

## Evaluating New Top-Level Domains: Opportunity or Threat?

### Abstract

The basic structure of Internet naming is likely to undergo its most significant change since its inception—and the implications for users and global corporations are extensive. ICANN, the international body governing Internet naming and addressing practices, has announced a plan which, if approved, would allow for a virtually unlimited number of new Top-Level Domains (TLDs), including new non-English, character-set International Domain Names (IDNs) to the Internet landscape.

The likely benefits of these top-level domains—ranging from new branding and marketing opportunities to enhanced security—are substantial, as are the costs and potential risk. Most notably, the possibility for brand abuse will expand significantly, resulting in increased defensive domain registrations. This shift in the way information is found by users has the potential to fundamentally change the way business is conducted on the Internet.

Given the relatively short timeline proposed by ICANN, companies should begin top-level domain strategy development immediately. Every brand owner will need to carefully assess the impacts, choose an offensive, defensive or combined strategy, and begin developing processes to execute that strategy.

This report proposes a framework for examining potential benefits, risks, costs and implications for corporations as they develop a strategy in response to the expanding TLD landscape.

**This paper is based on the draft New gTLD Applicant Guidebook published by ICANN and is subject to change based upon the final Applicant Guidebook and supporting material.**

## Contents

Executive Summary .....	3
The New Shape of the Internet .....	3
Immediate and Prolonged Impact: How Corporations Will Be Affected .....	5
Business Opportunities .....	5
Risks .....	7
How to Assess Costs .....	8
Becoming a TLD Operator .....	9
What to Do Now .....	10
Wait-and-See: Not an Option .....	10
Glossary .....	11

## Executive Summary

The basic structure of Internet naming is likely to undergo its most significant change since its inception—and the implications for users and global corporations are extensive. ICANN, the international body governing Internet naming and addressing practices, has announced a plan which, if approved, would allow for a virtually unlimited number of new Top-Level Domains (TLDs), including new non-English, character-set International Domain Names (IDNs) to the Internet landscape.

The likely benefits of these top-level domains—ranging from new branding and marketing opportunities to enhanced security—are substantial, as are the costs and potential risk. Most notably, the possibility for brand abuse will expand significantly, resulting in increased defensive domain registrations. This shift in the way information is found by users has the potential to fundamentally change the way business is conducted on the Internet.

With the advent of entire new classes of open (i.e., .company, .trademark, .anything) and community-based TLDs (i.e., .navajo), corporations will quickly need to choose whether to apply for one or more top-level domains, or limit their strategy to proactively defending their brand online during the ICANN application process and beyond.

In every case, due to the cost and complexity, developing and executing a TLD strategy will be a major undertaking, and will require the participation of a range of corporate stakeholders including Marketing, eCommerce, IT, Security and Legal—with significant involvement by executive management. Faced with the realities of competition and brand abuse in this increasingly complex domain space, brand owners should begin to evaluate their new TLD strategy now, rather than await further developments in the process. A decision to delay the creation of a TLD strategy may encourage competitors, both legitimate and illicit, to lay irreversible claim to vast and valuable online territory in the first application period.

Given the relatively short timeline proposed by ICANN, companies should begin top-level domain strategy development immediately. Every brand owner will need to carefully assess the impacts, choose an offensive, defensive or combined strategy, and begin developing processes to execute that strategy.

This report proposes a framework for examining potential benefits, risks, costs and implications for corporations as they develop a strategy in response to the expanding TLD landscape.

## The New Shape of the Internet

Currently there are fewer than 300 top-level domains: the familiar generic (gTLD) categories such as .com, .info, .org and .biz represent roughly 21 TLDs, plus there

This shift has the potential to fundamentally change the way business is conducted on the Internet.

are close to 250 country-code TLDs (ccTLDs) such as .jp and .fr. Under the new plan, any established entity may apply for TLDs representing nearly any industry or area of interest such as .car, .sports or .bank. Individual corporations may also apply for branded TLDs such as .ford, .wsj, and .airbus.

Successful applicants will be able to secure their own “islands” on the Internet. However, they will also need to assume all of the responsibilities associated with operating a domain name registry, a complex and expensive undertaking.

ICANN’s initiative would open the door for hundreds, if not thousands, of new top-level domains and will profoundly transform the Internet’s hierarchy from its current vertical alignment into a much more horizontal structure.

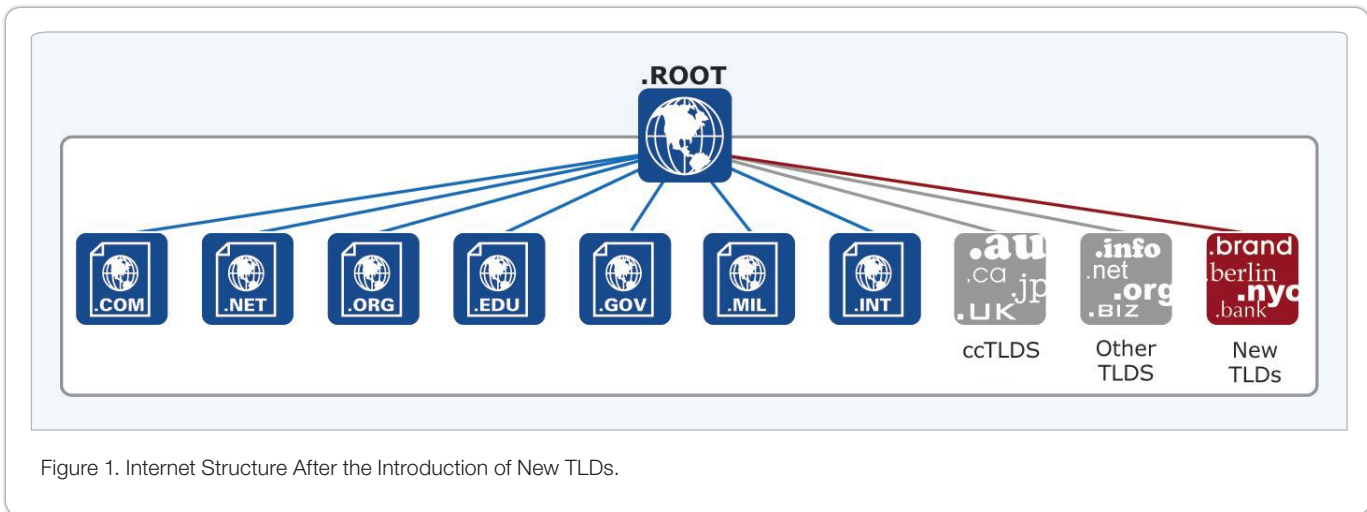


Figure 1. Internet Structure After the Introduction of New TLDs.

With no as-yet announced limitation on the number of domains, the Internet could theoretically grow to include more than 60 million top-level domains. Realistically, however, operational and administrative constraints will likely limit early growth to a few hundred new TLDs during the first application period, which is expected to open in the first quarter of 2010. If ICANN proceeds as planned, the first set of new top-level domains is likely to be approved in late 2010 and launched in 2011.

ICANN has defined two types of new TLDs:

**Community-based:** This type of TLD addresses a clearly-defined community that is operated for the benefit of a restricted population.

In order to qualify for a community TLD, the applicant must:

1. Demonstrate an ongoing relationship with a defined community that consists of a restricted application.
2. Have applied for a TLD string related to that community.

3. Have proposed registration and use policies for registrants in the proposed TLD.
4. Have its application endorsed by an established institution representing the community.

**Open:** Any application that has not been designated as community-based will be considered as an open TLD. Open TLDs can be used for any purpose consistent with application and evaluation criteria. An open TLD may or may not have a formal relationship with an exclusive registrant or user population. It may or may not employ usability restrictions.

Types of open TLDs expected include branded TLDs such as “corporate closed” models, where a TLD is used internally by the corporation, and “corporate open” models, where a corporation will potentially allow partners and/or customers to register domain names within the TLD in addition to corporate registrations.

## Immediate and Prolonged Impact: How Corporations Will Be Affected

The new top-level domain landscape will leave no brand owner unaffected. Yes, there will be opportunities: to enhance brand image, build secure communities for customers and trading partners, improve segmentation and targeting effectiveness, and market within new, community-focused TLDs. But the added risks are both substantial and urgent. Brand abuse will be a significant and enduring problem, while defending against it adds even more complexity. Whether or not a company anticipates leveraging the possible new TLD advantages, a strategy to minimize risks will require the attention of every brand owner.

### Business Opportunities

The advantages of acquiring proprietary territory on the Internet could be substantial, and the top-level domain expansion represents a new opportunity to secure and develop that territory. Additionally, a branded TLD offers advantages and opportunities that haven't been feasible while brands have been limited to gTLDs like .com and .biz.

**Marketing advantages.** Many corporate marketing professionals see the potential of branded TLDs for enhancing brands and creating a more positive user experience, by creating an “island on the Internet” where customers, partners and subsidiaries can gather in a secure, convenient community that can reinforce relationships and build market share.

Branded TLDs can benefit companies by providing a tighter association between their brands—online and off. Many corporations have talked about using TLDs to create and host new online services and products with close association to their brand. Branded TLDs can also signal both site legitimacy and safety to end-

Whether or not a company anticipates leveraging the possible new TLD advantages, a strategy to minimize risks will require the attention of every brand owner.

users, as corporations control all domains and content within their own TLDs. This is potentially powerful for channel partners, as only legitimate parties could participate within a “corporate open” TLD. A branded TLD can also visibly—and subconsciously—signal a company’s industry leadership, while providing unique opportunities to build online communities around a brand, communities where innovative ideas can be created and promoted.

On the more tactical side, a number of practical advantages will arise: for example, a TLD owner can better target finite audiences through customized content (i.e., `services.markmonitor`, `brandprotection.markmonitor`, `partners.markmonitor`, etc.). Access to this content may also improve through more intuitive direct navigation as well as potentially better search engine ranking results. To the extent that more consumers use direct navigation to reach websites, applicants may be able to reduce its online advertising expenditures. Corporations can also build community and create stickiness among customers by offering customized email addresses (i.e., `jack@marketing.markmonitor`; `info@services.markmonitor`). Top-level domains under company ownership and control can also provide safe, secure pre-launch platforms for development of content supporting new products, services and brands.

Industry consortiums may also leverage new TLDs to attract and direct users within online trusted communities such as `.bank` or `.pharmacy`. Naturally, these community-based TLDs will present their own challenges, requiring cooperation from industry competitors on goals, policies, and practices. But the potential for industry benefits—especially on the security side—will likely lead to domain policies that will work for all industry members.

**Security benefits.** Because branded TLD owners can set the domain registration policy for their own TLDs—in essence controlling who is eligible to register for a domain—and control content within their TLD, they have the opportunity to completely prevent unwanted activity by domainers (for-profit traders of domain names) and cybersquatters (who use domain names to unfairly capitalize on brands they don’t own), but only within the TLD they own. Domainers and squatters can continue their activities within other TLDs, so the need for monitoring and enforcement will not disappear.

Unauthorized sales and channel non-compliance will be considerably more difficult within a branded TLD. Because it is possible that only authorized resellers would be granted second-level domains within a TLD, gray market and counterfeit activities could only occur outside a brand’s TLD, enabling customers to confidently purchase legitimate goods and services. In addition, companies can monitor for policy compliance within its own branded TLD and take corrective measures against any violator.

Phishing threats could also be reduced, though not eliminated. Phishers will likely be unable to acquire domains within the TLD for the purpose of hosting spoofed company websites; however, they can continue to use spoofed email addresses which appear to be within a brand’s TLD but is actually not.

A TLD owner will also have the option of protecting against DNS cache poisoning, or pharming attacks, which redirect Internet traffic to unintended locations. DNS security extensions, also known as DNSSEC, can protect against such attacks by providing additional authentication and data integrity checks, but only when properly implemented by a TLD's registry. At present, DNSSEC is being implemented for .org and a few ccTLDs such as .ca (the Canadian ccTLD).

## Risks

The new TLD landscape does present a number of new risks—from risks associated with the application process to those resulting from the significant expansion of new TLDs on the horizon.

**User adoption/confusion.** While industry analysts predict that most businesses will continue to use the .com TLDs, there is some early indication that at least a handful of large corporations will pursue branded TLDs and, perhaps, gradually migrate their online presence to these branded TLDs over the next several years.

Extensive marketing and informational campaigns should serve to ease the transition for users, and brand constituents will learn quickly enough how to navigate to their desired location. Nonetheless, the potential, however temporary, for lost business and customer confusion is real.

**Brand abuse still likely.** Any temporary confusion within user ranks is likely to be exploited by brand abusers. It's important to remember that abuse found in currently existing TLDs can and most likely will continue—and the addition of potentially thousands of new TLDs with non-stringent eligibility requirements will create new locations for domainers, squatters, phishers and others to exploit. Monitoring for abuse will now have to be extended to a much wider universe.

Risks of brand abuse will even extend to within a brand's own TLD—there's no guarantee that authorized domain owners (customers, partners, internal business units) will abide by a TLD's use policies—so TLD owners will need to monitor for abuse even on their own turf. But at least brand owners will have the power to set and enforce their own use policies, and can do so with detection and enforcement in mind. As the operator of a branded TLD's registry, corporations would have the power to remove use policy violators.

**Defensive registration: still a reality—and then some.** Roughly 90%+ of today's corporate domain portfolios are comprised of defensive domain registrations. With the number of TLDs set to multiply, defensive registration will likely increase, as will the complexity of identifying needs and registering.

**Acquiring a TLD will be both challenging and expensive.** TLD applicants will be required to demonstrate their ability to meet ICANN's stringent business, operational, and technical requirements. To mitigate corporate liability risks, best practices indicate, they may need to establish a separate legal entity to own and operate the TLD.

TLD-related costs, both initial and ongoing, will be significant. Also, because a standard ICANN registry contract spans a full 10 years—and due to the high risks involved in any web strategy reversal—the commitment will be a long-term one.

**Risk losing a key TLD.** Applications will be considered initially in rounds, and then on a continuous basis thereafter. Thus, if an applicant is awarded a TLD in round one, then that TLD will not be available later on. This particular aspect of the application process may pose a risk to brand owners, especially if other parties apply for and can demonstrate a right to a particular TLD string (i.e., others holding trademarks in different classes or jurisdictions); brands whose names resemble generic terms are especially prone to this risk. Another risk is that if brand owners wait to apply for a branded TLD in a later round that particular TLD will not be awarded if it is deemed too similar to a TLD that was awarded in an earlier round; this particular risk is especially profound given that IDNs may also conflict. Finally, if corporations decide to wait until round two or later, they may risk waiting for a long time, as potentially hundreds if not thousands of applications will be evaluated in round one, thus making it unclear when the next opportunity will be to apply for a TLD.

**Community gets preference.** A related risk exists in that brand owners who may want a given TLD, even with a timely application, may not win it, because a community group has requested the same domain string or because the community simply objects to the domain. (Example: a candy manufacturer may apply for .candy; but a consortium of manufacturers may object). ICANN has consistently demonstrated a strong community bias; its charter and mission practically require it to do so.

Communities are provided a significant voice and a certain degree of preference, beginning with the power to object to any application. Additionally, bona fide, community-based applicants may request a comparative evaluation—in which only community-based applicants participate—to determine which applicant can most convincingly demonstrate that their ownership of the TLD will add more value to the Internet domain space. Only if no community-based applicant emerges as the clear winner, will an auction process be used to award the disputed TLD among all applicants.

## How to Assess Costs

With an application fee of \$185,000 and a minimum annual ICANN fee of \$25,000, becoming a TLD registry comes at a considerable price. Even before winning a TLD, applicants face the possibility of string contention and challenge fees (and the costs to respond to the challenge). There may also be costs associated with application advocacy; and legal fees may be substantial. In the end, some estimate that to simply apply for a branded TLD the figure would most likely approach \$500,000, plus another \$300,000 or more annually to operate it—exclusive of development costs and registrations.

**Ongoing costs.** Aside from the \$25,000 yearly ICANN fee, TLD owners will need internal staff to administer registrations and ensure policy compliance. Other costs to expect include specialized accounting and audit activities, litigation, and the cost of maintaining a registry infrastructure—managed in-house or outsourced.

Creating and operating a registry infrastructure and its surrounding systems represents significant cost and effort. TLD applicants will need to understand how they will fill this need early on, as they must outline their registration policies and any proposed registry services as part of the application.

Registries must provide for a wide range of functions including, but not limited to zone file publication, data escrow, DNS operations, database production and maintenance, and protocol interoperability. Also, because no TLD registry may currently discriminate among ICANN-accredited registrars (according to the GNSO's 19th recommendation), owners may need to develop, market to, and support a registrar/distribution channel. Given this complexity, corporations will want to carefully assess which of these functions should be maintained in-house and which should be outsourced.

Some large corporations have already admitted to budgeting nearly \$1 million just to acquire and launch a TLD. Costs will vary, of course, with intended use, projected brand protection requirements and possible economies of scale if multiple TLDs are owned.

## Becoming a TLD Operator

After the arduous application and award process, brand owners who win the right to operate their own TLDs will face significant pre-launch activity and ongoing maintenance. Prior to launch, domain registry and management systems will need to be fully implemented.

Dependent upon the type of TLD operated, TLD owners will also need to negotiate and finalize contracts with back-end registry operators and relevant registrars; finalize validation requirements and processes; develop implementation and testing plans; setup accounting and administrative functions; establish customer support for registrar(s) and potentially registrants; potentially manage rights protection processes on open or community-based TLDs; and last, but not least, proactively manage the overall launch. Once the TLD is launched, TLD owners will need to operate registration, modification and renewal processes while maintaining accurate Whois and other registry records.

Many of these activities require specialized knowledge and skills not found inside most corporations; and the effort required can often be beyond the bandwidth of internal staff. Most corporations will seek outside help to staff some or all of these activities, and expert guidance in order to effectively plan and manage them.

## What to Do Now

The expansion of TLDs will impact virtually every corporation. Companies should begin now, if they haven't already, to develop a strategy to seize opportunities and protect against the potential for new or expanded threats.

**Assess.** First, companies should create a cross-functional team to evaluate the corporation's strategic situation. The team, which should include stakeholders from Marketing, eCommerce, IT, Security, Legal, and domain management units, must also have strong backing from and participation by executive management. Issues to study begin with potential impact on the company's strategic goals and the business model under which a proposed TLD would operate (cost recovery, revenue generation, or brand investment). The team should also study potential financial commitments, in-house resource availability and outsourcing opportunities.

**Participate.** Companies should carefully review ICANN's proposed application process discuss issues with key advisors and industry partners, and raise concerns to ICANN as appropriate. Also, brand owners may wish to seek out industry experts (such as MarkMonitor, which acts as an advocate for brand owners throughout the process) to gain clarification and share opinions.

**Monitor and defend.** As applications become public in the first as well as in subsequent rounds, prudent brand owners will monitor them closely for possible brand threats and file objections within ICANN's specified timeframe to protect their brands. As new TLDs are launched, to prevent potential cybersquatting, corporations should plan to make practical, defensive domain acquisitions within new TLDs with non-stringent eligibility requirements as well as monitor and respond to potential brand infringement.

**Consult.** With the impending fundamental changes in online business strategies, it makes sense to leverage industry expertise. Brand owners should seek out resources with deep knowledge of domain registration processes, registry operation and the inner workings of ICANN. Most organizations will need to look beyond their internal staff to locate this expertise, or to supplement internal experts as the new process places additional demands on brand owners.

## Wait-and-See: Not an Option

The rapid expansion of community-based and company-branded TLDs will impact every large—and many smaller—corporations worldwide. Given the significant risks and opportunities ahead, each brand owner will need to carefully assess that impact, choose an offensive, defensive or combined strategy, and begin developing processes to execute that strategy.

These efforts will take time—but time is limited by ICANN's aggressive schedule. The time to begin crafting strategy is now.

## Glossary

**Backend Registry Operator (BRO)** – See Registry below.

**Country Code Top-Level Domain (ccTLD)** – Two letter top-level domains, such as .uk (United Kingdom), .de (Germany) and .jp (Japan), are called Country Code Top-Level Domains (ccTLDs) and correspond to a country, territory, or other defined geographic territory.

**Data Escrow** – Registrars must submit to ICANN or, at the registrar’s election and expense, to a reputable escrow agent, a copy of the electronic database maintained by the registrar reflecting domain registrations.

**Domain Name System (DNS)** – The Domain Name System (DNS) helps users find their way around the Internet. Every computer on the Internet has a unique address—just like a telephone number—which is a rather complicated string of numbers. It is called its “IP address” (IP stands for “Internet Protocol”). IP Addresses are hard to remember. The DNS makes using the Internet easier by allowing a familiar string of letters (the “domain name”) to be used instead of the arcane IP address. So instead of typing 207.151.159.3, you can type www.internic.net. It is a “mnemonic” device that makes addresses easier to remember.

**DNS Security Extensions (DNSSEC)** – DNS security extensions, or DNSSEC, address the problem of DNS cache poisoning by providing a set of DNS extensions which provide origin authentication and integrity checks of DNS data. DNSSEC, however, is only truly effective if a particular TLD zone is DNS protected, and this requires implementation by registries.

**Dispute Resolution Provider (DRP)** – ICANN plans to use independent Dispute Resolution Providers to resolve any disputes between an objector and applicant during the dispute resolution phase of the New gTLD application process. A gTLD application can be objected to on any of the following four criteria: 1) String Confusion, 2) Existing Legal Rights, 3) Morality and Public Order, and 4) Community Objection.

**Extensible Provisioning Protocol (EPP)** – The Extensible Provisioning Protocol (EPP) is the industry standard protocol used by registries and registrars to communicate domain name-specific details to each other for the purpose of registering and maintaining domain names.

**Generic Names Support Organization (GNSO)** – The Generic Names Support Organization (GNSO) advises the ICANN Board on issues relating to generic top-level domains. In August 2007, the GNSO provided 19 “recommendations” and 17 “implementation guidelines” to ICANN for the introduction of new gTLDs into the domain name. These recommendations and guidelines were approved by the ICANN Board in June 2008.

The GNSO is the body of six constituencies, as follows: the Commercial and Business constituency, the gTLD Registry constituency, the ISP constituency, the non-commercial constituency, the registrar’s constituency, and the IP constituency (which represents brand owners).

**Generic Top-Level Domain (gTLD)** – Most TLDs with three or more characters are referred to as “generic” TLDs, or “gTLDs”. They can be subdivided into two types, “unsponsored” TLDs (uTLDs) and “sponsored” TLDs (sTLDs).

Generally speaking, unsponsored TLDs (including .com, .net, .org, .biz, and .info) operate under policies established by the global Internet community directly through the ICANN process, while sponsored TLDs (including .aero, .coop, .edu, .jobs, .mobi, and .museum) are specialized TLDs that have Sponsors representing the narrower community that

is most affected by the TLD. The Sponsor carries out delegated policy-formulation responsibilities over many matters concerning the TLD.

**Internationalized Domain Name (IDN)** – An Internationalized Domain Name (IDN) is an Internet domain name that contains one or more non-ASCII characters. Such domain names could contain letters with diacritics, as required by many non-English languages, or characters from non-Latin scripts such as Arabic, Hebrew, Chinese or Hindi.

**Internet Assigned Numbers Authority (IANA)** – The IANA is the authority originally responsible for the oversight of IP address allocation, the coordination of the assignment of protocol parameters provided for in Internet technical standards, and the management of the DNS, including the delegation of top-level domains and oversight of the root name server system. Under ICANN, the IANA continues to distribute addresses to the Regional Internet Registries, coordinate with the IETF and others to assign protocol parameters, and oversee the operation of the DNS.

**Internet Corporation for Assigned Names and Numbers (ICANN)** – The Internet Corporation for Assigned Names and Numbers (ICANN) is responsible for managing and coordinating the Domain Name System (DNS) to ensure that every address is unique and that all users of the Internet can find all valid addresses. It does this by overseeing the distribution of unique IP addresses and domain names. It also ensures that each domain name maps to the correct IP address.

ICANN is also responsible for accrediting the domain name registrars. “Accredit” means to identify and set minimum standards for the performance of registration functions, to recognize persons or entities meeting those standards, and to enter into an accreditation agreement that sets forth the rules and procedures applicable to the provision of Registrar Services.

**Top-Level Domain (TLD)** – A top-level domain (TLD) is the last part of an Internet domain name; that is, the letters that follow the final dot of any domain name. These domains represent the highest level of categorization or classification of all Internet resources; until approximately 2010 there will be fewer than 250 TLDs. Management of most top-level domains is delegated to responsible parties or organizations by ICANN. Types of TLDs include:

- Infrastructure top-level domain (only one exists: .arpa)
- Country-code top-level domains (ccTLD)
- Sponsored top-level domains (sTLD)
- Generic top-level domains (gTLD)

**Registrant** – Registrants are individuals, including individuals representing corporations, who register domain names. The registrant is required to enter a registration contract with a registrar or registry, which sets forth the terms under which the registration is accepted and will be maintained.

**Registrar** – Domain names are registered through many different companies known as Registrars. MarkMonitor, for example, is an ICANN-accredited registrar with an exclusive focus on corporate domain portfolios. A complete listing of registrars is in the Accredited Registrar Directory.

A registrar asks individuals, or “registrants”, for an array of contact and technical information that becomes part of the registration. The registrar maintains records of the contact information and submits the technical information to a central directory known as the “registry.”

**Registry** – The Registry is the authoritative, master database of all domain names registered in each Top-Level Domain. The registry operator keeps the master database and also generates the Zone File which allows computers to route Internet traffic to and from top-level domains anywhere in the world.

**Request for Proposal (RFP)** – A Request for Proposal (RFP) is being issued by ICANN to solicit applications for an unlimited number of new generic Top-Level Domains (gTLDs). The RFP will establish the application process for the new gTLDs. A draft RFP is expected in Q4-08 and the final RFP is expected in Q1-09.

**Root Zone** – The root zone is the top level of the Domain Name System. The root exists above the TLDs and defines a given name space by identifying the nameservers that will answer authoritatively for a given TLD. IANA, for example, manages the root zone on which the great majority of Internet traffic flows. It is possible to have more than one root and in fact some alternate root servers do exist, but have not gained much popularity to date. The root that IANA administers is centrally managed, but service of the root zone file is provided by a series of geographically and operationally diverse root servers.

**Root Nameserver** – A root nameserver is a DNS server that answers requests for the DNS root zone, and redirects requests for a particular TLD to that TLD's nameservers. Although any local implementation of DNS can implement its own private root nameservers, the term "root nameserver" is generally used to describe the thirteen well-known root nameservers that implement the root namespace domain for the Internet's official global implementation of the Domain Name System.

**Shared Registration System (SRS)** – The Shared Registration System (SRS) is the software provided by a registry to facilitate the registration of domain names, updates of nameservers, contact information and overall management of a registry. The SRS is used by registrars to connect to the registry.

**Sponsor** – A Sponsor is an organization to which is delegated some defined ongoing policy-formulation authority regarding the manner in which a particular sponsored TLD is operated. The sponsored TLD has a Charter, which defines the purpose for which the sponsored TLD has been created and will be operated. The Sponsor is responsible for developing policies on the delegated topics so that the TLD is operated for the benefit of a defined group of stakeholders, known as the Sponsored TLD Community, that are most directly interested in the operation of the TLD. The Sponsor also is responsible for selecting the registry operator and to varying degrees for establishing the roles played by registrars and their relationship with the registry operator. The Sponsor must exercise its delegated authority according to fairness standards and in a manner that is representative of the Sponsored TLD Community.

**Thick Registry** – With a thick registry model, all WHOIS information associated with domain names, including both technical information (nameservers) and contact information (registrant, administrative and technical contacts) is stored within the registry repository.

**Thin Registry** – With a thin registry model, primarily technical data for each domain (nameserver and IP address information) is stored in the central registry database, while contact and billing information is maintained by the registrar managing the domain name. In this model, the registry only knows the mapping from a domain name to a registrar as well as the associated nameservers. WHOIS services operated by the registry publish that mapping, while the registrant's identity is then published by the registrar.

**WHOIS** – WHOIS provides domain name ownership information to allow for the rapid resolution of technical problems and to permit enforcement of consumer protection, trademark, and other laws. ICANN-accredited registrars are required to maintain a free, publicly available database of WHOIS data for query by others for domain names that are registered through them.

**Zone File** – In the context of this paper, Zone File is a mapping of domain names to IP addresses.

## About MarkMonitor

MarkMonitor, the global leader in enterprise brand protection, offers comprehensive solutions and services that safeguard brands, reputation and revenue from online risks. With end-to-end solutions that address the growing threats of online fraud, brand abuse and unauthorized channels, MarkMonitor enables a secure Internet for businesses and their customers. The company's exclusive access to data combined with its real-time prevention, detection and response capabilities provide wide-ranging protection to the ever-changing online risks faced by brands today.

To learn more about ICANN's new generic Top-Level Domain initiative and MarkMonitor Top-Level Domain Services, visit [www.markmonitor.com/topleveldomains](http://www.markmonitor.com/topleveldomains)

More than half the Fortune 100 trust MarkMonitor to protect their brands online.  
**See what we can do for you.**

MarkMonitor, Inc.  
U.S. (800) 745.9229  
Europe +44 (0) 207.840.1300  
[www.markmonitor.com](http://www.markmonitor.com)