Article #:030030	Date: **2011 年 11 月 15 日**
Article Name: 评估问题 30：安全策略	AGB Reference:none
Version #:v01	Category:Knowledge Article – Evaluation Questions

1. 补充说明：

2011 年 11 月 15 日

1.1 对于问题 30(a)：

- 安全级别由申请人确定。申请人需按照确定的安全级别，列出其将向目标注册人作出的承诺。同时还应提交针对所列各承诺的简要说明。
- 独立评估报告应证明针对 IT 基础架构（将用于注册管理机构业务的运营）的安全控制办法有效。申请人的回应应陈述独立评估报告中要求协调的任何被强调部分。请注意，ICANN 将不会公布独立评估报告。

1.2 对于问题 30(b)，则必须提供仅侧重于申请人注册管理机构业务的安全策略和程序。鉴于此类信息性质敏感，ICANN 将不会公布申请人的安全策略。

2. 最佳做法建议：

2011 年 11 月 15 日

2.1 申请人应完整地阅读每个评估问题，包括其说明、标准及评分文本。答案应解决所有指定的标准，并包括证明对标准已充分理解的详细理由（即展示您所做的工作）。

2.2 若使用缩写，申请人应在缩写首次出现时拼出全名，即便该缩写表示的是常见的术语/产品/服务。

2.3 建议将注册管理机构业务中一个或多个职能外包的申请人必须解决各个相关问题中指出的所有标准，并包括证明对标准已充分理解的详细理由（即展示您所做的工作）。

2.4 只提供简历不会被视为可证明技术/运营能力，也不能确立资源已到位的“证据”。申请人应提供资源配置计划的详细说明，其中应包括诸如管理/运行职能所需的资源、必备技能、招聘计划等方面。简历可用于补充提议的资源配置计划。

2.5 申请人若在答案中引用了某项政策/程序，则应提供该类政策/程序的摘要。除非有特别要求，否则申请人不应附上所引用政策/程序的副本。

2.6 如果申请人提出定制开发软件，则应明确包括软件开发流程在内的定制范围和程度。明确说明可以帮助评估小组了解定制软件的完整性。

3. 问题文本：

(a) 为计划建立的注册管理机构提供一份安全策略摘要，其内容包括但不限于：

- 指出能够证明安全性能的任何独立评估报告以及定期进行独立评估报告以测试安全性能的规定；
- 描述与所申请的 gTLD 字符串性质相适应的任何扩增的安全级别或功能，其中包括认同申请人承诺遵守的任何当前的国际或行业相关标准（必须提供参考网站）；
- 列出向注册人作出的关于安全级别的承诺。

若要获得 2 分的合格成绩，答案还必须包括：

- 表明安全控制办法（例如，ISO 27001）有效的独立评估报告的证明资料。

上述内容的总结不应超过 20 页。请注意，针对注册管理机构的完整安全策略应根据问题 30(b) 提交。

(b) 针对计划建立的注册管理机构提供完整的安全策略和程序，包括但不限于：

- 确保维持系统安全运转的系统（数据、服务器和应用程序/服务）和网络访问控制（包括系统监控、日志记录、备份方式的详细说明）；
- 保护注册管理机构系统和名称服务器之间更新的完整性以及不同名称服务器之间更新（如有）的完整性的资源；
- 证明安全性能的独立评估报告（如有，以附件形式提交）；
- 为缓解拒绝服务攻击造成的风险而采用的预防手段和其他措施；
- 计算机和网络事故响应策略、计划和流程；
- 最大程度降低未经授权的系统访问或注册管理机构数据被篡改的风险；
- 入侵检测机制，针对计划建立的注册管理机构所面临的威胁的分析和应对这些威胁而部署的防范措施，以及定期更新威胁分析数据的规定；
- 有关针对所有网络访问的审查能力的详细说明；
- 物理安全措施；
- 指定对注册管理机构的安全组织负责的部门或团体；
- 对安全人员进行的背景核查；
- 说明已确认的对注册管理机构运营的主要安全威胁；以及
- 用于标准中此方面的初步实施和持续维护的资源配置计划（分配到该方面的职员数量与职能描述）。


ICANN
NewgTLDs