Assessing legal risks of closed generic top-level domains

Tobias Mahler[1]

Cite as Mahler T., "Assessing Legal Risks of Closed Generic Top-Level Domains", in European Journal of Law and Technology, Vol 5, No 3, 2014.

ABSTRACT

Since the recent introduction of new generic top-level domains (TLDs), a variety of new Internet domain names have become available for registration. These include new domain endings such as <.berlin>, <.club> or <.global>, which anyone can purchase. At the same time, an entire class of new TLD applications has arguably failed. Several well-known corporations applied for 'closed generic TLDs'. The applicants wanted to reserve these generic words for internal use, thus disallowing third party registrations. Examples included <.beauty> (L'Oreal), <.ketchup> (Heinz), <.blog> (Google) and <.book> (Amazon). These applications have either been withdrawn or will be converted into open TLDs, largely as a consequence of changes or clarifications in rules for TLDs published by the Internet Corporation for Assigned Names and Numbers (ICANN).

This article advances two arguments. The first argument is that these applications for closed generic TLDS were fairly risky because they implied some level of legal risk for the applicants. The failures indicate that some risks have now materialized. The article also discusses what methods, if any, TLD applicants could have used to identify and manage such risks. The second argument put forth is that standard risk management techniques can and should be applied to the analysis of legal risk.

1. INTRODUCTION

Internet top-level domains (TLDs), such as <.com>, <.org>, <.de> and <.uk>, are vital to web surfing and forming email addresses. Thus far, their number has been very limited; however, these limitations were recently lifted. After years of discussions, the Internet Corporation for Assigned Names and Numbers (ICANN) opened up the application process for new generic top-level domains (gTLDs). Proposals in the first round include, among others, genuinely generic names, such as <.music>, <.bike> or <.bank>, and geographic strings, such as <.berlin>, <.москва> (which is the Cyrillic word for Moscow), and <.nyc> (which is the abbreviation for New York City). Several major corporations are applying to use their brand names as top-level domains. Many are seeking the introduction of new TLDs to offer domain name registry services and meet the expanding demand for Internet domain names. It is also possible that some new TLDs may facilitate truly novel and innovative business models.

One particularly controversial aspect of the new TLD program was that several applicants applied for TLDs that were generic words, such as book, blog and beauty; the applicants planned to use these words exclusively for their own purposes. In other words, domain names under these TLDs would not be offered on the market but used only for internal purposes, such as the sale of books by a single bookstore. Over the past year, it has become clear that this business model is not permitted under ICANN's rules. Consequently, most applicants for closed gTLDs have withdrawn or amended their applications.

Applying for a new TLD is quite costly because applicants must disburse *inter alia* a substantial application fee, the possible costs for an auction and start-up costs. Any business venture can be risky because of the possibility that initial investments will be lost. Some of the many sources of risk for a TLD are related to legal or policy issues. If a chosen business model infringes on competition or trademark rules according to applicable law, the business model might not be viable. In addition, TLD applications are submitted to ICANN, which has its own rules and decision-making procedures that can influence the success of a TLD.

This article commences by retrospectively analysing the legal problems that led to the apparent failure of closed generic TLDs (see below Sections 2 and 3). Although ICANN's rules for new generic TLDs were publicly available in advance, applicants seem to have failed to predict the rules' effects on their applications. An alternative interpretation is that these applicants were aware of the risk and decided to go ahead nevertheless. Part of the underlying issue is that these applications were submitted in a regulatory environment with evolving rules at ICANN. Ideally, policy decisions should have been concluded prior to receiving TLD applications, but for a number of reasons this was not the case. This continued evolution of important rules represents an obvious challenge for applicants, not least because ICANN's internal decision-making procedures are both complex and subject to change.[2] In particular, the influence of the world's governments in ICANN is growing, and governmental advice was decisive for the failure of closed generic TLDs. Taken together these factors have contributed to a situation in which several large international corporations have applied in vain for closed generic names, leading to the loss of substantial project-related investment costs.

In the second part (see Sections 4 to 6) the focus shifts to examining these problems at the meta-level of legal methodology. What methods, if any, might have been useful for a proactive analysis of these legal problems? The legal and policy issues facing applications for closed generic TLDs are thus used as a starting point for a case study in legal risk management. The underlying hypothesis of this case study is that more formalized legal risk management methods could be introduced as suitable additions to practising lawyers' working methods. This raises a number of questions. What is risk management and how can it be applied to assess legal risk? What characterizes legal risk and to what degree is legal uncertainty relevant for its analysis? How could applicants for closed generic TLDs have used risk management to manage legal risks related to their applications?

2. APPLYING FOR A TLD

Before discussing the specific problems and risks related to closed generic TLDs we need to briefly introduce how an organization can apply for a generic TLD.

The Internet domain name system is structured around country code TLDs (ccTLDs), such as <.uk> for the United Kingdom, and gTLDs, such as <.com> and <.org>.[3] Any hierarchical addressing system requires some level of organization or coordination, and for the Internet's domain name system this is provided by ICANN, the Internet Corporation for Assigned Names and Numbers. Therefore, applications for new TLDs need to be addressed to ICANN. The new TLD program has opened up the previously closed market for TLDs.[4]

The present extension of the domain name system technically focuses on new gTLDs, but the 'generic' category is open-ended and may also include applications for TLD strings containing trademarks and other specific denominators. An applicant may essentially apply for any string as long as the name is not within the very limited sets of restricted names.[5]

Applications for new TLDs can be made during limited periods ('application windows') following a process described in ICANN's applicant guidebook. After the first application window closes, ICANN is expected to open further rounds that could be based on fairly similar application rules. The application process for the first round included, *inter alia*, an evaluation of the TLD name applied for and the applicant's financial and technical capabilities.[6] The full details of the application process cannot be provided here; the process is rather comprehensive and potentially lengthy, particularly if conflicting applications must be evaluated or if disputes must be resolved.[7]

Not all applications are successful; among other reasons, an application may fail due to competing applications for a similar name or successful objections against an application. The application process thus implies the risk of failure because the application may not pass the criteria or competing applications may prevail. Thus, applying for a TLD is a risky endeavour, and decision-makers should have an interest in managing risk adequately.

One aspect of the risk is related to legal and contractual rules that are binding for an applicant. In addition to the applicable law(s), these include, in particular, the application rules in the applicant guidebook and contractual rules in the contract between a successful applicant and ICANN (the 'registry agreement'). As shown below these contractual rules are particularly tricky for closed generic TLDs. ICANN refrained from defining different categories of applications, so there are no *specific* rules for closed generic TLDs. However, an annex to the registry agreement contains a general rule that, according to recent practice, is interpreted to rule out closed generic TLDs.[8] As further explained below we can say in hindsight that this rule represented a legal risk for applicants intending to exclusively use generic strings in TLDs.

3. THE PROBLEMS WITH CLOSED GENERIC TLD APPLICATIONS

Closed gTLD applications are for the exclusive use of a generic word, such as 'ketchup', at the highest level of the Internet's domain name system (e.g. <.ketchup>). The expression 'closed generic TLD' is almost a contradiction in terms because 'generic' is usually defined as 'relating to a whole group or class' or 'having a non-proprietary name'.[9] This seems to indicate some measure of openness, which is somewhat contradictory to the proprietary and exclusive use of the term in a TLD where only one organization can register names. Thus, when Heinz applied for <.ketchup>, it intended to use this TLD to the exclusion of others involved in the production of cold tomato sauces. This would have been a new marketing tactic only if the hierarchy of name levels is considered. Consumers are already used to the exclusive use of generic words at the second level of the domain name system, such as in <ketchup.com>, so the proprietary use of generic words on the Internet is not new.

Other closed TLD applications submitted to ICANN included words such as 'blog' (in the <.blog> applications submitted by, *inter alia*, Google and Amazon) and 'beauty' (in an application submitted by L'Oreal). Closed gTLD applications have been criticized for monopolizing generic words,[10] and it was not entirely clear whether these applications were compatible with ICANN's rules when they were submitted.

Because of this uncertainty, the effect of applying these rules was not certain. According to one interpretation of the rules, closed gTLDs are not permissible. This possibility of rule infringement could be characterized as a legal risk, not least because it carries the possibility of sanctions. In comparison, TLD applications planning to sell domain names do not face this significant potential conflict with ICANN's rules. In this sense closed generic TLDs are more risky than regular[11] TLD applications.

3.1 ICANN RULES ON CLOSED GENERIC TLDS

To understand the nature of this issue, we must take a closer look at ICANN's rules for TLDs. Two sets of rules should be distinguished here. First, ICANN published an application guidebook that contained some procedural rules for TLD applications and the selection of successful candidates. These rules can be examined when assessing the risk of unsuccessful applications, i.e. the possibility of not being allocated an applied-for TLD. These rules are of crucial practical significance, but we can nevertheless disregard them here because a second set of rules is much more significant for closed gTLDs. The latter are included in the registry agreement, i.e. the contract between a successful applicant and ICANN. This standardized agreement effectively limits what a TLD holder can do with a TLD, and it has gradually become clear that the agreement disallows closed gTLDs. The registry agreement is included in ICANN's applicant guidebook.[12]

ICANN's conceptual starting point when drafting the TLD agreement seems to have been a use case focusing on domain name sales in TLDs. This use case has had great relevance for all pre-

existing TLDs, such as <.com>, <.org> and <.edu>, and ccTLDs, which also operate by selling domain names, which also operate by selling domain names. Depending on the TLD, the class of potential registrants may be defined widely (e.g. 'anyone can register a <.com> address') or it may be restricted to members of a community (e.g. <.edu> is limited to certain actors in the educational sector).

The sale of domain names is a useful point of departure for understanding most TLD applications, but it disregards the possibility of registering exclusive TLDs. Demand is clearly present for proprietary TLDs, such as <.microsoft> or <.apple>, and ICANN never ruled out such applications. Applicants for proprietary TLDs presumably do not intend to offer domain names under the respective TLDs to third parties. To the contrary, some applicants are interested in excluding competitors from their 'private namespace'.[13] ICANN, which has a primary focus on facilitating a competitive domain name market, only reluctantly recognized this interest in exclusive uses of TLDs.

Most of the ICANN rules do not imply problems for the exclusive use of TLDs, but some do. A particularly relevant provision is contained in Section 1(b) of the Registry Operator Code of Conduct (hereinafter Code of Conduct).[14] This provision asserts the principle that the registry operator (i.e. the TLD holder) is prohibited from registering domain names in its own right, with a few exceptions. Thus, for example the registry operator for <.berlin> is prohibited from registering more than a few names in its own right, but it can offer remaining names on the market.

If there were no exemptions to this rule, no brand holder would be able to use a TLD as a proprietary platform for its Internet presence, and third parties would have to open up brand TLDs, such as <.ibm>, <.audi> or <.toyota>, for registration. The demand for brand TLDs may have been the main reason behind allowing registry operators to request an exemption from the prohibition under Section 1(b). According to Section 6 of the Code of Conduct, an exemption may be granted under specified conditions. ICANN may grant such a request if (i) all domain name registrations in the TLD are registered to and maintained by the registry operator for its own exclusive use; (ii) the registry operator does not sell, distribute or transfer control or use of any registrations in the TLD; and (iii) the application of the Code of Conduct is not necessary to protect the public interest.[15]

3.2 LEGAL UNCERTAINTIES

Several aspects of this rule are uncertain for closed gTLD applications. First, the possibility of an exemption is conditional on the requirement that the registry operator does not sell, distribute or transfer control or use of any registrations in the TLD to any third party. This is not necessarily a problem for most closed TLDs, such as <.ketchup>, because this is exactly how the TLD was intended to be used. In the case of <.ketchup>, this use is evidenced in the application: '[a subsidiary of] Heinz Company ("Heinz"), has filed this application for a .KETCHUP gTLD with the intention of bringing to market a trusted, hierarchical, and intuitive namespace for consumers to access content related to Heinz Tomato Ketchup worldwide.'[16]

However, in some cases the applicant states that it will use the TLD only for its own purposes, even though the planned use indicates that third parties will receive domain names in the TLD. For example, Google's application for <.blog> states that '[t]he purpose of the proposed gTLD, .blog, is to provide a dedicated Internet space where Google can continue to innovate on its Blogger offerings. The mission of the proposed gTLD is to provide a dedicated domain space in which users can publish blogs.'[17] This statement is not entirely clear, but one interpretation is that bloggers could get a domain name under <.blog> from Google. The problem for Google is that this would likely be seen as a 'transfer of control or use of any registrations in the TLD'. This, in turn, would exclude an exemption to the Code of Conduct according to Section 6(ii). It must have been clear to Google at the time of application that, if this was the case, Google would need to open the TLD for registrations outside the company and would not be allowed to register names in its own rights. Nevertheless, it is difficult to see how this would provide the dedicated Internet space intended by Google.

A second factor of uncertainty regards the possibility that an exception to the Code of Conduct is not granted for other reasons. The Code of Conduct foresees that a request for an exception can be rejected if necessary to protect the public interest.[18] Depending on how extensively the expression 'public interest' is interpreted, it could lead to the consideration of many types of interests related to society at large. The wording itself does not specify limitations on what might be considered a public interest, and a systematic interpretation of the applicant guidebook could indicate a rather broad scope.[19] For example, in the context of Amazon's application for <.author>, the applicant must have considered the possibility that ICANN considers it a public interest to keep the TLD <.author> open for registrations by independent writers. Was Amazon certain that the exclusive use of the <.author> registry only for Amazon's own author registrations is acceptable from a public interest point of view?

Some applicants seem to have realized that they might not get an exemption from the Code of Conduct and have taken a variety of approaches to avoid the problem. For example, L'Oreal stated in its application for <.beauty> that it intended to initially allocate names (e.g. cosmetics and perfume) to itself[20] but nevertheless claimed that '[t]he registration and use of these domain names are intended to be within the scope of Section 1B of Specification 9 [the Code of Conduct]'.[21] This claim seems to be a contradiction in terms because this provision clearly prohibits the applicant from registering names in its own right.

A third element of uncertainty was not visible in the wording of the Code of Conduct, but it might have been anticipated with a sufficient understanding of ICANN processes. After the applications became publicly known, ICANN faced an internal policy debate about how it should regulate closed TLDs containing generic words. Although the time frame for policy decisions should have ended before applications were accepted, this is not necessarily a deterrent for new interpretations of the existing policy. A group of ICANN participants asked ICANN to issue a clarifying statement to the effect that exemptions under Section 6 of the Code of Conduct would only be granted for TLD strings identical to a trademark, excluding generic terms.[22] This led ICANN into policy discussions that ended with a decision that currently bans closed generic TLDs.

3.3 SUBSEQUENT POLICY DEVELOPMENT

ICANN responded to the criticism against closed gTLDs by conducting a public comment forum to understand all the views and potential ramifications relating to closed gTLDs.[23]

According to the summary of comments compiled by ICANN, many commenters argued that closed gTLDs for generic industry terms (such as .book, .security) are not in the public interest and should not be allowed. [24] Several argued that these strings should be open and unrestricted because generic words used in a generic way belong to everyone.[25] Allowing such closed gTLDs would harm competition, limit consumer choice and confuse consumers.[26]

Several large corporations, such as IKEA and Yahoo!, voiced the concern that it would be very difficult to reverse such grants in the future. [27] The worry was that the registry operator would have perpetual control over the TLD. Based on ICANN's rules against future TLDs that are confusingly similar, the proprietor would be able to prevent others from operating a similar gTLD in the future. In this respect, competition policy was mentioned as a key concern. For example, Microsoft focused on gTLDs that represent an industry category in which the applicant competes and requested that such TLDs would be open to competitors.[28] Many commenters perceived closed gTLDs as a threat to the openness and freedom of the Internet.[29] On the other hand, closed gTLDs also received some support, partly due to the difficulty of distinguishing exactly what is a generic term. [30] In addition, several commenters argued that generic terms in domain names do not represent a problem and that ICANN has no reason to dictate business models.[31]

The underlying issue relates in part to concepts that are known from trademark law. It is generally not possible to register as a trademark a term that is generic for the goods or services identified in the applied-for mark; therefore, someone who sells apples can typically not register 'apple' as a trademark. However, unrelated generic terms can be registered, as illustrated by the trademark for Apple computers.[32] Thus, specific rules exist in trademark law, but ICANN had not solved this issue before opening for TLD applications.

ICANNs policy debates of closed generic TLDs seem to have started in 2012, after the applications and the intended business models became known. Arguably, at least two factors have contributed to this issue remaining open despite the issue being raised after application submissions. First, the expression 'public interest' in Section 6 of the Code of Conduct is sufficiently open to accommodate a variety of interpretations. It was thus possible to argue that the acceptance of closed gTLDs was contrary to public interest. A second reason is arguably related to the governmental advice received at ICANN. ICANN's Governmental Advisory Committee (GAC) can issue advice to the ICANN board, and the GAC has made ample use of this authority in relation to gTLDs.[33] If the GAC reaches a consensus and advises ICANN that a particular application should not proceed, this creates the strong presumption for the ICANN board that the application should not be approved.[34] Because the GAC's authority is not clearly delimited, [35] the GAC has taken the opportunity to make broad policy recommendations, including those regarding closed gTLDs.

In its Beijing Communiqué, the GAC expressed concern with strings representing generic terms being operated as exclusive access registries and advised that 'for strings representing generic terms, exclusive registry access should serve a public interest goal'.[36] The GAC identified a long list of strings that represent generic terms for which applicants proposed providing exclusive registry access, including <.antivirus>, <.app>, <.autoinsurance>, <.baby>, <.beauty>, <.blog>, <.book> and <.broker>.

Reacting to governmental advice, ICANN decided in June 2013 on a moratorium for closed generic strings pending a dialogue with the GAC.[37] Thus far, this has not been lifted. This means that applicants insisting on a closed gTLD do not proceed to contracting even though they may have met all the other criteria. At the same time, ICANN introduced additional contractual limitations for registry operators not seeking to impose exclusivity.[38] Accordingly, the 'Registry Operator of a "generic string" TLD may not impose eligibility criteria for registering names in the TLD.'[39] Interestingly, ICANN also developed a definition for a 'generic string': 'a string consisting of a word or term that denominates or describes a general class of goods, services, groups, organizations or things, as opposed to distinguishing a specific brand of goods, services, groups, organizations or things from those of others'.[40]

One interpretation of this new rule is that the term 'book' is a generic string in <.book> when describing a class of goods, while 'apple' is not a generic string when distinguishing the computer manufacturer's brand name in <.apple>. It remains to be seen whether this will have implications for brand holders with names that can also be generic. On the other hand, it seems as if no leeway is currently given for the exclusive use of a generic string when it is used as a generic word or term. In other words, while it may be too early to declare closed gTLDs as definite failures, the business model has a very uncertain future.

3.4 CONSEQUENCES AND WAY FORWARD

As a consequence of the problems facing closed generic TLDs, several applicants have completely withdrawn their applications. These include, for example, Safeway's application for <.grocery> and Heinz's application for <.ketchup>. Others, such as Amazon[41] and Google[42], filed change requests with ICANN to facilitate the transition from closed to open TLD. Some actors may thus still see some utility in pursuing an open TLD application, while others may simply conclude that significant investments in these projects are lost.

At this point, this paper might have considered in greater detail why these applicants chose to apply for closed gTLDs in the first place or considered the role gTLDs should have in a global trademark strategy. A third possibility would be to discuss how ICANN's processes could be improved to avoid such failures in the future.

Instead, the story of these failures will be used as a starting point for reflections about legal methodology. What methods, if any, do lawyers use to proactively manage such risks? What is the role of legal advice in a context of legal uncertainty such as the one described here?

4. HOW COULD THESE RISKS BE PROACTIVELY MANAGED?

At this point, we invite the reader to participate in a small thought experiment. The year is 2010 and you are a lawyer working for a pharmaceutical corporation intending to improve its global marketing platform by applying for the closed gTLD <.pharma>. A group of lawyers and other experts is tasked to assess the risks related to such a project. As a starting point, we should look at the methodological toolbox you are equipped with. As a lawyer, you have a good understanding of many relevant legal issues. Let us also assume that you can count on a sufficiently good understanding of the complexity of ICANN's rules and the processes for decision-making. This good, but you would presumably also need some methods to identify and assess risks.

There are a number of useful starting points for your task of assessing risk. First, nature has endowed humans with a number of instinctive responses to risk, and fear does play an important role in our decision-making. These instinctive responses to risk were developed early in our evolutionary history and have allowed us to handle many risky situations in our daily lives. On the other hand, fear is not always the best guidance, and our instinctive responses may not necessarily serve us best when we face a difficult decision in a complex environment. Applying for a closed gTLD involves legal and technology issues and has implications for budget and future strategy.

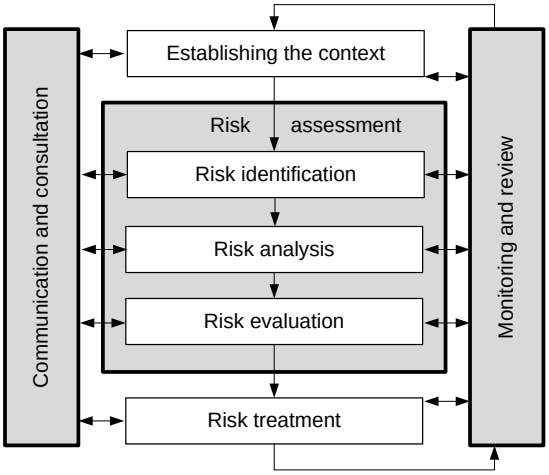
For the remainder of this paper, the reader is therefore invited to consider a second strategy. Would it be possible and useful to apply standard risk management practices to assess the legal risks of applying for a closed gTLD? You may wonder what use this can possibly have because we already know that closed gTLDs are not a viable business model. However, this involves a dangerous hindsight bias. It is always much easier to draw conclusions *ex post facto*. This thought experiment only works if the reader adopts a perspective from 2010, when closed gTLDs still appeared as a potentially viable and definitely attractive business model for many large corporations.

In the following sections, we review what risk management methods entail and why they may be particularly relevant here. Once review is complete, we examine the standard risk management approach to determine what adaptations should be made to address the legal context.

4.1 RISK MANAGEMENT

The International Standardization Organization (ISO) defines risk management as a set of 'coordinated activities to direct and control an organization with regard to risk'.[43] Risk management is intended to aid decision-making by considering uncertainty and its effect on objectives. In the context of an organization, risk management can be understood as a form of management activity. However, risk management is not necessarily limited to the management of organizations. Risk for an individual or risk related to a system can also be managed through dedicated activities outside any clearly determined organizational context.

Figure 1: Risk management process (ISO)



The kernel of this ISO standard is a dedicated risk management process[44] consisting of the systematic application of management policies, procedures and practices to the tasks illustrated in Figure 1.[45] The process includes tasks in three columns, with the centre column being the most important. Risk management begins by establishing the focus of the analysis (the 'context') before concentrating on risk assessment and then risk treatment. For example, the risk related to a particular project (e.g. transporting humans to Mars) can be assessed by identifying the risk (what could go wrong), analysing each risk (if it is a high risk) and evaluating the risk (can the risk be accepted) before concluding with risk treatment (e.g. if the risk is not acceptable either improve the technology or drop the project). When NASA assesses the risks involved in space travel, they apply standardized processes because they presume that they are 'critical to mission success'.[46]

4.2 THE NEED FOR LEGAL RISK MANAGEMENT

Applicants for new gTLDs need to carefully assess and manage risks. From the applicant's perspective, relevant risks can be related to the business model, the applicant's financial situation or operational, technical and legal issues.

The assessment of legal risks, which is the key focus of this paper, is essential for any applicant for at least two reasons. First, it should be in the applicant's interest to identify and manage legal risks in an early phase while cost-efficient proactive action is still possible. Thus, decision-makers should have an incentive to manage risks in their own interest. Typically, this is taken into account rather informally by incorporating legal advice and being proactive in identifying and addressing possible future problems. However, it is also possible to put more effort into identifying and assessing risks by adopting some methods from standard risk management; this idea is explained further below. The reason for a more structured approach is the presumption that a well-structured, systematic approach to risk management under optimal conditions may

lead to a better outcome. Moreover, a structured approach to managing risk does not need to fully replace informal ways of handling of risk; several approaches can complement each other.

Traditionally, many lawyers have not adopted standardized risk management processes. However, this does not necessarily mean that such processes do not exist. Legal risk management approaches have been used to assess legal risks in parts of the financial market[47] and legal risk management frameworks have been used in the public sector.[48] In addition there are approaches for the analysis of contractual risks.[49]

One reason for implementing risk management is the requirement making such practises obligatory. Many industries and contexts have risk management requirements, focusing on financial risk, enterprise risk, IT security risk, etc. The interesting aspect of gTLD applications is that ICANN's application rules also include an explicit requirement to assess legal risks.[50] All applicants were required to assess their legal risks when preparing a mandatory contingency plan for their applications. Applicants were evaluated based on a scoring system; to achieve the highest score, they had to show that they had thoroughly identified key risks, including legal risks.[51] The applicant's risk assessment is an important source of input for the mandatory contingency plan, which must address many types of contingencies, including legal risks. Thus, in preparing the contingency plan, all applicants had to carry out a legal risk assessment and consider 'the impact of any regulation, law or policy that might impact the Registry Services'. [52] Applicants also had to 'describe the measures to mitigate the key risks'.[53] Thus, a good legal risk assessment was essential, and an application could ultimately have been rejected if the contingency plan was found to be insufficient.[54] We can assume that all applicants made some effort to identify legal risks. However, the identified legal risks and the proposed mitigations are unknown because those parts of the applications were not made publicly available.

The specific legal risks related to a TLD application inevitably depend on the characteristics of the project, including factors such as the intended business model, the potential for conflict due to name sensitivity and third parties' rights. The choice of a more risky business model or a TLD name with specific sensitivities—such as <.gay>—should affect the overall risk picture. The same should be true for a risky business model such as a closed generic TLD.

4.3 LEGAL RISK MANAGEMENT

The following section provides a snapshot of a generic method used to identify and assess legal risks. The relevance and usability of this method does not depend on the characteristics of any specific project, but it would be possible and useful to adapt this approach to the relevant context. Moreover, the method is not set in stone; it contains only an initial suggestion that should be used as a starting point for future method developments.

As a point of departure, a legal risk assessment can be performed based on a standard risk management approach, e.g. as in enterprise risk management. Generally speaking, the aim of all legal risk management is the adequate management of risk in the legal context. In principle, legal risk management is a sufficiently general method to be suitable and useful for a broad range of contexts (e.g. projects or contracts) in which legal risk is relevant. However, it is particularly

relevant for the new TLD context because legal risk management is a mandatory part of the application process.[55]

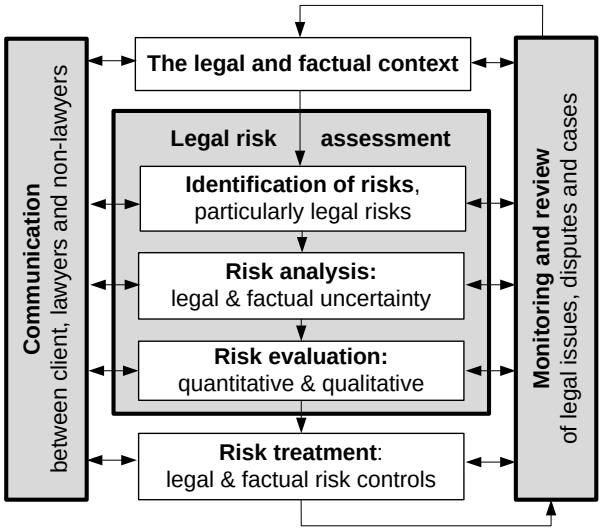
The approach is only briefly sketched here. It is explained in detail blow in Section 5, where the method is applied in the context of analysing legal risks related to closed generic TLDs.

The proposed approach is not intended as a replacement for existing methods used by lawyers but rather as a complementary approach. Lawyers already identify and control risks, but it is necessary to integrate such practices with established risk management methods practised in other fields. This section explains one possible approach for applying legal risk management by building on the state-of-the-art risk management standard ISO 31000.[56] In short, this standard states that risks should be managed by employing a systematic approach for their identification, analysis and evaluation.

When risk management is applied with a focus on legal issues, it can be called legal risk management. However, the labels used for an activity are less important than what is actually done. This might, alternatively, be called 'integrating legal issues into enterprise risk assessment' because the legal issues are only a subset of issues for an organization to tackle. However, it is a general practice in risk management to use a label identifying the focus of a risk assessment (e.g. financial risk management, project risk management); therefore, we can use the term 'legal risk management' if we manage the integration with other perspectives.

The proposed approach for legal risk management can be organized based on the above-mentioned general risk management process described in ISO 31000. It consists of five discrete process steps and two continuous practices (Figure 2).

Figure 2: Legal risk management process



The process commences by establishing the legal and factual context. For example, a legal risk assessment could commence with a description of the new TLD project in the relevant legal

context. During this stage, an examination of the applicable law should occur. In the TLD context, we may have to ask what rules ICANN has defined for new TLDs and how such rules can be changed. In addition, the contractual context of the project should be reviewed. It is important to establish the legal context, because this is the basis for identifying and analysing legal risk.

The next block is the risk assessment, which is the heart of the process and consists of three steps. First, risk is identified, including legal risk. The risk identification is envisaged here as a brainstorming activity in which qualified experts contribute their knowledge and experience. In essence, the brainstorming should concentrate on what may happen in the project and assessing this under the law. We do not need to limit ourselves to 'hard law'; soft law may also carry risks. In the TLD context, ICANN's rules for TLD applications are difficult to classify into existing categories, but that should not stop us from assessing their potential effect on the project. Therefore, 'law' should arguably be defined as wide as possible at this point, and a good case may be made to include ethical considerations or certain social expectations. Of particular relevance in the present context is how the application of the law may lead to a significant loss (monetary or other) for the applicant. For example, if the proposed project raises concerns with respect to the permissibility of the underlying business model under ICANN rules, the risk identification should describe how the application of such a law could lead to a negative outcome for the applicant.

In the second step, the identified risks are analysed, estimating risk levels. In other words, every identified risk should be examined to establish whether it is, for example, a high risk or a low risk. This risk level depends in practice on the likelihood of the risk's occurrence and the severity of the risk's consequences. For example, if it is very likely that the closed TLD business model cannot be used because it infringes on ICANN rules and if this has severe consequences for the applicant, then we could say this is a high risk. If we believe it is unlikely that the application might not proceed because of a potential intellectual property conflict (which would need to be further explained), then this is a low risk.

Once the identified risks have been analysed, we can proceed to the third step: the risk evaluation, which involves making decisions about risk. At this stage, the results of the risk analysis are evaluated with reference to the applicant's risk criteria. A decision-maker may be risk aversive or risk seeking, and such a preference can be incorporated into the risk evaluation criteria. Based on these criteria, some risks may be acceptable and others may need to be treated. For example, one could accept a low risk but not a high risk.

The discrete process concludes with the risk treatment, which identifies risk controls and selects controls that should be implemented. Both legal and other risk controls should be considered. To manage the identified risks, the applicant might consider slightly amending the business model or (re)negotiating particularly risky contractual agreements if these options are available. A contingency budget may also be useful to ensure that the applicant can handle the risk if it materializes. If the risks are too high, the project may have to be abolished.

5. CASE STUDY

The previous section began with a thought experiment inviting the reader to assume the position of a lawyer in a pharmaceutical company applying for the closed gTLD <.pharma>. As mentioned above, this only works if we use the perspective from 2010, when closed gTLDs seemed to be attractive, although slightly uncertain, business models. Let us take this thought experiment a step further. How could a lawyer in that position have applied standard risk management practices to assess the legal risks related to the <.pharma> closed gTLD project?

This section explains how the identified legal risks can be assessed by applying the above-mentioned steps of the risk management process, including risk identification, risk analysis, evaluation and treatment.[57]

5.1 THE LEGAL CONTEXT

This analysis commences by establishing the context and delimiting what will be analysed. While it may be challenging to define the scope of the risk assessment in other contexts, this should not be the case when assessing a new TLD project, which must be described clearly in the application for a TLD.

The ISO risk management standard distinguishes between the internal and external context of risk assessment. The external context includes, in particular, the legal and contractual framework within which the TLD will be operated. As a minimum, the contractual context comprises the prospective registry agreement between the applicant and ICANN as well as any agreements with other involved parties, such as technology providers.

The internal context is the internal environment in which the organization seeks to achieve its objectives. Such objectives are regularly extra-legal and result from the organization's internal decision-making. It is important to understand such objectives to help in the identification of risk. In the ISO risk management vocabulary, risk is defined as the 'effect of uncertainty *on objectives*' (emphasis added).[58] Therefore, understanding objectives is important.

Presumably, the objectives pursued by a TLD project are partly related to the mission, or purpose, of the TLD and partly reflect the applicant's financial projections.[59] For example, the purpose of the imaginary TLD <.pharma> may be to offer domain names to all entities within its corporate structure. This would generate a competitive advantage over other actors in the same industry, who would be excluded from registering domains.

5.2 LEGAL RISK IDENTIFICATION

The risk identification aims at generating a comprehensive list of risks that form the basis of further risk assessment. As pointed out by the ISO, standard risk identification focuses on events that affect the organization's ability to achieve its objectives and seeks to discover aspects such as the sources of risk, areas of impact, and the causes and potential consequences of certain events.[60] When identifying legal risk, we can apply a similar approach.

As a starting point, 'legal risk' can be defined as a risk that has a legal issue as its source.[61] A 'legal issue' is simply a set of circumstances (or facts) that are assessed under the law. To identify legal risk, we must determine how a potential legal issue can give rise to risk. This means, in practice, that we must discover the outcome of a legal issue in some kind of 'event'.[62] For example, the legal issues with closed TLDs might lead an applicant to withdraw the application and lose all their investments in the project. At this point, the legal issue becomes visible because someone is applying the law with specific consequences for the stakeholder whose risk we are assessing.

In the context of the <.pharma> application, the risk could be that the applicant has to withdraw the application, because it becomes clear that there is no possibility of achieving the intended objective. We saw above that some applicants for closed gTLDs (Amazon and Google) did not withdraw their application but changed them from closed to open. Presumably, this would not be a viable choice for a typical pharmaceutical company unless it wants to develop a new domain name sales division. Thus, if the TLD <.pharma> cannot be used exclusively, the project would likely be considered a failure.

At this point we can observe an important difference between legal risk and other risk. In other contexts risk typically relates to external events (such as earthquakes, or financial crises) that harm the stakeholder. This is why the ISO standard 31000 speaks of an 'event'. In comparison it is characteristic for legal risk that the outcome 'event' can be much more subtle, because it can consist in the stakeholder's own action in recognition of his or her legal position. The example of closed generic TLD applicants shows that they probably withdrew or amended their applications because they understood that the rules do not allow the achievement of their goal. No external involvement—beyond clarifying the rules—was necessary.

On the other hand, legal risk can also involve external actions. Legal risk can materialise in any kind of legal action or decision, such as the termination of a contract, a lawsuit or a court decision. An example of an external act for the TLD context is ICANN's potential decision to terminate the registry agreement, which would effectively imply the loss of the TLD.[63]

It may even be easier to identify legal risk by focusing on potential actions of other parties, rather than having to focus on one's own actions. For example, in the context of closed generic TLDs being disallowed under the Code of Conduct, one could have focused on ICANN's potential rejection of an application for an exemption under the Code of Conduct.[64]

A variety of different methods and approaches could be used to identify legal risk. A starting point could be a checklist of typical legal issues that can be examined to assess the relevance of each issue. In addition or as an alternative, an interdisciplinary group of experts could employ certain risk identification techniques[65] of a more open nature, such as structured brainstorming. For example, a risk analyst may guide the discussions of a group of experts, focusing on particular aspects of the TLD project. The structuring element for a brainstorming session could be law-centred, i.e. focusing primarily on the legal and contractual framework, or facts-centred, i.e. focusing on the plan for the TLD project. The latter perspective could, for example, consider potential technical problems caused by the new TLD.

For the sake of the example, we will focus on the law-centred approach. Guiding questions should thus focus on selected legal rules. Relevant rules should be addressed in terms of their likely impact on the project. Guiding questions could, for example, include the following:

- Is this plan permitted? For example, in the closed gTLD context one might ask whether an exclusive use of a gTLD string is permitted under ICANN rules or under competition law.
- What would be the consequences of non-compliance with this rule? For example, one could focus on certain restrictions for using a TLD and consider the potential consequences.
- What facts could trigger this rule? For example, ICANN has a contractual right to terminate the registry agreement, which would lead to the loss of the TLD.[66] Brainstorming could focus on whether a situation might arise in which ICANN would have a reason to act on this authority.

The risk identification should be concluded by documenting the identified risks. In general terms, a legal risk can be described based on (i) some facts, (ii) a legal assessment thereof and (iii) the description of a resulting 'outcome'.[67] Table 1 shows these factors for one risk.

Table 1: Risk description for Risk 1

Facts	The TLD <.pharma> is planned to be used exclusively by a pharmaceutical corporation while excluding others.
Legal assessment	Such exclusive use of a gTLD string might not be permitted under ICANN's rules (Section 6 of the Code of Conduct).
Outcome	The applicant may be forced to withdraw the application or make potentially costly changes to its business model, because the intended objective cannot be achieved.

The risk described in Table 1 is based on our current insight regarding what has actually happened with closed gTLD applications. In a more realistic setting, we would have to carry out a broader risk identification, which would likely show several risks. Table 2 provides an abbreviated, simplified list of potential legal risks that could result from a quick brainstorming exercise.

Table 2: Risk table

Risk #	Abbreviated description
Risk 1:	ICANN could prohibit the exclusive use of the generic string (see details in Table1).
Risk 2:	A competition authority or court could require the TLD applicant to open up the <.pharma> TLD to competitors in the pharmaceutical industry.[68]
Risk 3:	ICANN could terminate the registration agreement because of some infringement by the TLD Registry Operator.[69]

So far, a number of risks are identified. They require further analysis.

5.3 RISK ANALYSIS

In the ISO framework, risk analysis is a process (i) to comprehend the nature of risk and (ii) to determine the level of risk. The latter is the magnitude of a risk and is usually expressed in terms of the combination of consequences and their likelihood. For example, the consequences of a plane crash or an automobile accident might be the loss of life. The differences in likelihood that exist between these two risks are the determinant for the respective risk level. Similarly, legal risk analysis is envisaged here to consist of two corresponding aspects. First, to comprehend the nature of the legal risk, we must analyse the uncertainty with respect to the legal issue. Second, we can estimate the risk level on this basis.

Let us first address the uncertainty with respect to the legal issue. We can distinguish between legal uncertainty (uncertainty about the law) and uncertainty about other aspects ('empirical uncertainty'). An example of empirical uncertainty is whether the TLD string will lead to technical problems. This may be uncertain, but it does not depend on a legal issue.

The recent experiences with closed gTLDs provide a good example of what might be included in legal uncertainty. Arguably, the applicants did not necessarily understand at the time of application that closed gTLDs were not permissible under ICANN's rules. This became clearer when existing rules were clarified and new developments led ICANN to introduce new rules (see section 3.3). The challenge is to understand what is uncertain, why it is uncertain and whether potential ways exist for reducing uncertainty. For example, it might be possible to access additional legal expertise to better understand the problem or an applicant could have asked ICANN this question in advance. However, it is typically not possible to reduce all uncertainty, and one must make a decision based on what is known so far. The uncertainty can then be incorporated into a likelihood estimate.

Once we have described and analysed the uncertainty regarding the legal issue, we may estimate the risk level of the identified risks. Risk can be estimated in many ways, but for the purposes of the present paper we will refer to the simplest method, in which the risk level is calculated by multiplying the values of the estimated likelihood and the estimated consequences.[70] The most common approach for estimating risk is to use a risk matrix, such as the one shown in Table 3, which relates the likelihood and consequence of an event.

Table 3: Risk matrix showing combined risk level[71]

		CONSEQUENCE				
		Minor	**Minor**	**Moderate**	**Major**	**Severe**
LIKELIHOOD	**Very likely**	Medium	High	High	Critical	Critical
	Likely	Medium	Medium	High	High	Critical
	Possible	Low	Medium	Medium	High	High
	Unlikely	Low	Medium	Medium	Medium	High
	Rare	Low	Low	Medium	Medium	Medium

In general, the values in risk matrices can be quantitative (using numbers) or semi-qualitative (as in the example in Table 3). If semi-qualitative values are chosen, it is advisable to clarify their meaning in the respective context. For example, a qualitative value such as 'major' may be defined as being equivalent to an approximate sum of money (e.g. CAN$1 million) even in cases involving too much uncertainty to make exact calculations. What counts as a respectively major or catastrophic consequence depends on the views of the stakeholder assuming the risk. Thus, this is not a legal issue, and it could be left for others to decide.

For the sake of the example, we could relate the consequence levels to the above-mentioned objectives within the project. If the focus is on project success, i.e. the ability to have a closed gTLD <.pharma>, then we might assume that the total loss of all investments in the project could be called 'severe'. For the sake of the example, we disregard the possibility of a refund of application costs.

Table 4 provides estimated risk levels for the three risks identified. The risk level depends on the consequence value and the likelihood value.

Table 4: Risk table showing risk levels

Risk	Likelihood	Consequence	Risk level
Risk 1	Very likely	Severe	Critical
Risk 2	Unlikely	Severe	High
Risk 3	Rare	Severe	Medium

All three risks involve the complete loss of the <.pharma> TLD, which would be severe. Estimating a likelihood level might be more difficult because it should be assessed in light of the respective legal issues. In a realistic scenario, it would be expected that the experts involved might hold divergent opinions on likelihood values, leading to the need to agree on a consensus estimate.

5.4 RISK EVALUATION

While risk identification and risk analysis focus mostly on understanding the risk, evaluation is the first step towards making decisions about the risk. The function of the risk levels is to assist in making decisions about whether and how to treat the risk. In its simplest form, the evaluation is a comparison of the initially defined risk criteria with the results of the risk analysis. Based on this comparison, the need for treatment can be considered.[72]

According to the ISO, risk criteria are defined as 'terms of reference against which the significance of a risk is evaluated'.[73] In practice, risk evaluation is often based on the risk level in the sense that a risk level above a certain threshold must be treated. For example, risk criteria could state that a critical risk must be treated (risk 1), a high risk should be treated (risk 2) and a medium risk must be monitored (risk 3).

5.5 RISK TREATMENT

Risk treatment is the process of developing, selecting and implementing 'risk controls'.[74] In extreme cases, the risks may be so high that the treatment may need to include an assessment of whether the TLD project should be discontinued. Alternatively, the treatment options may be less drastic and include removing a source of risk, changing its nature or likelihood, changing the consequences or sharing the risk. The latter could include transferring the risk to another contract party or to a third party, such as an insurance company.

Preferably, the risk treatment should take a holistic approach that integrates a variety of practical risk controls. It may also be useful to assess the effect of each risk control. In practice, a technical or financial change may have legal implications, and changes to the contract may carry technical, financial or business implications, which the multidisciplinary risk assessment team can discuss. The final step within the treatment phase is then to prepare and implement a treatment plan that lists the details of the selected controls.

How should legal risks in the <.pharma> case be treated? Risks 1 and 2 are based on the exclusive use of the generic string in the TLD. One option would be to open up the TLD to competitors; however, this would imply a completely different business model, which may no longer be attractive for an applicant interested in a closed gTLD. Another alternative could be to apply for a trademarked name rather than a generic word. If this alternative is not chosen, there seem to be few alternatives to abolishing the project.

6. DISCUSSION AND CONCLUDING REMARKS

This paper has discussed the proactive assessment of legal risks in the context of new TLDs. Thus, our focus was on some of the concrete legal issues highlighted by new TLDs and, at a meta-level, on methodological issues related to the use of risk management in the legal context.

Clearly, introducing risk management methods requires time and effort. Lawyers who wish to apply legal risk management must learn a new set of methods, which is always challenging and can be costly. Therefore, one should carefully consider the potential benefits. There is reason to believe that a legal risk assessment of the kind described here may significantly contribute to the success of a project if risks are identified and managed adequately. If risks can be foreseen, a systematic method should enable us to manage legal risks proactively, which would likely lead to long-term benefits.

The quality of the risk assessment results depends both on the quality of the methodology and on the quality of the input into the assessment process. Let us start with the latter. First, an adequate risk assessment requires good input. Therefore, one needs to involve individuals with experience about and knowledge of the domain in question. However, few individuals have a comprehensive understanding of all the relevant aspects of a complex business contract. A lawyer can analyse the contract clauses and the applicable law but often lacks detailed operational knowledge of the project. Similarly, technical or financial experts may lack detailed information about the legal consequences of technical or other problems. Therefore, it may be

useful to carry out a legal risk assessment with a suitable multi-disciplinary team of experts as appropriate, including lawyers, managers, financial experts and/or IT specialists. The use of risk management in the legal context can often be integrated with other risk management approaches in adjacent disciplines, such as project risk management or enterprise risk management.

The utility of legal risk management also depends on the quality of the employed risk assessment methods. The assessment should examine if the method works in practice and is sufficiently adaptive to address a variety of legal issues. Risk management promises an approach to future legal problems that is intended to be more systematic and structured than the traditional approaches followed by many[75] practising lawyers. On the other hand, the introduction of systematic risk management approaches for the assessment of legal problems is a rather recent phenomenon, and our experiences are, so far, limited. It is likely that the methods seen so far, including the approach described above, would benefit from future research and development. The case study in this paper demonstrates that it is possible to apply standard risk management to the analysis of legal problems.

From a research perspective, it is difficult to ascertain whether the results of a risk assessment are sufficiently good or useful. How should this be judged? One solution could be to ask risk assessment participants whether they believe that the risk assessment improved their understanding of the risks and their decision making. Participants in a previous case study indicated that this was the case.[76] Another option is to assess a case in which a legal risk has materialized, e.g. the case of closed gTLDs. Is it realistic that this risk (risk 1) could have been identified through systematic risk identification?

Any applicant for a TLD had access to the ICANN gTLD applicant guidebook, which contained not only the application rules but also the draft registry agreement, including the Registry Operator Code of Conduct. A careful reading of this document should have revealed that a TLD holder (a registry operator) is forbidden to register domain names in its own right and that it could be difficult to fulfil the requirements for an exemption. My personal assessment is of little significance in this context, but it might help illustrate the point. I was not aware of closed gTLDs before the deadline for applications, so I did not comment on this issue before 2012. However, once the applications and business models became known in 2012, I pointed out the legal risks, including this one.[77] Thus, I would argue that this risk could have been identified.

If applicants did estimate this risk as critical, they should have abandoned the project unless they were highly risk-seeking. Indeed, it is possible to argue that the potential benefits of acquiring a closed gTLD would be so large that a very high risk is acceptable. This could be one explanation for the fact that so many large corporations chose to apply.

It is also possible that some applicants for closed gTLDs might have underestimated the likelihood of this risk affecting them. Consequently, they might have estimated the risk level to be lower, thus resulting in an acceptable risk. While this possibility exists, this would not lower the utility of the risk management method. We cannot guard against misjudgement as long as we employ our best effort to identify, estimate and manage risks. The approach described in this article is intended to achieve exactly that.

[1] Associate Professor, Norwegian Research Center for Computers and Law, University of Oslo, tobias.mahler@jus.uio.no. The article was written in the framework of a research project titled 'Governance of the Domain Name System and the Future Internet: New Parameters, New Challenges' ('Igov2'), which is jointly funded by the Norwegian Research Council and UNINETT Norid AS (see http://www.jus.uio.no/ifp/english/research/projects/internet-governance/). Thanks are due to my colleagues on the 'Igov2' project, particularly Lee Bygrave, Emily Weitzenboeck, Samson Esayas and Kevin McGillivray. This article is dedicated to the memory of Professor Jon Bing, under whose supervision the author commenced the research of legal risk management.

[2] Regarding ICANN's policymaking see, e.g., Weitzenboeck, E (2014), 'Hybrid Net: the Regulatory Framework of ICANN and the DNS', International Journal of Law and Information Technology 22(1), 49-73.

[3] See Bygrave, L A and Bing, J (2009), Internet Governance: Infrastructure and Institutions (Oxford: Oxford University Press).

[4] See Manheim, K M and Solum, L B (2003) 'An Economic Analysis of Domain Name Policy' Loyola-LA Public Law Research Paper No 2003-14 http://ssrn.com/paper=410640; Mueller, M (2002), *Ruling the Root: Internet Governance and the Taming of Cyberspace* (Cambridge: MIT Press); Mueller, M (2010), *Networks and States: The Global Politics of Internet Governance* (Cambridge: MIT Press); Null, E and Prahl, D (2011) 'The New Generic Top-Level Domain Program: A New Era of Risk for Trademark Owners and the Internet' Trademark Reporter 101, 1757.

[5] For an overview see ICANN (2011), gTLD Applicant Guidebook, Version 2011-09-19, Module 1.

[6] See Borchert, B W (2011), 'Imminent Domain Name: The Technological Land-Grab and ICANN's Lifting of Domain Name Restrictions', Valparaiso University Law Review 45:2, 505-49 http://scholar.valpo.edu/vulr/vol45/iss2/3; Easton, C (2012), 'ICANN's Core Principles and the Expansion of Generic Top-Level Domain Names', International Journal of Law and Information Technology 20, 273-290 http://ijlit.oxfordjournals.org/content/20/4/273.full.pdf

[7] It is also worth mentioning that the application guidebook provides rules prioritizing 'community-based' applications, which are supported by the members of a community and presumably apply to specific situations, such as the Vatican applying for the TLD <.catholic>. The community priority evaluation is described in ICANN (2011), gTLD Applicant Guidebook, Version 2011-09-19, Section 4.3.2 of Module 4. The TLD <.catholic> is only used as a potential example; the Vatican did not have competition for its application, but it would, arguably, have prevailed in a contention set. Many community priority evaluations (e.g. <.gay>, <.music>, <.taxi>) ended without giving priority to the claimed community. In addition, restrictive rules are in place regarding certain geographical names that are either excluded (country names such as <.sweden>) or that require support or express non-objection from a local authority (e.g. <.london>); see ICANN (2011), gTLD Applicant Guidebook, Version 2011-09-19, Module 2, Section 2.2.1.4. See further McGillivray K (2012) 'Anticipating Conflict—An Evaluation of the New gTLD Dispute Resolution System', 9:2 SCRIPTed 195.

[8] Specification 9, Registry Operator Code of Conduct, Section 6, in Module 5 of ICANN (2011), gTLD Applicant Guidebook, Version 2011-09-19. See further below Section 3.1.

[9] 'Generic.' Merriam-Webster.com. n.d. Web. 8 Dec 2014. http://www.merriam-webster.com/dictionary/generic.

[10] See e.g. Corwin, P (2012), 'New gTLDs: Competition or Concentration? Innovation or Domination?' DomainNameNews. http://www.domainnamenews.com/new-gtlds/new-gtlds-competition-or-concentration-innovation-or-domination/11833. Accessed 18 January 2013.

[11] This large group of 'regular' applications encompasses both open (as opposed to closed) TLDs and strings that are not 'generic'. However, it remains to be seen what 'generic' means in this context. This is further discussed in the next sections.

[12] See Module 5 of ICANN (2011), gTLD Applicant Guidebook, Version 2011-09-19.

[13] Regarding the successful TLD applicants' rights to new TLDs, see Mahler, T (2014), 'A gTLD Right? Conceptual Challenges in the Expanding Internet Domain Namespace', International Journal of Law and Information Technology 22(1), 27-48.

[14] See Section 2.14 of the Draft Registry Agreement as specified in Module 5 of ICANN (2011), gTLD Applicant Guidebook, Version 2011-09-19.

[15] Specification 9, Registry Operator Code of Conduct, Section 6, in Module 5 of ICANN (2011), gTLD Applicant Guidebook, Version 2011-09-19.

[16] See ProMark Brands' (a subsidiary of H.J. Heinz Company) answer to question 18(a) in the application for <.ketchup>, available at https://gtldresult.icann.org/application-result/applicationstatus/applicationdetails/1683. Accessed 10 December 2014.

[17] See Google's answer to question 18(a) in the application for <.blog>, available at http://gtldresult.icann.org/application-result/applicationstatus/applicationdetails/527. Accessed 30 January 2013. Note that Google filed the application under the name Charleston Road Registry Inc.
[18] See Specification 9, Registry Operator Code of Conduct, Section 6(iii), in Module 5 of ICANN (2011), gTLD Applicant Guidebook, Version 2011-09-19.
[19] A wide interpretation here would fit well with the narrower notion of 'limited public interest' used elsewhere in the applicant guidebook. The applicant guidebook uses the phrase 'limited public interest', which is a subset of a public interest that can be the basis for an objection. This is narrowly related to 'whether the applied-for gTLD string is contrary to general principles of international law for morality and public order'; see ICANN (2011), gTLD Applicant Guidebook, Version 2011-09-19, Module 3, Section 3.5.3. From the difference in formulation (the Code of Conduct does not refer to 'limited' public interest), it might be argued that ICANN should apply a wider notion of public interest in the context of the Code of Conduct.
[20] See L'Oreal's answer to question 18(a), available at http://gtldresult.icann.org/application-result/applicationstatus/applicationdetails/1027. Accessed 30 January 2013.
[21] See L'Oreal's answer to question 18(a), available at http://gtldresult.icann.org/application-result/applicationstatus/applicationdetails/1027. Accessed 30 January 2013.
[22] See Murphy, K (2012), 'Industry Objection Forming to Google and Amazon's Keyword gTLD Land Grab' Domain Incite. http://domainincite.com/10525-industry-objection-forming-to-google-and-amazons-keyword-gtld-land-grab. Accessed 30 January 2013.
[23] ICANN, '"Closed generic" gTLD Applications', http://www.icann.org/en/news/public-comment/closed-generic-05feb13-en.htm. Accessed 06 February 2013.
[24] ICANN (2013), 'Report of Public Comments, "Closed Generic" gTLD Applications', p. 10, https://www.icann.org/en/system/files/files/report-comments-closed-generic-08jul13-en.pdf. Accessed 15 December 2014.
[25] ICANN (2013), 'Report of Public Comments, "Closed Generic" gTLD Applications', p. 11, https://www.icann.org/en/system/files/files/report-comments-closed-generic-08jul13-en.pdf. Accessed 15 December 2014.
[26] ICANN (2013), 'Report of Public Comments, "Closed Generic" gTLD Applications', p. 11, https://www.icann.org/en/system/files/files/report-comments-closed-generic-08jul13-en.pdf. Accessed 15 December 2014.
[27] ICANN (2013), 'Report of Public Comments, "Closed Generic" gTLD Applications', p. 11, https://www.icann.org/en/system/files/files/report-comments-closed-generic-08jul13-en.pdf. Accessed 15 December 2014.
[28] ICANN (2013), 'Report of Public Comments, "Closed Generic" gTLD Applications', p. 13, https://www.icann.org/en/system/files/files/report-comments-closed-generic-08jul13-en.pdf. Accessed 15 December 2014.
[29] ICANN (2013), 'Report of Public Comments, "Closed Generic" gTLD Applications', p. 15, https://www.icann.org/en/system/files/files/report-comments-closed-generic-08jul13-en.pdf. Accessed 15 December 2014.
[30] ICANN (2013), 'Report of Public Comments, "Closed Generic" gTLD Applications', p. 18, https://www.icann.org/en/system/files/files/report-comments-closed-generic-08jul13-en.pdf. Accessed 15 December 2014.
[31] ICANN (2013), 'Report of Public Comments, "Closed Generic" gTLD Applications', p. 19, https://www.icann.org/en/system/files/files/report-comments-closed-generic-08jul13-en.pdf. Accessed 15 December 2014.
[32] See e.g. EU law, Council Regulation (EC) No 207/2009 from 26 February 2009 on the community trademark Article 7(1)(c).
[33] For an overview of governmental advice regarding new gTLDs, see ICANN's overview at http://newgtlds.icann.org/en/applicants/gac-advice. Accessed 15 December 2014.
[34] See Section 3.1 of Module 3 in ICANN (2011), gTLD Applicant Guidebook, Version 2011-09-19.
[35] See Section 3.1 of Module 3 in ICANN (2011), gTLD Applicant Guidebook, Version 2011-09-19. See further regarding the GAC's role, Weinberg, J (2011), 'Governments, Privatization, and "Privatization": ICANN and the GAC' Michigan Telecommunications and Technology Law Review 18, 189-218, http://www.mttlr.org/voleighteen/weinberg.pdf.

[36] Governmental Advisory Committee (2013), 'Beijing Communiqué', Annex I, P. 11, available at https://www.icann.org/en/system/files/correspondence/gac-to-board-18apr13-en.pdf. For further information see also https://newgtlds.icann.org/en/applicants/gac-advice/cat2-safeguards. Accessed 15 December 2014.
[37] ICANN New gTLD Program Committee (2013), Resolution 2013.06.25.NG06, https://www.icann.org/resources/board-material/resolutions-new-gtld-2013-06-25-en#2.c.
[38] ICANN New gTLD Program Committee (2013), Resolution 2013.06.25.NG04, https://www.icann.org/resources/board-material/resolutions-new-gtld-2013-06-25-en#2.c. The 'Proposed PIC Spec Implementation of GAC Category 2 Safeguards' (20 June 2013) were attached as Annex I to this Resolution and subsequently incorporated into the Registry Agreement as Specification 11, Section 3 lit. c. and d.
[39] Registry Agreement, Specification 11, Section 3 lit. d.
[40] Registry Agreement, Specification 11, Section 3 lit. d.
[41] Originally, Amazon's mission statement (according to question 18 on the application form) for <.book>, <.author> and <.music> was as follows: 'Provide Amazon with additional controls over its technical architecture, offering a stable and secure foundation for online communication and interaction.' This is now changed to a more open statement: 'Offer a stable and secure foundation for online communication and interaction.' See changes to question 18. Amazon's <.music> application is available at https://gtldresult.icann.org/applicationstatus/applicationchangehistory/966.
[42] Google has made a change to their application. Original: 'The purpose of the proposed gTLD, .blog, is to provide a dedicated Internet space where Google can continue to innovate on its Blogger offerings.' Updated: 'The mission of the proposed gTLD is to provide a dedicated domain space in which users can publish blogs.' See answer to question 18a. Both versions are available at https://gtldresult.icann.org/applicationstatus/applicationchangehistory/527.
[43] The ISO has defined a general risk management vocabulary and a universal risk management process in the ISO 31000. Both documents provide a good overview of key concepts and processes in risk management, independent of any specific organizational or other context. The key concept is risk, which is simply defined as 'the effect of uncertainty on objectives' (see ISO, Guide 73: Risk Management—Vocabulary (2009) Section 1).
[44] ISO 31000 (n 43)13 et seq; ISO Guide 73 (n 43) Section 3.1.
[45] Figur can be seen as the common ground for many risk analysis approaches. It originated from Standards Australia and Standards New Zealand, Risk Management AS/NZS 4360:2004 (2004). It was subsequently adopted by ISO 31000 (n 43).
[46] NASA, NASA Risk Management Page, http://www.hq.nasa.gov/office/codeq/risk/. Accessed 4 December 2014.
[47] See e.g. McCormick, R (2010), Legal Risk in the Financial Markets (Oxford: Oxford University Press).
[48] Department of Justice (Canada) (2013), Legal Risk Management in the Department of Justice, http://www.justice.gc.ca/eng/rp-pr/cp-pm/eval/rep-rap/08/lrm-grj/p2.html#sec22.
[49] See Mahler T (2010), 'Legal Risk Management: Developing and Evaluating Elements of a Method for Proactive Legal Analyses, With a Particular Focus on Contracts ' (Oslo: University of Oslo).
[50] ICANN (2012), gTLD Applicant Guidebook, Evaluation Questions and Criteria, Question 49, p. A-41 http://newgtlds.icann.org/en/applicants/agb. Accessed 30 January 2013.
[51] ICANN (2011), gTLD Applicant Guidebook, Version 2011-09-19, Attachment to Module 2, Question 49, pp. A-39 et seq.
[52] ICANN (2011), gTLD Applicant Guidebook, Version 2011-09-19, Attachment to Module 2, Question 49, pp. A-39 et seq.
[53] ICANN (2011), gTLD Applicant Guidebook, Version 2011-09-19, Attachment to Module 2, Question 49, pp. A-39 et seq.
[54] ICANN (2011), gTLD Applicant Guidebook, Version 2011-09-19, Attachment to Module 2, Question 49, pp. A-39 et seq.
[55] See ICANN (2011), gTLD Applicant Guidebook, Version 2011-09-19, Evaluation Questions and Criteria, Question 49, p. A-41 http://newgtlds.icann.org/en/applicants/agb. Accessed 30 January 2013.
[56] ISO (2009), International Standard ISO 31000. Risk Management—Principles and Guidelines on Implementation. See further Mahler T (2010), 'Legal Risk Management: Developing and Evaluating Elements of a Method for Proactive Legal Analyses, With a Particular Focus on Contracts ' (Oslo: University of Oslo), 43.
[57] Technically, risk treatment is not part of the risk assessment but follows as a subsequent step. However, it is included here to simplify the presentation.

[58] As mentioned above, this is the risk definition used in ISO Guide 73 (n 43) Section 1.
[59] The objectives must also be explained in the TLD application. See ICANN (2011), gTLD Applicant Guidebook, Version 2011-09-19, Attachment to Module 2, question 18.
[60] See ISO 31000 (n 43) Section 5.4.2.
[61] Mahler T (2010), 'Legal Risk Management: Developing and Evaluating Elements of a Method for Proactive Legal Analyses, With a Particular Focus on Contracts ', 76 et seq.
[62] ISO defines 'event' as the occurrence or change of a particular set of circumstances. See ISO Guide 73 (note 17) Section 3.5.1.3.
[63] This remedy is available, for example, under the Registry Restrictions Dispute Resolution Procedure (RRDRP), which is incorporated in the Registry Agreement with ICANN. ICANN (2011), gTLD Applicant Guidebook, Version 2011-09-19, Module 5.
[64] See above Section 3.2.
[65] See ISO, 31010 Risk Management—Risk Assessment Techniques (2009).
[66] See Section 4.3 of the Registry Agreement, available in ICANN (2011), gTLD Applicant Guidebook, Version 2011-09-19, Module 5.
[67] In terms of the 'events' arising from a legal issue, the risk description would usually seem to include either a legal decision or the consequences of a legal decision.
[68] This risk would require further analysis. In brief, this issue can be illustrated in two recent cases from Germany and the United States.
In the case of *Volkswagen v. Denic* (OLG Frankfurt, 29 April 2008, Kommunikation und Recht 2008, 449 et seq.) the German courts decided that the registry for <.de>, Denic, was not permitted to deny the domain name vw.de to the car manufacturer Volkswagen despite alleged potential technical problems with delegating a two-letter domain name. This ruling was essentially based on the court's view that Denic had dominant market power in the relevant market for German domain names. According to the court, the TLD <.de> has a special position in the German domain name market because the TLD denotes the abbreviation for Germany. As the dominant actor in this market, Denic is prohibited from engaging in unjustified discrimination of other undertakings. This had already been stated in the earlier decision by the same court (see OLG Frankfurt, 13.12.2007 [11 U 24/6 (Kart)]). In practice, this means that the law limits to some extent how Denic can delegate and administrate domain names. Furthermore, any discriminated undertaking may seek legal recourse in court. It must be emphasized, however, that this case is specifically related to the market situation of Denic in Germany. Arguably, it might be more difficult to argue for market dominance in the context of a gTLD compared to a ccTLD.
The practical relevance of these issues can be further illustrated by the recent litigation about the use of the TLD <.xxx> in the case of *Manwin et al. v. ICM*. United States District Court, Central District of California, Case CV 11-9514 PSG, 14 August 2012 (see law.com blog post 'Big Porn. Big Web Ruling Could Spell Trouble for ICANN'
http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202567792748&slreturn=2012072806357
). The TLD <.xxx> was delegated in 2011 after a long process of debate and deliberations at ICANN. It is dedicated to, but opposed by parts of, the 'adult entertainment industry'. The plaintiffs are part of this industry but oppose the TLD; they claimed that this forces them to defensively register their names. Moreover, the plaintiffs claimed that the registry for <.xxx> has reserved some of the most interesting names for itself or sells these at prices above those in a competitive market in violation of US and Californian antitrust and competition law. The case was settled, so the underlying issue has not been clarified.
[69] See Section 4.3 of the Registry Agreement, available in ICANN (2011), gTLD Applicant Guidebook, Version 2011-09-19, Module 5.
[70] The ISO states that 'risk is often expressed in terms of a combination of the consequences of an event or change of circumstances, and the associated likelihood of occurrence' (see ISO Guide 73 (n 43) Section 1, Note 3).
[71] Adapted version of risk matrix in Standards Australia and Standards New Zealand, Risk Management Guidelines Companion to Australian/New Zealand Standard AN/NZS 4360: 2004 (HB 436:2004) (Sydney, Australia/Wellington, New Zealand: Standards Australia/Standards New Zealand 2004) 55
[72] ISO 31000 (n 43) Section 5.4
[73] See ISO Guide 73 (n 43) Section 3.3.1.3, emphasis added
[74] ISO Guide 73 (n 43), Section 3.3.7

[75] We cannot disregard the possibility that many legal practitioners have already adopted and adapted more risk management practices than so far noted by scholars.
[76] See Mahler T (2010), 'Legal Risk Management: Developing and Evaluating Elements of a Method for Proactive Legal Analyses, With a Particular Focus on Contracts ' 237 et seq.
[77] Mahler, T (2012), 'New Top-Level Domains and Legal Risks', in A Gunn and B Bekken (eds.) Dag Wiese Schartum, Yulex, Norwegian Research Center for Computers and Law, 163-185.