate subject.”

**[UP-D1-R8]** – Individual Internet Use – “Identifying the organization using a domain name to instill consumer trust, or contacting that organization to raise a customer complaint to them or file a complaint about them.”

**[UP-D1-R9]** – Business Domain Name Purchase or Sale – “Making purchase queries about a DN, acquiring a DN from another Registrant, and enabling due diligence research.”

**[UP-D1-R10]** – Academic/Public-Interest DNS Research – “Academic public-interest research studies about domain names published in [gTLD registration directory services], including public information about the Registrant and designated contacts, the domain name’s history and status, and DNs registered by a given Registrant.”

**[UP-D1-R11]** – Legal Actions – “Investigating possible fraudulent use of a Registrant’s name or address by other domain names, investigating possible trademark infringement, contacting a Registrant/Licensee’s legal representative prior to taking legal action and then taking a legal action if the concern is not satisfactorily addressed. ”

**[UP-D1-R12]** – Regulatory and Contractual Enforcement – “Tax authority investigation of businesses with online presence, UDRP investigation, contractual compliance investigation, and registration data escrow audits.”

**[UP-D1-R13]** – Criminal Investigation & DNS Abuse Mitigation – “Reporting abuse to someone who can investigate and address that abuse, or contacting entities associated with a domain name during an offline criminal investigation.”

**[UP-D1-R14]** – DNS Transparency – “Querying the registration data made public by Registrants to satisfy a wide variety of needs to inform the general public.”

**[UP-D1-R15]** – gTLD registration directory services must support active deterrence of known malicious activities to the extent other requirements are satisfied. (See paragraph c on page 25.)

**[UP-D1-R16]** –“All purposes/contacts must be codified by policymakers through a defined process for adding, changing, or deleting purposes.” (p.37)

**[UP-D1-R17]** – Since it is likely that further [permissible purposes] will be identified over time, any [gTLD registration directory service] must be designed with extensibility in mind.

**[UP-D1-R18]** – gTLD registration directory services must provide the “ability to determine all domains registered by a given entity (commonly referred to as Reverse WHOIS).” (p. 26)

**[UP-D1-R19]** – gTLD registration directory services must provide the “The ability to determine historical domain name registration information (commonly referred to as WhoWas).”

**[UP-D1-R20]** – ICANN must publish, in one place, a user-friendly policy describing the purpose and permissible uses of registration data, to clearly inform Registrants why this data is being collected and how it will be handled and used.

**[UP-D1-R21]** – There must be clearly defined permissible/impermissible uses of gTLD registration data and directory services.

**[UP-D1-R22]** – gTLD registration directory services must support defined permissible purposes, including uses that involve:

**[UP-D1-R23]** – Identifying the Registrant and contacts designated for a given purpose;

**[UP-D1-R24]** – Communicating with contacts designated for a given purpose;

**[UP-D1-R25]** – Using data published by Registries about Domain Names; and

**[UP-D1-R26]** – Searching portions of registration data required for a given purpose.

**[UP-D1-R27]** – gTLD registration directory services must be designed with the ability to accommodate new users and permissible purposes that are likely to emerge over time.

**[UP-D1-R28]** – An application process must be defined.

**[UP-D1-R29]** – Applications must be reviewed against defined criteria.

**[UP-D1-R30]** – Applications that pass review must be evaluated and approved by a multistakeholder review board as determined by a policy development process.

**[UP-D1-R31]** – Approved applications must be added to the gTLD registration directory services privacy policy and scheduled for implementation periodically (e.g., quarterly, annually) as defined by policy.

**[UP-D1-R32]** – All identified permissible purposes should be accommodated by gTLD registration directory services in some manner, with the exception of known malicious Internet activities that must be actively deterred.

**[UP-D1-R33]** – All permissible purposes must be mapped to specific contact data needed for that specific purpose. (p.36)

**[UP-D1-R34]** – gTLD registration directory services must meet contact data requirements associated with permissible purposes through the following principles 8-14 on pp. 35-36.

**[UP-D1-R35]** – Purpose-based contact data must be provided for every registered domain name which makes public the union of data elements that are mandatory. [See DE ***possible*** requirements.]

**[UP-D1-R36]** – All mandatory purpose-based contact data must be syntactically accurate and operationally reachable to meet the needs of every codified permissible purpose.

**[UP-D1-R37]** – During domain name registration, the Registrant must be informed of all permissible purposes and given an opportunity to publish contact data for each purpose, including replacing the Registrant’s contact data for any or all purposes.

**[UP-D1-R38]** – A domain name must not be activated (put into the global DNS) until valid contact data is provided for every applicable purpose.

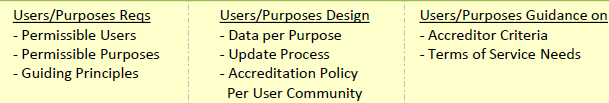
**[UP-D1-R39]** – If contact data becomes invalid for its designated purpose, a process that provides the Registrant with the ability to specify a new valid contact must ensue, allowing reasonable notification and time for update to occur. [See DA ***possible*** requirements].

**[UP-D1-R40]** – A process and policies must be developed enabling Registrant-designated contacts to opt-in/opt-out of having their data published as contacts for domain names, to support the rights of persons and entities to accept or reject responsibility for serving in specific roles for particular domain registrations.

**[UP-D1-R41]** – Any system for providing purpose-based contact data must be flexible and allow for new purposes and contact types to be created and published.

**[UP-D1-R42]** – gTLD registration directory services must allow registrants to optionally supply “designated administrative, technical, accredited Privacy/Proxy Provider, and business contacts” to be made accessible when appropriate for those specific purposes.

**[UP-D1-R43]** –“. . . the [gTLD registration directory service] portal [must] make the definitions for every purpose-based contact type readily accessible to users (for example, using hover-over pop-up definitions) to clearly indicate that contacts are published to handle inquiries for permissible purposes, and that a point of contact must be designated to cover those purposes.” (p.57)

See Additional Key Inputs for this charter question ([hyperlinked on this Wiki page](https://community.icann.org/pages/viewpage.action?pageId=56986720)) which may be consulted as a potential source of ***possible*** requirements. The PDP WG may also identify additional sources by themselves or through community outreach.  
  
[CHECK FOR ALIGNMENT WITH PROCESS FRAMEWORK PHASE 1 FOR THIS QUESTION]

**Gated Access (GA)**

The following ***possible*** requirements address the charter question on Gated Access (GA): *What steps should be taken to control data access for each user/purpose?****Possible*** requirements for WG deliberation include:

**[GA-D1-R1]** –“gTLD registration data must be collected, validated, and disclosed for permissible purposes only, with some data elements being accessible only to authenticated requestors that are then held accountable for appropriate use.” (Permissible Purpose Principle 6 on page 31, relevant to both UP and GA Questions)

**[GA-D1-R2]** –“Every Registrant must have the ability to access all public and gated information published in the [gTLD registration directory services] about their domain name, including designated contact data.” (Permissible Purpose Principle 7 on page 31, relevant to both UP and GA Questions)

**[GA-D1-R3]** –To maximize Registrant privacy, Registrant-supplied data must be gated by default, except where there is a compelling need for public access that exceeds resulting risk.

**[GA-D1-R4]** – Registrants can opt into making any gated Registrant-supplied data public with informed consent. (Data Disclosure Principle 35 on page 45)

**[GA-D1-R5]** – gTLD registration directory services must make data accessible only in conformance with specified Data Access Principles (41-55 on pages 58-61), as follows:

**[GA-D1-R6]** – A minimum set of data elements, at least in line with the most stringent privacy regime, must be accessible by unauthenticated users.

**[GA-D1-R7]** – Multiple levels of authenticated data access must be supported, consistent with stated permissible purposes.

**[GA-D1-R8]** – gTLD registration directory services user access credentials must be tied to an auditable accreditation process.

**[GA-D1-R9]** – Access must be non-discriminatory (i.e., the process must create a level playing field for all requestors, within the same purpose).

**[GA-D1-R10]** – The gTLD registration directory service must deter misuse and promote accountability:

**[GA-D1-R11]** –All gTLD registration data element access must be based on a stated purpose;

**[GA-D1-R12]** –Access to gated data elements must be limited to authenticated requestors that assert a permissible purpose; and

**[GA-D1-R13]** –Requestors must be able to apply for and receive credentials for use in future authenticated data access queries.

**[GA-D1-R14]** – Some type of accreditation must be applied to requestors of gated access to gTLD registration data:

**[GA-D1-R15]** –When accredited Requestors query data, their purpose must be stated every time a request is made.

**[GA-D1-R16]** –Different terms and conditions may be applied to different purposes.

**[GA-D1-R17]** –If accredited requestors violate terms and conditions, penalties must apply.

**[GA-D1-R18]** – To raise the standard of gTLD registration data protection, all directory services queries/responses must make use of commonly-available message encryption and authentication measures to protect the confidentiality and integrity of data in transit.

**[GA-D1-R19]** – To meet the needs of authenticated users with permissible purposes, the gTLD registration directory must provide a Reverse Query service that searches public and gated data elements for a specified value and returns a list of all domain names that reference that value.

**[GA-D1-R20]** – To meet the needs of authenticated users with permissible purposes, the directory service must provide a WhoWas service that returns historical snapshots of public and gated data elements for specified domain names, limited to the historical data available.

**[GA-D1-R21]** – The gTLD registration directory service must support innovative services that make use of gTLD registration data elements, as follows.

**[GA-D1-R22] -** Third parties must be able to provide existing and future innovative services – including Reverse Queries and WhoWas – using public data elements and held to terms and conditions of gTLD registration data use.

**[GA-D1-R23]** In the event that third parties offer innovative services involving gated data elements, those third parties must be accredited and held to terms and conditions of gTLD registration data use.

**[GA-D1-R24]** – All disclosures of gated data elements must occur through defined gTLD registration directory service access methods (including those described above). The entire registration data set for all gTLDs (or the entire Registry data set for a single gTLD) must not be exported in bulk form for uncontrolled access.

**[GA-D1-R25]** – Disclosures may occur through interactive display and other gTLD registration directory service access methods.

**[GA-D1-R26]** – To make data easier to find and access in a consistent manner, a central point of access (e.g., web portal) must be offered.

**[GA-D1-R27]** – Secure access to public gTLD registration data must be available to all requestors through an unauthenticated query method (at minimum, via secure website).

**[GA-D1-R28]** – Secure access to gated gTLD registration data must be supported through secure web and other access methods and formats based on authenticated requestor and purpose.

**[GA-D1-R29]** – Requestors must be able to obtain authoritative data from the gTLD registration directory service in real-time when needed.

**[GA-D1-R30]** – The gTLD registration directory service must accommodate automation for large-scale lookups for various use cases and permissible purposes.

**[GA-D1-R31]** – To be truly global, the gTLD registration directory service must accommodate the display of registration data in multiple languages, scripts and character sets, including Internationalized domain names (IDNs).

**[GA-D1-R32]** – The gTLD registration directory service should support all future GNSO-defined transliteration policies for gTLDs.

**[GA-D1-R33]** – The gTLD registration directory service should enable collection and display of registration data elements in local languages.

**[GA-D1-R34]** – “All access must be purpose-based, returning only data elements permitted for the stated purpose.” (bottom of p.62)

**[GA-D1-R35]** – “. . for each [gTLD registration directory services] user community identified [under the Charter question on Users/Purposes] desiring access to gated data for permissible purposes, community experts must be consulted to confirm EWG-identified registration data purposes, the data elements that must be accessible for that purpose, and ***possible*** User Accreditors.” (top of p.63)

**[GA-D1-R36]** – “Non-accredited, unauthenticated access to non-gated (i.e., public) data must be possible in real-time.”

**[GA-D1-R37]** – “Accreditation of [gTLD registration directory service] users for access to [registration data] does not have to happen in real-time for all use cases and/or requesters.”

**[GA-D1-R38]** – “[gTLD registration directory services] must only apply the minimum accreditation scheme necessary to provide users access to gated data elements for the stated purpose.”

**[GA-D1-R39]** – “There must be no requirement to pre-approve or provide credentials to every potential user of [gTLD registration directory services.] A request and fulfilment process can be created for each type of accredited user (i.e., [gTLD registration directory services] user community).”

**[GA-D1-R40]** – Accreditation for [gTLD registration directory services] users seeking access to data for permissible purposes could be granted in various ways as determined by data access policy. For example, None (i.e., unauthenticated access to public data only), self-accreditation by the person/entity requesting the data, or accreditation by some trusted third party.

**[GA-D1-R41]** – Whenever possible, any third party accreditation process must leverage existing accreditation processes within each user community that needs credentialing.

**[GA-D1-R42]** – “Third party accreditation processes must be vetted by an authority responsible for implementing and enforcing [gTLD registration directory services] user accreditation policy (for example, ICANN, a multistakeholder panel) and reviewed on a periodic basis.”

**[GA-D1-R43]** – “Any organization serving as a [gTLD registration directory service] user accreditor must have a signed agreement with ICANN and/or the registration directory service provider to offer such accreditation processes under agreed-upon guidelines, and establish a framework to allow for due process, accountability, security, fair access, and adherence to applicable law.”

**[GA-D1-R44]** – Accreditors must take on defined sets of responsibilities, such as establishing criteria for membership, setting credentialing requirements, defining and enforcing terms and conditions of membership, providing functions such as user account creation, credential issuance, suspension and revocation, lifecycle user account management, and associated processes such as dispute handling and ToC enforcement.

**[GA-D1-R45]** – Accreditors that wish to participate in handling gTLD registration directory services requests for data on behalf of their members must be able to do so in ways that enable auditing and abuse complaint resolution and hold parties responsible for compliant usage and accountable in the event of abuse.

**[GA-D1-R46]** – [gTLD registration directory services] must provide real-time access to credentialed requestors via multiple methods. Access credentials issued during accreditation must be suitable for use with all defined access methods.

**[GA-D1-R47]** – “Best practices may be defined for credential management; Accreditors must be expected to adhere to best practices.”

**[GA-D1-R48]** – gTLD registration directory services “must require individual credentials for authenticated access.”

**[GA-D1-R49]** – “Authenticated access [to gTLD registration data] must not be transitive (i.e., an authenticated user shall not share gated data with others outside of its accreditation).”

**[GA-D1-R50]** – “A process for responsible revelation of gated data to further the original purpose it was requested for must be created and enforced.”

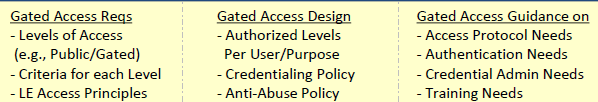
**[GA-D1-R51]** – “An organization seeking access to [gTLD registration] data must be able to apply for user accreditation and have all people using the registration directory service in their organization covered by that one accreditation, [accepting responsibility] for managing accredited access within its own organization.”

**[GA-D1-R52]** –“Audits and data analytics must be used to identify abuse of the system and access credentials.”

**[GA-D1-R53]** – “An appeals process must be defined to allow [gTLD registration directory services] users to refute abuse allegations when seeking to reactive/reinstate access credentials.”

**[GA-D1-R54]** – “Every Registrant must receive a credential to be able to examine their own contact data as stored by the [gTLD registration directory service] in relation to domain names that are registered to them.”

**[GA-D1-R55]** – “A process for adding additional accreditors that either supplement current processes or offer new, innovative ways to provide user accreditation for approved purposes of the [gTLD registration directory service] must be established.”

See Additional Key Inputs for this charter question ([hyperlinked on this Wiki page](https://community.icann.org/display/gTLDRDS/Gated+Access+-+Key+Inputs)) which may be consulted as a potential source of ***possible*** requirements. The PDP WG may also identify additional sources by themselves or through community outreach.   
[CHECK FOR ALIGNMENT WITH PROCESS FRAMEWORK PHASE 1 FOR THIS QUESTION] 

**Data Accuracy (DA)**

The following ***possible*** requirements address the charter question on Data Accuracy (DA): *What steps should be taken to improve data accuracy?*   
***Possible*** requirements for WG deliberation include:

**[DA-D1-R1]** –“Standard validation [must be applied] to all gTLD registration data. In addition to periodic checks, validation would occur at the time of collection, with an option to pre-validate blocks of contact data for reuse in multiple domain name registrations.” (top of p.69)

**[DA-D1-R2]** –“The [gTLD registration directory services] ecosystem must include a pre-validated Contact Directory, conceptually separate from the Domain Name Directory, to promote the quality and reusability of data elements used to contact domain name Registrants and people or organizations that can be designated by Registrants as contacts for various purposes associated with a domain name registration, and to deter the fraudulent use of personal data.” (top of p.69)

**[DA-D1-R3]** – [gTLD registration directory services must support a] Pre-validation process (Section b on pp.71-72)

**[DA-D1-R5]** –[gTLD registration directory services must support an] Accuracy, Audit & Remediation Process (Section c on pp. 72-73)

**[DA-D1-R6]** –[gTLD registration directory services must include an] Operational Framework for Contact IDs (Section d on pp. 74-75)

**[DA-D1-R7]**–[gTLD registration directory services must have specified] Principles for Interaction between Contact Holders & Validators 83-89 (pp. 75-76)

**[DA-D1-R8]**–[To create and maintain] any given Contact, a Contact Holder may choose any Validator.

**[DA-D1-R9]**–Oversight and accountability policies related to the management of Contacts must be developed.

**[DA-D1-R10]**–Contact Holders must be able to modify the contact information…through the issuing Validator.

**[DA-D1-R11]**–Validators must use Contact Holder authentication to deter unauthorized modification of contact information. Validators may offer multiple levels of Contact Holder authentication.

**[DA-D1-R12]**–Contact Holders must be able to choose providers based on cost/benefit propositions tied to ease-of-use, security, costs, and other logical business factors.

**[DA-D1-R13]**–Validators must publish their policies on authentication in a manner that can be utilized globally for reputation management [to] encourage better accuracy and accountability.

**[DA-D1-R14]**–Validators must be able to validate contact information submitted in the Contact Holder’s native language [to] improve accuracy of native-language data and support scalability of the domain name registration system into a multi-lingual environment.

**[DA-D1-R15]** –[gTLD registration directory services must have specified] Principles for Contact Validation 90-104 (pp.76-78)

**[DA-D1-R16]** –All contact data elements must be validated at a syntactic level. This represents a base-level of validation that must be achievable by any entity in the industry.

**[DA-D1-R17]** –All mandatory contact data elements for a particular purpose must be validated operationally before that contact can be included in domain name registration data for that purpose.

**[DA-D1-R18]** –A Contact Holder must be able to voluntarily seek optional higher levels of validation (e.g., optional identity validation), bearing associated costs in return for perceived benefits (e.g., greater consumer confidence in domain names registered to identity-validated entities).

**[DA-D1-R19]** –Given costs involved with optional identity validation, a low-cost mechanism for economically disadvantaged Contact Holders to receive optional identity validation is desirable.

**[DA-D1-R20]** –In order to preserve associations and allow for a correction process, contact data can have a status of “inaccurate” and remain in the system.

**[DA-D1-R21]** –Validation Status of contact data must be tracked and published as appropriate [in the registration directory service], along with the most recent time the validation status was determined.

**[DA-D1-R22]** –Third parties may file inaccuracy reports to challenge the Validation Status of contact data, triggering a standard remediation process that may result in the contact being flagged as “inaccurate” and in further consequences for domain names using that contact data.

**[DA-D1-R23]** –Active domains cannot have a mandatory contact with an “inaccurate” status without some sort of remediation.

**[DA-D1-R24]** –A minimum level of cross-field validation must be checked for all contact data elements associated with contacts where cross-field validation is applicable (e.g. physical address).

**[DA-D1-R25]** –Revalidation of contact data must be carried out on a regular basis to ensure data is accurate at the declared level.

**[DA-D1-R26]** –If a Contact Holder provides optional data elements, those elements must be at least syntactically validated. Optional data elements must not be validated beyond syntax unless the Contact requests and presumably pays for any costs associated with such validation.

**[DA-D1-R27]** –The level of validation achieved beyond syntactical validation for data elements that can be operationally- or (optionally) identity-validated must be recorded and maintained by the Validator.

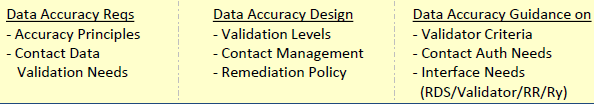
**[DA-D1-R28]** –The Validator must determine and publish [in the gTLD registration directory service] the overall validation status achieved by each contact.

**[DA-D1-R29]** –For any data element that has undergone validation, the timestamp of that validation must also be recorded and maintained.

**[DA-D1-R30]** –[gTLD registration directory services must offer an optional] Unique Contact Data Capability (Section g on p.78)

**[DA-D1-R31]** – “To allow for much greater accuracy across such a diverse space and ease-of-use for such contacts, it is desirable to provide mechanisms to allow easy use of such contacts by multiple Registrants; for example, a web hosting company providing their NOC’s unique ID for “technical” and “abuse” contacts for domains controlled by their customers.” (Bottom of p.69) [Also included as a possible Benefits requirement]

**[DA-D1-R32]** – “. . when such an entity needs to update their contact information to reflect a new address/phone number or a merger/acquisition, it must be easy to update that information in one place and have that reflected to all domains associated with that contact data set (as designated by a unique identifier).” (Top of p.70) [Also included as a possible Benefits requirement]

See Additional Key Inputs for this charter question ([hyperlinked on this Wiki page](https://community.icann.org/display/gTLDRDS/Data+Accuracy+-+Key+Inputs)) which may be consulted as a potential source of ***possible*** requirements. The PDP WG may also identify additional sources by themselves or through community outreach.   
[CHECK FOR ALIGNMENT WITH PROCESS FRAMEWORK PHASE 1 FOR THIS QUESTION] 

**Data Elements (DE)**

The following ***possible*** requirements address the charter question on Data Elements (DE): *What data should be collected, stored, and disclosed?*   
***Possible*** requirements for WG deliberation include:

**[DE-D1-R1]** –The [gTLD registration directory service] must accommodate purpose-driven disclosure of data elements.

**[DE-D1-R2]** – Not all [gTLD registration] data collected is to be public; disclosure must depend upon Requestor and Purpose.

**[DE-D1-R3]** – Public access to an identified minimum data set must be made available [by the gTLD registration directory service], including contact data published expressly to facilitate communication for this purpose.

**[DE-D1-R4]** – Data Elements determined to be more sensitive (after conducting the risk & impact assessment) must be protected by gated access, based upon:

• Identification of a permissible purpose,

• Disclosure of requestor/purpose, and

• Auditing/Compliance to ensure that gated access is not abused.

**[DE-D1-R5]** – Only the data elements permissible for the declared purpose must be disclosed (i.e., returned in responses or searched by Reverse and WhoWas queries).

**[DE-D1-R6]** – The only [gTLD registration] data elements that must be collected are those with at least one permissible purpose.

**[DE-D1-R7]** – Each [gTLD registration] data element must be associated with a set of permissible purposes.

**[DE-D1-R8]** – An initial set of acceptable uses, permissible purposes, and data element needs are identified [by possible requirements for Users/Purposes.]

**[DE-D1-R9]** – Each permissible purpose must be associated with clearly-defined data element access and use policies.

**[DE-D1-R10]** – An on-going review process must be defined to consider proposed new purposes and periodically update permissible purposes to reflect approved additions, mapping them to existing data elements.

**[DE-D1-R11]** – A Policy Definition process must be defined to consider proposed new data elements and, when necessary, update defined data elements, mapping them to existing permissible purposes.

**[DE-D1-R12]** – The list of minimum data elements to be collected, stored and disclosed must be based on known [permissible purpose] use cases and a risk assessment.

**[DE-D1-R13]** – In support of the overarching legal principles (see Privacy Question), Registrars and Validators should afford domain name Registrants and purpose-based contacts the opportunity, at the time of data collection, to consent to the use of their data for pre-disclosed permissible purposes, in accordance with the data protection laws of their jurisdiction. In formulating the policy, this principle must be addressed in the broader context of these overarching legal principles.

**[DE-D1-R14]** – To meet basic domain control needs, it must be mandatory for Registries and Registrars to collect and Registrants to provide the following data elements when a domain name is registered:

a. Domain Name

b. DNS Servers

c. Registrant Name

d. Registrant Type

Indicates the kind of entity identified by Registrant Name, for use in applying registration data requirements (e.g., undeclared, privacy/proxy provider, legal person, natural person –further described on pp 42-43)

e. Registrant Contact ID

A unique ID assigned to each Registrant Contact [Name+Address] during validation

f. Registrant Postal Address

Includes Street, City, State/Province, Postal Code, Country (as applicable)

g. Registrant Email Address

h. Registrant Phone

Includes the following data elements: Number, Extension (when applicable)

**[DE-D1-R15]** – To improve both Registrant privacy and contactability, Registrars must collect and Registrants must provide purpose-based contacts for every registered domain name.

**[DE-D1-R16]** – Registrants may optionally designate Privacy/Proxy-supplied contacts or authorized third party contacts for specified permissible purposes.

**[DE-D1-R17]** – To meet the communication needs associated with each permissible purpose, contacts created through a Validator and subsequently associated with a domain name must satisfy minimum mandatory data element requirements.

**[DE-D1-R18]** – If a Registrant does not designate a contact for each mandatory permissible purpose, the Registrant’s own contact data must be used by default. (Note that the Registrant can avoid this by using an accredited Privacy/Proxy service, or by designating other contacts.

**[DE-D1-R19]** – To avoid collecting more data than necessary, all other Registrant-supplied data not enumerated above and used for at least one permissible purpose must be optionally collected at the Registrant’s discretion. Validators, Registries and Registrars must allow for this data to be collected and stored if the Registrant so chooses.

**[DE-D1-R20]** – To maximize Internet stability, the following mandatory data elements must be provided by Registries and Registrars:

a. Registration Status

b. Client Status (Set by Registrar)

c. Server Status (Set by Registry)

d. Registrar

e. Registrar Jurisdiction

f. Registry Jurisdiction

g. Registration Agreement Language

h. Creation Date

i. Registrar Expiration Date

j. Updated Date

k. Registrar URL

l. Registrar IANA Number

m. Registrar Abuse Contact Phone Number

n. Registrar Abuse Contact Email Address

o. URL of Internic Complaint Site

**[DE-D1-R21]** – For TLD-specific data elements, the TLD Registry must establish and publish a data collection policy (consistent with these over-arching principles) and be responsible for any validation of those TLD-specific data elements.

**[DE-D1-R22]** – Validators, Registries and Registrars may collect, store, or disclose additional data elements for internal use that is never shared with the [gTLD registration directory service].

**[DE-D1-R23]**  To maximize Registrant privacy, Registrant-supplied data must be gated by default, except where there is a compelling need for public access that exceeds resulting risk. Registrants can opt into making any gated Registrant-supplied data public with informed consent.

**[DE-D1-R24]** – To maximize Internet stability, all Registry or Registrar-supplied registration data must be always public, except where doing so results in unacceptable risk. Registrants can opt into making any public Registry/Registrar-supplied data gated, except as noted below to enable basic domain control.

**[DE-D1-R25]** – To maximize reachability, all purpose-based contacts must be public by default. Contact Holders can opt into making any contact data element gated, except [for data elements] required to satisfy the designated purpose.

**[DE-D1-R26]** – To meet basic domain control needs, the following Registrant-supplied data, which is mandatory to collect and low-risk to disclose, must be included in the minimum public data set:

a. Domain Name

b. DNS Servers

c. Registrant Type

d. Registrant Contact ID

e. Registrant Email Address

f. Tech Contact ID

g. Admin Contact ID

h. Legal Contact ID

i. Abuse Contact ID

j. Privacy/Proxy Provider Contact ID

(mandatory only if Registrant Type = Privacy/Proxy Provider)

k. Business Contact ID

(mandatory only if Registrant Type = Legal Person)

**[DE-D1-R27]** – To balance simplicity and reachability, if a Registrant does not supply a mandatory purpose-based contact, the Registrant must be informed that [Registrant data elements] will be used [for that purpose]. The Registrant can avoid this disclosure by specifying one or more third party contacts or by using an accredited Privacy/Proxy service.

**[DE-D1-R28]** – For TLD-specific data elements, the TLD Registry must establish and publish a data disclosure policy (consistent with these over-arching principles) and be responsible for identifying permissible purposes for any gated TLD-specific data elements.

**[DE-D1-R29]** –[gTLD registration directory services] must be expandable in the future to support “multiple contacts specified for each type of purpose-based contact, allowing direct contact with specific individuals with critical responsibilities.”

**[DE-D1-R30]** –All purpose-based contacts “must be aware of and agree to fulfill the designated role(s) for each registered domain name.” (p.39)

**[DE-D1-R31 ]** –Each contact’s approval must be obtainable in a scalable, real-time or near real-time manner to avoid delaying domain name registrations or domain name updates.

**[DE-D1-R32]** – Policies and processes must prevent unauthorized use of contact data.

**[DE-D1-R33]** – Either the designated contact or the Registrant must be able to rescind approval at a later time.

**[DE-D1-R34]** – Registrants must be able to easily designate themselves as contacts for their domain names without external/third party approval.

**[DE-D1-R35]** – Contact management must be feasible separately from domain management, allowing contact portability and accountability separate from domain names and controlled by the actual individuals or entities listed under such contacts.

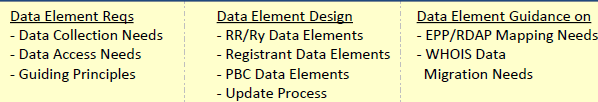
**[DE-D1-R36]** – Contacts must be managed using Validators who manage contact databases, implement validation regimes, and maintain information on the level of validity for the contact and its data elements (accessible through the [gTLD registration directory service]).

**[DE-D1-R37]** – Domain registrations may be associated with Contact IDs designated by their Registrants and approved by such designated contacts for various purposes associated with a domain name.

**[DE-D1-R38]** – Such contacts must contain valid mandatory data elements. Policies and oversight will be needed to manage these processes to ensure that Contact IDs are not used without contact’s authorization and meet minimum standards.

**[DE-D1-R39]** – Change management and authorization of use of contact information is controlled by the Contact Holder and affects all domains associated to a contact. Processes and policies to ensure accurate, authentic, and timely implementation of desired changes without burdening contacts or Registrants must be developed to support this new paradigm.

**[DE-D1-R40]** – Each individual block of contact data must have a Contact ID which uniquely identifies both the Validator and the Contact Holder to enable retrieval and update of associated contact data. This Contact ID must be published in any public display of [registration] data.

See Additional Key Inputs for this charter question ([hyperlinked on this Wiki page](https://community.icann.org/display/gTLDRDS/Data+Elements+-+Key+Inputs)) which may be consulted as a potential source of ***possible*** requirements. The PDP WG may also identify additional sources by themselves or through community outreach.   
[CHECK FOR ALIGNMENT WITH PROCESS FRAMEWORK PHASE 1 FOR THIS QUESTION] 

**Privacy (PR)**

The following ***possible*** requirements address the charter question on Privacy (PR): *What steps are needed to protect data and privacy?* ***Possible*** requirements for WG deliberation include:

**[PR-D1-R1]** – “. . . in some jurisdictions, privacy rights extend to legal persons and to entities with respect to free speech and freedom of association.” (Next to last paragraph on p.81)

**[PR-D1-R2]** – As described under Option (2) of the Summary of Data Protection Mechanisms Considered table on p.85 with further description on p.86, a basic ICANN privacy policy for gTLD registration directory services must] be drafted, based on standard best practices for privacy protection, and standard contractual clauses [must] be developed which give effect to this policy throughout the [registration directory services] ecosystem. Standard clauses could be included in all contracts between ICANN and all ecosystem actors engaged in data transfers, ensuring a sufficiently high level of data protection to permit unfettered transfer within this ecosystem.

**[PR-D1-R3]** –The gTLD registration directory service must comply with a defined “policy using standard contractual clauses that are harmonized with data protection laws to implement the requirements of the policy, and ensure through various audit mechanisms that these privacy protections are enforced through contracts between all ecosystem actors involved in handling personal information.” (pp.86-87)

**[PR-D1-R4]** –As described under Options (1) & (2) in the Summary of Data Protection Implementations Considered table on pages 87-88, gTLD registration directory services must protect data elements:

**[PR-D1-R5]** –Provide for legal compartmentalization by tagging data elements according to the applicable law for the data subject and treating that that data accordingly by applying those law(s) to each specific transfer.

**[PR-D1-R6]** –Select location(s) for gTLD registration data storage where the applicable national data protection law provides for a high level of protection.

**[PR-D1-R7]** –Mechanisms must be adopted to facilitate routine legally compliant data collection and transfer between actors within the [gTLD registration directory services] ecosystem.

**[PR-D1-R8]** –Standard contract clauses that are harmonized with privacy and data protection laws should be codified in a policy and enforced through contracts between all ecosystem actors involved in handling personal information.

**[PR-D1-R9]** –An information system to apply data protection laws and localization of data storage must be considered as two means of implementing the high level of data protection required. This must be ensured through standard contractual clauses, which flow from a logical privacy policy for the ecosystem.

**[PR-D1-R10]** –Summary of Law Enforcement Access Options Considered Option (1) on page 89; “In addition, for option (1), it has to be ensured that the legal framework for national law enforcement in jurisdiction(s) where registration data is stored does not override the framework established for the gTLD registration directory service. The geography of data localisation is therefore critically important.”

**[PR-D1-R11]** –Law Enforcement Access Principle 108: “[gTLD registration data] must [be] stored in jurisdiction(s) where law enforcement is globally trusted, regardless of implementation model.” (p.90)

**[PR-D1-R12]** – The following overarching legal principles normally found in data protection law must be considered when drafting policies and implementation processes for gTLD registration directory services:

* Personal data must be:

**[PR-D1-R13]** –processed lawfully, fairly and in a transparent manner in relation to the data subject,

**[PR-D1-R14]** –collected for specific, explicit and legitimate purposes and not further processed in a way incompatible with those purposes,

**[PR-D1-R15]** –adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed, and

**[PR-D1-R16]** –accurate and kept up-to-date as required for the specified purposes.

* Lawful processing, including transfer and disclosure can be – subject to the relevant jurisdiction – based on:

**[PR-D1-R17]** – consent of the data subject,

**[PR-D1-R18]** – the necessity for the performance of a contract to which the data subject is party, and

**[PR-D1-R19]** – the necessity for compliance with a legal obligation to which the controller is subject.

**[PR-D1-R20]** – A right of access to information and a right to rectify inaccuracy for the data subject have to be ensured.

**[PR-D1-R21]** –In addition to the privacy afforded by compliance with data protection laws, the [gTLD registration directory services] ecosystem must accommodate needs for privacy by including:

• An accredited Privacy/Proxy Service for general personal data protection and adherence to local privacy law; and

• An accredited Secure Protected Credentials Service for persons at risk, and in instances where free-speech rights may be denied or speakers persecuted.

**[PR-D1-R22]** –There must be accreditation for Privacy/Proxy service providers and rules regarding the provision and use of accredited Privacy/Proxy services. *[Note: See PPSAI PDP Final Report for GNSO consensus policy on accreditation of Privacy/Proxy service providers developed after the EWG Report was published.]*

**[PR-D1-R23]** –Outside of domain names registered via accredited Privacy/Proxy services, all Registrants must assume responsibility for the domain names they register.

**[PR-D1-R24]** –ICANN must investigate the development of a single, harmonized privacy policy which governs [gTLD registration directory services] activities in a comprehensive manner, as discussed on pp 96-97.

**[PR-D1-R25]** – ICANN must accredit Privacy and Proxy service Providers. At minimum, the accreditation program must continue the Privacy/Proxy commitments under the 2013 RAA Specification.

**[PR-D1-R26]** – Entities and natural persons may register domain names using accredited Privacy services that do not disclose the Registrant’s contact details except in defined circumstances (e.g., terms of service violation, subpoena).

**[PR-D1-R27]** – ICANN must require specific terms to be included in the terms of service. The terms of service must include requiring the service provider to endeavor to provide notice in cases of expedited take-downs.

**[PR-D1-R28]** – Accredited Privacy services must provide the Registrar with accurate and reliable contact details for all mandatory Purpose-Based Contacts, in order to reach the Privacy service provider and entities authorized to resolve technical, administrative, and other issues on behalf of the Registrant.

**[PR-D1-R29]** – Accredited Privacy services must be obligated to relay emails received by the Registrant’s forwarding email address to the Registrant.

**[PR-D1-R30]** – Entities and natural persons may register domain names using accredited proxy services that register domain names on behalf of the Proxy service customer.

**[PR-D1-R31]** – Accredited Proxy service providers must provide the Registrar with their own Registrant name and contact details, including a unique forwarding email address to contact the entity authorized to register the domain name on behalf of the Proxy service customer.

**[PR-D1-R32]** – As the registered name holder, accredited proxy service providers must assume all the usual Registrant responsibilities for that domain name, including provision of accurate and reliable mandatory Purpose-Based Contacts and other registration data.

**[PR-D1-R33]** – Accredited Proxy services must provide the Registrar with accurate and reliable contact details for all mandatory Purpose-Based Contacts, in order to reach the Proxy service provider and entities authorized to resolve technical, administrative, and other issues on behalf of the Proxy service customer.

**[PR-D1-R34]** –Accredited Proxy services must be obligated to relay emails received by the Registrant’s forwarding email address.

**[PR-D1-R35]** –Accredited Proxy services must be obligated to respond to reveal requests in a timely manner as outlined in the escalation procedures.

**[PR-D1-R36]** –The six key functions listed on pages 104-105 must be developed to provide enhanced security to at-risk entities. These functions include:

* A process to establish criteria for at-risk entity eligibility.
* Application forms, attestations, and financial systems to protect identities of at-risk entities.
* An independent review board to evaluate and approve applications.
* Trusted parties willing to relay secure protected credentials.
* Accredited proxy service providers willing to accept secure protected credentials.
* Policies surrounding expedited takedown procedures and other DNS abuse mitigations.

**[PR-D1-R37]** –“Secure Protected Credentials (must) be developed for limited use and after ensuring entities availing themselves of the service do indeed have legitimate need for anonymity.” (1st paragraph on p.106)

**[PR-D1-R38]** –“Information generated from the actual use of a domain name must be the responsibility of the entities applying for and using secure credential-registered domain names, and it may be important to provide information underscoring this risk.” (2nd paragraph on p.106)

**[PR-D1-R39]** – Individuals and groups who can demonstrate that they would be at risk if identified must be able to anonymously apply for and receive domain names registered using secure credentials, aided by attestors and trusted third parties to provide a shield between at-risk entities and Registrars/Validators.

**[PR-D1-R40]** – ICANN must facilitate the establishment of an independent trusted review board that will validate claims of at-risk organizations or individuals to approve (and when necessary, revoke) credentials. Such an organization – referred to herein as a Secure Credential Approver (SCA) -- might develop other services, such as educating users about risks and safe Internet practices.

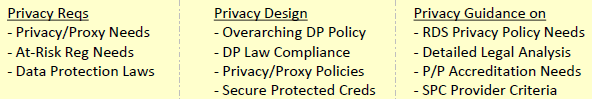
**[PR-D1-R41]** – ICANN must facilitate the development or licensing of a Secure Credential Issuer that recognizes SCA approvals and generates corresponding Secure Credentials.

**[PR-D1-R42]** – The Secure Credential Approver must use issued Secure Credentials to license domain names from accredited Proxy Service Providers in the usual manner. Information of the proxy service provider will appear in the gTLD registration directory service. No data about the at-risk entity using the secure credential-registered domain name would be known to the registration directory service, and some system of anonymous or proxy payment would have to be used.

**[PR-D1-R43]** – Domain names registered using secure protected credentials must follow regular accredited Privacy/Proxy service provider reveal and take-down procedures. Failure of the Privacy/Proxy customer (i.e., the Secure Credential Approver) to respond in a timely manner, or evidence of DNS abuse, could result in expedited take-down of secure credential-registered domain names.

**[PR-D1-R44]** – Recognizing that domain names registered using secure protected credentials might be at risk themselves for cyberattack, or that investigation of offences would be difficult, heightened security monitoring of these domain names must be considered to mitigate risk.

**[PR-D1-R45]** – Policies and processes must be established for secure protected credential application approval and revocation.

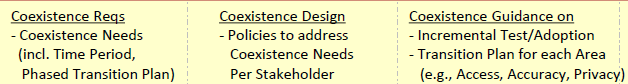
See Additional Key Inputs for this charter question ([hyperlinked on this Wiki page](https://community.icann.org/display/gTLDRDS/Privacy+-+Key+Inputs)) which may be consulted as a potential source of ***possible*** requirements. The PDP WG may also identify additional sources by themselves or through community outreach.   
[CHECK FOR ALIGNMENT WITH PROCESS FRAMEWORK PHASE 1 FOR THIS QUESTION] 

**[THE FOLLOWING SECTIONS HAVE NOT YET BEEN COMPLETED. IT IS EXPECTED THAT THE WG WILL FOCUS INITIALLY ON POSSIBLE REQUIREMENTS TO ADDRESS FUNDAMENTAL QUESTIONS. HOWEVER, CROSS-CUTTING QUESTIONS HAVE ALSO BEEN INCLUDED BELOW AS PLACE-HOLDERS TO BE EXPANDED LATER AND TO ALLOW FOR POSSIBLE REQUIREMENTS TO BE MOVED OR ADDED.]**

**Coexistence (CX)**

The following **possible** requirements address the charter question on Coexistence (CX):   
*What steps should be taken to enable next-generation RDS coexistence with & replacement of the legacy WHOIS system?* **Possible** requirements for WG deliberation include:

**[CX-D1-Rx]** –Draw from Section 5a, Alignment with 2013 RAA and New Data Elements, and Annex F, System Models – Ease of Transition. [TO DO – COPY/PASTE possible requirements from this section HERE]

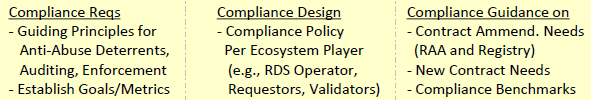
See Additional Key Inputs for this charter question ([hyperlinked on this Wiki page](https://community.icann.org/pages/viewpage.action?pageId=56986720)) which may be consulted as a potential source of ***possible*** requirements. The PDP WG may also identify additional sources by themselves or through community outreach.   
[CHECK FOR ALIGNMENT WITH PROCESS FRAMEWORK PHASE 1 FOR THIS QUESTION] 

**Compliance (CM)**

The following ***possible*** requirements address the charter question on Compliance (CM): *What steps are needed to enforce these policies?* ***Possible*** requirements for WG deliberation include:

**[CM-D1-Rx]**– Draw from Contractual Relationship Principles 109-113 on page 91  
[TO DO – COPY/PASTE EWG Principles 109-113 HERE]

**[CM-D1-Rx]** – Draw from Accountability & Audit Principles 114-133 on pages 91-94. See also summary of types of accountability and audit requirements in Table 6 on page 95.  
[TO DO – COPY/PASTE EWG Principles 114-133 HERE]

See Additional Key Inputs for this charter question ([hyperlinked on this Wiki page](https://community.icann.org/display/gTLDRDS/Coexistence+-+Key+Inputs)) which may be consulted as a potential source of ***possible*** requirements. The PDP WG may also identify additional sources by themselves or through community outreach.   
[CHECK FOR ALIGNMENT WITH PROCESS FRAMEWORK PHASE 1 FOR THIS QUESTION] 

**System Model (SM)**

The following ***possible*** requirements address the charter question on System Model (SM): *What system requirements must be satisfied by any next-generation RDS implementation?*   
***Possible*** Requirements for WG deliberation include:

**[SM-D1-R1]** –The gTLD registration directory service “must be designed with extensibility in mind” (p.27)

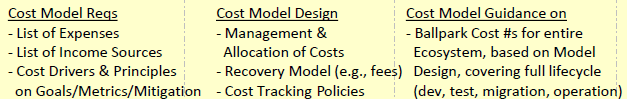
**[SM-D1-R2]** –gTLD registration directory service must “log all access to gTLD registration data, including unauthenticated access to public data elements, and access restrictions to deter bulk harvesting.” (p.40)

**[SM-D1-R3]** –gTLD registration directory service must “audit both public and gated data access to minimize abuse and impose penalties and other remedies for inappropriate use.” (p.40)

**[SM-D1-R4]** – Draw from Model Design Principles 157, 159 & 160 on page 109  
[TO DO – COPY/PASTE EWG Principles 157, 159 & 160 HERE]

**[SM-D1-R7]**– Draw from Data Storage, Escrow & Logging Principles 161-174 on pages 115-116  
[TO DO – COPY/PASTE EWG Principles 161-174 HERE]

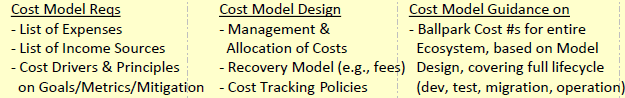
**[SM-D1-R21]** – Draw from Protocol Extensions &/or Additions on page 157  
[TO DO – TURN THIS INPUT INTO A POSSIBLE REQUIREMENT]

See Additional Key Inputs for this charter question ([hyperlinked on this Wiki page](https://community.icann.org/display/gTLDRDS/Compliance+-+Key+Inputs)) which may be consulted as a potential source of ***possible*** requirements. The PDP WG may also identify additional sources by themselves or through community outreach.   
[CHECK FOR ALIGNMENT WITH PROCESS FRAMEWORK PHASE 1 FOR THIS QUESTION] 

**Cost (CS)**

The following ***possible*** requirements address the charter question on Cost (CS): *What costs will be incurred & how must they be covered?*   
***Possible*** requirements for WG deliberation include

**[CS-D1-Rx]**– Draw from Cost Principles 175-180 on page 117  
[TO DO – COPY/PASTE EWG Principles 175-180 HERE]

See Additional Key Inputs for this charter question ([hyperlinked on this Wiki page](https://community.icann.org/display/gTLDRDS/Compliance+-+Key+Inputs)) which may be consulted as a potential source of ***possible*** requirements. The PDP WG may also identify additional sources by themselves or through community outreach.   
[CHECK FOR ALIGNMENT WITH PROCESS FRAMEWORK PHASE 1 FOR THIS QUESTION] 

**Benefits (BE)**

The following ***possible*** requirements address the charter question on Benefits (BE): *What benefits will be achieved & how will they be measured?*   
***Possible*** Requirements for WG deliberation include:

**[BE-D1-R1]** –The gTLD registration directory service must provide these benefits:  
 [INSERT Key benefits listed in Section d on pages 67-68]

**[BE-D1-R2]** – “. . the provision of purpose-based contacts by Registrants must lead to significant improvements in reachability of appropriate contacts for various purposes and creates an incentive for Registrants to provide accurate information for those roles.

**[BE-D1-R3]** – Gated access to more sensitive data elements must reduce Registrant incentive to supply inaccurate data and increase Registrant accountability for data accuracy.” (Bottom of p.68)

**[BE-D1-R4]** –“Pre-validation of Registrant or other contact information [must result in measurable benefits, including]:

**[BE-D1-R5]** –Increase accuracy of contact information by utilizing pre-validation to check data prior to use for a new domain name and to promote consistent data across all registrations (reduces error and fraud);

**[BE-D1-R6]** –Avoid the need to validate Registrant or other designated contact data each time a Registrant registers a new domain name by performing validation once and then reusing that block of contact data for several domain registrations (simplifies the process and reduces work requirements); and

**[BE-D1-R7]** –Avoid delay in the processing of a domain registration, since validation has to take place at the time of registration.” (Section a on p.69)

**[BE-D1-R8]** – “To allow for much greater accuracy across such a diverse space and ease-of-use for such contacts, mechanisms [must be provided] to allow easy use of such contacts by multiple Registrants; for example, a web hosting company providing their NOC’s unique ID for “technical” and “abuse” contacts for domains controlled by their customers.” (Bottom of p.69)   
[Also included as a requirement for DA Question]

**[BE-D1-R9]** – “. . when an entity needs to update their contact information to reflect a new address/phone number or a merger/acquisition, it must be easy to update that information in one place and have that reflected to all domains associated with that contact data set” (Top of p.70) [Also included as a requirement for DA Question]

**[BE-D1-R10]** –The gTLD registration directory service must provide these benefits:  
[TO DO: INSERT Summary of Data Quality Key Benefits from Section h on pp. 79-80]

**[BE-D1-R11]** –The gTLD registration directory service must provide these benefits:   
[TO DO: INSERT Advantages from all of page 108]

**[BE-D1-R12]** – The gTLD registration directory service must provide benefits compared to Current Whois under the 2013 RAA, including… [TO DO: INSERT Section b, pp.118-119]

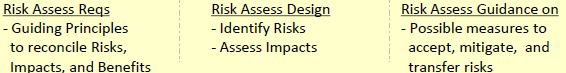
See Additional Key Inputs for this charter question ([hyperlinked on this Wiki page](https://community.icann.org/display/gTLDRDS/Benefits+-+Key+Inputs)) which may be consulted as a potential source of ***possible*** requirements. The PDP WG may also identify additional sources by themselves or through community outreach.   
[CHECK FOR ALIGNMENT WITH PROCESS FRAMEWORK PHASE 1 FOR THIS QUESTION] 

**Risks (RI)**

The following ***possible*** requirements address the charter question on Risks (RI): *What risks do stakeholders face & how will they be reconciled?*   
***Possible*** requirements for WG deliberation include:

**[RI-D1-R1]** – “A widely scoped risk/impact analysis [must be done] to confirm that these principle-based [data element] classifications do in fact result in appropriate collection and disclosure of data for defined purposes.” (p.56 & in Section c on pp.119-120)

[TO DO – ADD FURTHER REQUIREMENTS FROM RISK ANALYSIS SECTION?]

See Additional Key Inputs for this charter question ([hyperlinked on this Wiki page](https://community.icann.org/display/gTLDRDS/Risks+-+Key+Inputs)) which may be consulted as a potential source of ***possible*** requirements. The PDP WG may also identify additional sources by themselves or through community outreach.   
[CHECK FOR ALIGNMENT WITH PROCESS FRAMEWORK PHASE 1 FOR THIS QUESTION] 

**Other Questions (OQ)**

The following ***possible*** requirements would apply to a totally new next-generation RDS or a modification of the existing WHOIS system, but may not belong under any of the 11 charter questions. During deliberation, the WG may determine these ***possible*** requirements are in fact already covered under other questions, or the WG may decide that questions(s) should be added to the charter to fill gaps.

**[OQ-D1-R1]** – “Provides appropriate access to accurate, reliable, and uniform registration data” (p.7)

**[OQ-D1-R2]** – gTLD registration directory services must provide for “accountability for all parties involved in the disclosure and use of gTLD domain name registration data.” (p.10). [This can be done by:]

**[OQ-D1-R3]** – “Logging all access to gTLD registration data, including unauthenticated access to public data elements, to enable detection and mitigation of abuses; =

**[OQ-D1-R4]** – “Gating access to more sensitive data elements that would only be available to requestors who applied for and were accredited to receive gTLD registration data access, at the level appropriate for each user and stated purpose; and

**[OQ-D1-R5]** – “Auditing both public and gated data access to minimize abuse and impose penalties and other remedies for inappropriate use, in accordance with terms and conditions explicitly agreed upon by each requestor.”

**[OQ-D1-R6]** – A “centralized interface must enable appropriate requestors to access registration information across all gTLDs, including unauthenticated public data access and authenticated gated data access.” (p.14)

**Foundational Questions (FQ)**

This section contains possible answers provided by key inputs to the charter’s foundational questions:

* Is a new policy framework and next-generation RDS needed to address these requirements?
* If no, does the current WHOIS policy framework sufficiently address these requirements?
* If not, what revisions are recommended to the current WHOIS policy framework to do so?

[**FQ-D1]** – Abandon today’s Whois model: “The EWG unanimously recommends abandoning today’s WHOIS model of giving every user the same entirely anonymous public access to (often inaccurate) gTLD registration data.” (p.5)

**Annex A. Key Input Documents**

**[D1]** [EWG Final Report](https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf)

**[D2]** Additional Key Input Documents (hyperlinked) to be inserted here as requirements are added.  
Document titles and hyperlinks will be [copied from (or as necessary, added to) these WG Wiki](https://community.icann.org/display/gTLDRDS/Questions) pages.