Appendix A - HSTLD Control Worksheet

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
Principle#1: The Registry maintains effective controls to provide reasonable assurance that the security, availability, and confidentiality of systems and information assets supporting critical registry IT (i.e., registration services, registry databases, zone administration, and provision of domain name resolution services) and business operations are maintained by performing the following: ** defining and communicating performance objectives, policies, and standards for system and information asset security, availability, confidentiality, and privacy; ** utilizing procedures, people, software, data, and infrastructure to achieve defined objectives in accordance with established policies and standards; and ** monitoring the system and information assets and taking action to achieve compliance with defined objectives, policies, and standards.				**Principle #1 Illustrative Control Examples**			
1.1	Key elements of the IT components that support the TLD infrastructure are secured and appropriately protected from unauthorized physical and logical access.	1.1.1	Responsibility and accountability for the entity's Information System assets containing customer data is maintained according to defined procedures.	All assets that are in-scope for registry operations should be clearly identified and an inventory of all in-scope assets drawn up and maintained.	ISO 27002 - 7.1.1	Asset Management	1. Information asset classification and associated security controls, especially, for sensitive information processing systems/devices 2. Asset Management system should be in place for tracking all information assets (if applicable) 3. Sensitive documentation to be labeled per the data classification policy and handled in accordance with the entity's data classification scheme 4. Systems/devices (laptops, servers, routers etc.) to be
				All information and assets associated with information processing facilities for registry operations should be owned by a designated part of the organization.	ISO 27002 - 7.1.2	Asset Management	1. Ownership of in-scope assets should be clearly identified and documented. 2. Asset Management system should contain ownership information (if applicable) 3. There should be a policy/procedure in place to update ownership as part of the periodic update to the list of managed assets that are in-scope

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
				Rules for the acceptable use of information and assets associated with information processing facilities for registry operations should be identified, documented, and implemented. Appropriate personnel should be informed about such rules and be trained on them periodically	ISO 27002 - 7.1.3	Asset Management	1. Asset Management/Data Classification policy/procedures should documented and enforced 2. Asset Management/Data Classification policy/procedures should be communicated and trained upon as part of the periodic (e.g. annually) employee/contractor training and awareness program
				Information should be classified in terms of its value, legal requirements, sensitivity, and criticality to the organization.	ISO 27002 - 7.2.1	Asset Management	1. Asset Management/Data Classification policy/procedures should list the criteria applicable to classify information and assets in to various categories
				An appropriate set of procedures for information labeling and handling should be developed and implemented in accordance with the classification scheme adopted by the organization. Appropriate personnel should be informed about such procedures and be trained on them periodically	ISO 27002 - 7.2.2	Asset Management	1. Asset Management/Data Classification policy/procedures should documented and enforced 2. Asset Management/Data Classification policy/procedures should be communicated and trained upon as part of the periodic (e.g. annually) employee/contractor training and awareness program
				Procedures for the handling and storage of information should be established to protect this information from unauthorized disclosure or misuse.	ISO 27002 - 10.7.3	Communications And Operations Management	sensitive information should be encrypted in storage and procedures to achieve the same should be documented and communicated

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
		1.1.2	The entity's information systems network is monitored and managed to maintain defined service levels and security requirements.	Networks should be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.	ISO 27002 - 10.6.1	Communications And Operations Management	1. Network devices, such as: Routers, switches, firewalls, load balancers etc. should be configured to protect the server and application infrastructure. 2. Network devices should be monitored to alert respective personnel regarding the health of the network and any attacks 3. IPS can also be looked at to know whether it has been configured to automatically change network device configurations on detecting specific attacks (E.g. DDOS attack on DNS server infrastructure)
				Security features, service levels, and management requirements of all network services should be identified and included in any network services agreement, whether these services are provided in-house or outsourced.	ISO 27002 - 10.6.2	Communications And Operations Management	The management should facilitate identifying the security features and service level requirements of all network services, particularly for the DNS server infrastructure
				Information involved in electronic messaging should be appropriately protected.	ISO 27002 - 10.8.4	Communications And Operations Management	Sensitive information transferred via email (including attachments) between registrants, registrars and/or registration authority and registry, should be protected using appropriate technical controls (network encryption, file encryption, email encryption etc.)
				Information involved in on-line transactions should be protected to prevent incomplete transmission, mis-routing, (Encryption requirements) unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	ISO 27002 - 10.9.2	Communications And Operations Management	Network, DNS server and Application infrastructure should be configured and managed appropriately, and made resilient in order to prevent incomplete transmission, mis-routing etc. Encryption controls in section below

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
Appropriate authentication methods should be used to control access by remote users.	ISO 27002 - 11.4.2	Access Control	1. Two-factor authentication for remote connectivity. 2. Two-factor authentication for access to critical systems like: Directory services, DNS infrastructure (server, network, application) OR 2. Separate management network restricted to specific source IPs should be used for administrative functions on Network, DNS servers etc.,
Automatic equipment identification should be considered as a means to authenticate connections from specific locations and equipment.	ISO 27002 - 11.4.3	Access Control	Laptops, desktops and other client devices (smart phones etc.) should be authenticated at the LAN layer
Physical and logical access to diagnostic and configuration ports should be controlled.	ISO 27002 - 11.4.4	Access Control	Console access to the DNS infrastructure (Network, Servers and Applications) should be restricted to appropriate personnel - this might include physical access to DC, cage access to specific devices/systems etc. Devices/ Systems should be configured to have inactive configuration ports, which can be activated for specific purposes by relevant personnel with appropriate access This can be partly covered under physical security
Groups of information services, users, and information systems should be segregated on networks.	ISO 27002 - 11.4.5	Access Control	Network should be logically separated based on the services offered y that subnet. E.g. DNS servers could have a separate subnet with specific rules for the network traffic traversing the subnet

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
				For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network should be restricted, in line with the access control policy and requirements of the business applications.	ISO 27002 - 11.4.6	Access Control	Any dedicated/shared network links between registry and registrars and/or registration authority should be configured to allow minimal administrative access, based on business needs. Further, specific network rules should be configured to allow only certain type of network traffic
				Routing controls should be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.	ISO 27002 - 11.4.7	Access Control	This includes network routers, switches, load-balancers and firewalls
				A formal policy should be in place, and appropriate security measures should be adopted to protect against the risks of using mobile computing and communication facilities.	ISO 27002 - 11.7.1	Access Control	Corporate LAN configuration should prevent foreign laptops or smart phones from being able to connect to the Corporate network This should be mentioned in relevant policy and enforced. Can be partly covered under security management
				A policy, operational plans and procedures should be developed and implemented for teleworking activities.	ISO 27002 - 11.7.2	Access Control	Policies/procedures should be in place for use of network by personnel with teleworking job profiles (E.g. remote connectivity, sending unencrypted attachments or emails etc.) Can be partly covered under security management
				Formal exchange policies, procedures, and controls should be in place to protect the exchange of information through the use of all types of communication facilities.	ISO 27002 - 10.8.1	Communications And Operations Management	Can be partly covered under security management
		1.1.3	Procedures exist to protect against access to the entity's systems from unauthorized	An access control policy should be established, documented, and reviewed based on business and security requirements for access.	ISO 27002 - 11.1.1	Access Control	One can consider including provisions for special access requirements for the overall DNS infrastructure (Servers, Network and Applications)

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria
			users and malicious processes.

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
There should be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.	ISO 27002 - 11.2.1	Access Control	One can consider including provisions for special provisioning requirements for the overall DNS infrastructure (Servers, Network and Applications) and personnel with specific responsibilities
The allocation and use of privileges should be restricted and controlled.	ISO 27002 - 11.2.2	Access Control	Access provisioned based on principle of least privilege
The allocation of passwords should be controlled through a formal management process.	ISO 27002 - 11.2.3	Access Control	Password mgmt could be more strict for overall Registry Operations Infrastructure
Management should review users' access rights at regular intervals using a formal process.	ISO 27002 - 11.2.4	Access Control	Access review could be more frequent for overall Registry Operations Infrastructure
Users should be required to follow good security practices in the selection and use of passwords.	ISO 27002 - 11.3.1	Access Control	Stronger passwords may be needed for overall Registry Operations Infrastructure
Users should ensure that unattended equipment has appropriate protection.	ISO 27002 - 11.3.2	Access Control	Computer/Laptop locks, password protected screen savers etc.
A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted.	ISO 27002 - 11.3.3	Access Control	Privacy screens, no passwords on post it notes etc.
Users should only be provided with access to the services that they have been specifically authorized to use (at the Network Layer)	ISO 27002 - 11.4.1	Access Control	User access could be restricted to specific subnets or logical networks, particularly for Registry Operations Infrastructure
Access to operating systems should be controlled by a secure log-on procedure.	ISO 27002 - 11.5.1	Access Control	Two-factor based authentication for system-level access for Registry Operations
All users should have a unique identifier (user ID) for their personal use only, and a suitable authentication technique should be chosen to substantiate the claimed identity of a user.	ISO 27002 - 11.5.2	Access Control	Two-factor based authentication for application-level access for Registry Operations

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
Systems for managing passwords should be interactive and should ensure quality passwords.	ISO 27002 - 11.5.3	Access Control	self-service password reset. Also, password reset requests over the phone should require user to answer multiple security questions to establish user identity, particularly for Registry Operations Infrastructure
The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled.	ISO 27002 - 11.5.4	Access Control	Access provisioned only to relevant personnel and via 2-factor authentication for Registry Operations Infrastructure
Inactive sessions should shut down after a defined period of inactivity.	ISO 27002 - 11.5.5	Access Control	Includes: VPN connectivity, connection to Registry Operations Infrastructure (remote administrative access over the management network or via 2-factor authentication)
Restrictions on connection times should be used to provide additional security for high-risk applications.	ISO 27002 - 11.5.6	Access Control	Registry Operations Infrastructure (Server, Network and Applications) may be considered to be made available during specific times, based on business need
System documentation should be protected against unauthorized access.	ISO 27002 - 10.7.4	Communications And Operations Management	Should be labeled appropriately and handled accordingly. E.g. Shredded on site by a vendor or by internal personnel etc.
The integrity of information being made available on a publicly available system should be protected to prevent unauthorized modification.	ISO 27002 - 10.9.3	Communications And Operations Management	Registry and Registrar entities should: - remain alert and collect intelligence on phishing emails to registrants, - monitor modification of content on their web site by malicious users etc. - monitor fraudulent websites that resemble registry or registrar website.

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
		1.1.4	Application systems and remote sessions carrying sensitive data are authenticated and validated according to established requirements.	Access to information and application system functions by users and support personnel should be restricted in accordance with the defined access control policy.	ISO 27002 - 11.6.1	Access Control	principle of least privilege
				Sensitive systems should have a dedicated (isolated) computing environment.	ISO 27002 - 11.6.2	Access Control	Registry Operations Infrastructure could be in a separate logical network
				Statements of business requirements for new information systems, or enhancements to existing information systems should specify the requirements for security controls.	ISO 27002 - 12.1.1	Information Systems Acquisition, Development And Maintenance	Security requirements should be considered from the initial stages of acquiring new systems or enhancing existing systems
				Data input to applications should be validated to ensure that this data is correct and appropriate.	ISO 27002 - 12.2.1	Information Systems Acquisition, Development And Maintenance	Input validation controls
				Validation checks should be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.	ISO 27002 - 12.2.2	Information Systems Acquisition, Development And Maintenance	Input validation controls to include checks for SQL injection etc. Processing errors should result in standardized error messages that do not contain sensitive information or information on OS version, Database server version, the backend code (SQL) etc.
				Requirements for ensuring authenticity and protecting message integrity in applications should be identified, and appropriate controls identified and implemented.	ISO 27002 - 12.2.3	Information Systems Acquisition, Development And Maintenance	Applications in the Registry Operations Infrastructure should contain controls/checks for validating the integrity of processed data. The input validation controls should incorporate controls for validating the authenticity of the entity providing that data
				Data output from an application should be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.	ISO 27002 - 12.2.4	Information Systems Acquisition, Development And Maintenance	Applications in the Registry Operations Infrastructure should contain controls/checks for validating the results from data processing and for displaying it in a standardized format/manner

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
		1.1.5	Procedures exist to safeguard on-line information sessions through the use of cryptographic authentication or equivalent security techniques. Policies containing these procedures are communicated to relevant personnel periodically.	A policy on the use of cryptographic controls for protection of information should be developed and implemented.	ISO 27002 - 12.3.1	Information Systems Acquisition, Development And Maintenance	The policy should specifically mention the required standards for cryptographic controls particularly for the Registry Operations Infrastructure
				Key management should be in place to support the organization's use of cryptographic techniques.	ISO 27002 - 12.3.2	Information Systems Acquisition, Development And Maintenance	The Key management infrastructure should require similar standards for Network Security, Access Control, Application Security etc., as the Registry Operations Infrastructure
				Policies and procedures should be developed and implemented to protect information associated with the interconnection of business information systems. These policies and procedures should be communicated periodically and acknowledged by relevant personnel	ISO 27002 - 10.8.5	Communications And Operations Management	This could be partly covered under Security Management and Personnel Security
				Information involved in electronic commerce passing over public networks should be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.	ISO 27002 - 10.9.1	Communications And Operations Management	Information passing over internet should be encrypted, based on the standards defined in the policy on cryptographic controls
				Information involved in on-line transactions should be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	ISO 27002 - 10.9.2	Communications And Operations Management	Online transactions should be secured using SSL with a defined minimum encryption strength and assurance level (E.g. Only EV SSL Certificates may be allowed to be used by Registry or Registrar for collecting information from the Registrant). This could be partly covered by Network Security (incomplete transmission, mis-routing etc.)

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
		1.1.6	Design, acquisition, implementation, configuration, managemetn and modification of systems infrastructure and software related to operational systems are consistent with defined security policies to prevent unauthorized access and system modification.	There should be procedures in place to control the installation of software on operational systems.	ISO 27002 - 12.4.1	Information Systems Acquisition, Development And Maintenance	Privilege to install software on desktops/laptops/devices should be restricted to relevant personnel
				Test data should be selected carefully, and protected and controlled.	ISO 27002 - 12.4.2	Information Systems Acquisition, Development And Maintenance	Test data should not contain PII, credit card or bank account information etc.
				Access to program source code should be restricted.	ISO 27002 - 12.4.3	Information Systems Acquisition, Development And Maintenance	SoD should be implemented between development and production environments. Further, access to program code should be restricted to relevant personnel
				The implementation of changes should be controlled by the use of formal change control procedures.	ISO 27002 - 12.5.1	Information Systems Acquisition, Development And Maintenance	Third party to assess the change control procedure and inspect the change tickets and emergency change tickets. Composition of CAB needs to be evaluated. And, the statistics containing the no. of emergency changes v/s deliberate changes should be analyzed
				When operating systems are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	ISO 27002 - 12.5.2	Information Systems Acquisition, Development And Maintenance	Third party to assess the process followed to test the applications and inspect relevant documentation to validate whether: 1. Adequate test scenarios were considered 2. Results validated and bugs reported. 3. Bugs fixed before deployment 4. fixes for non-critical bugs slated for future application release

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
Modifications to software packages should be discouraged, limited to necessary changes, and all changes should be strictly controlled.	ISO 27002 - 12.5.3	Information Systems Acquisition, Development And Maintenance	Changes to application software configuration should be deliberated on, tested, documented and performed by relevant personnel
Opportunities for information leakage should be prevented.	ISO 27002 - 12.5.4	Information Systems Acquisition, Development And Maintenance	This could be considered as an umbrella control, which may include: 1. protection at Network layer, OS layer and Application layer 2. Application layer: E.g. processing errors should not be dumped on to the screen, which may reveal sensitive information etc.
Outsourced software development should be supervised and monitored by the organization.	ISO 27002 - 12.5.5	Information Systems Acquisition, Development And Maintenance	Outsourced software should undergo similar testing standards for confidentiality and integrity, as in house developed software (particularly, for registry operations)
Duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	ISO 27002 - 10.1.3	Communications And Operations Management	Developers should not have production access
Development, test, and operational facilities should be separated to reduce the risks of unauthorized access or changes to the operational system.	ISO 27002 - 10.1.4	Communications And Operations Management	Development, test, and operational facilities could be located in separate logical networks
Changes to information processing facilities and systems should be controlled.	ISO 27002 - 10.1.2	Communications And Operations Management	3rd party to assess whether any changes were made that were not accounted for. 3rd party could also inspect the standard changes that have been pre-approved by the entity in question and judge whether certain pre-approved changes need to be deliberated on by the CAB

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
It should be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.	ISO 27002 - 10.2.1	Communications And Operations Management	Entity should work closely with the 3rd party on any services being provided to ensure similar standards for security, service definitions and delivery levels
The services, reports and records provided by the third party should be regularly monitored and reviewed, and audits should be carried out regularly.	ISO 27002 - 10.2.2	Communications And Operations Management	
Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.	ISO 27002 - 10.2.3	Communications And Operations Management	This could be covered under Security Management
The use of resources should be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.	ISO 27002 - 10.3.1	Communications And Operations Management	Capacity planning meetings should be held periodically and notes documented
Acceptance criteria for new information systems, upgrades, and new versions should be established and suitable tests of the system(s) carried out during development and prior to acceptance.	ISO 27002 - 10.3.2	Communications And Operations Management	various requirements (including security) should be agreed on and documented during the initial stages of development or acquisition
Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures should be implemented.	ISO 27002 - 10.4.1	Communications And Operations Management	This could be considered as an umbrella control, which may include: 1. validation controls for preventing SQL injection etc. 2. Standardized error messages 3. Security Management: User awareness 4. etc.

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
				Where the use of mobile code is authorized, the configuration should ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code should be prevented from executing.	ISO 27002 - 10.4.2	Communications And Operations Management	
				Agreements should be established for the exchange of information and software between the organization and external parties.	ISO 27002 - 10.8.2	Communications And Operations Management	Security Management could cover this partially. The agreements should include requirements for: Confidentiality, Integrity and Availability of sensitive data and/or software service
				An acquisition of a 3rd party service or a software release should be accompanied by documented operating procedures which should be made available to all users who need them and maintained	ISO 27002 - 10.1.1	Communications And Operations Management	Documentation of an acquired system and how-to-use guidelines should be maintained, communicated and updated regularly
		1.1.7	Procedures exist to periodically test information systems according to defined security policies and take appropriate measures to address vulnerabilities.	Timely information about technical vulnerabilities of information systems being used should be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.	ISO 27002 - 12.6.1	Information Systems Acquisition, Development And Maintenance	consider vulnerabilities at all levels - system, network, app, database and also the aspect of deploying patches to fix the vulnerabilities discovered as part of the regular checking
		1.1.8	Procedures exist to monitor, identify, report, and act upon security breaches and incidents	Information security events should be reported through appropriate management channels as quickly as possible.	ISO 27002 - 13.1.1	Information Security Incident Management	The process of incident management and escalation needs to be assessed and evaluated. Further, one could inspect the SLAs for incidents at various severity levels and see if they satisfy the requirements for Registry/Registrar

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
All employees, contractors and third party users of information systems and services should be required to note and report any observed or suspected security weaknesses in systems or services.	ISO 27002 - 13.1.2	Information Security Incident Management	This could be part of Security Management-Employee Awareness and could be a specific training module for relevant personnel who work on Registry Operations Infrastructure One could assess and evaluate the process that is recommended to be followed for reporting any observed or suspected security weaknesses in systems or services
Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to information security incidents.	ISO 27002 - 13.2.1	Information Security Incident Management	The process of incident management and escalation needs to be assessed and evaluated. Further, one could inspect the SLAs for incidents at various severity levels and see if they satisfy the requirements for Registry/Registrar This could partly be covered by Security Management
There should be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.	ISO 27002 - 13.2.2	Information Security Incident Management	Statistics on the types, volumes, and costs of information security incidents should be available for inspection. One could look at the number of Sev-1 incidents over a period of time and perform trending to see if Sev-1 incidents have been increasing or decreasing
Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence should be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).	ISO 27002 - 13.2.3	Information Security Incident Management	Process for forensic investigation and maintaining chain of custody could be inspected and assessed. It could then be confirmed whether the process/procedures satisfy the requirements in the relevant jurisdiction

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
Audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring.	ISO 27002 - 10.10.1	Communications And Operations Management	Audit logs should be maintained for at least one year and should be protected against unauthorized access. Logs for Registry Operations Infrastructure may have greater needs for storage
Procedures for monitoring use of information processing facilities should be established and the results of the monitoring activities reviewed regularly.	ISO 27002 - 10.10.2	Communications And Operations Management	Access logs (physical and logical) should be reviewed regularly. Automated event correlation tools could be used and the signatures should be regularly updated to detect new patterns of events. In-house scripts could also be used, but should be accompanied by periodic updates to detect new patterns of events and a policy on updating such scripts should be documented and enforced
Logging facilities and log information should be protected against tampering and unauthorized access.	ISO 27002 - 10.10.3	Communications And Operations Management	only relevant personnel should have access to audit logs. The logs should not contain PII, financial information etc.
System administrator and system operator activities should be logged.	ISO 27002 - 10.10.4	Communications And Operations Management	logged and retained for the required amount of time
Faults should be logged, analyzed, and appropriate action taken.	ISO 27002 - 10.10.5	Communications And Operations Management	the process for analyzing logs and taking appropriate action should be inspected, and cases where action was needed and taken should be documented
DNS changes should be monitored for anomalies or abuse	APWG	Anti-phishing/Anti-Abuse	
The clocks of all relevant information processing systems within an organization or security domain should be synchronized with an agreed accurate time source.	ISO 27002 - 10.10.6	Communications And Operations Management	A reliable time source should be used for synchronization of time on all systems. One should inspected that multiple sources of time are not used. Further, only the relevant network port should provide the time service

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
		1.1.9	The entity's information system infrastructure is designed and managed to maintain DNS zone and name server availability and be current with solutions to know DNS vulverabilities.	DNS infrastructure should be robust and resilient to DDOS attacks	NA	DNS Security	This is an umbrella control that may be used to look at various aspects of the DNS infrastructure (Network, Server, Application etc.) and lead a professional opinion by the 3rd party performing the assessment for the HSTLD Certification Program. The following more specific controls (Rows 90-94) could be used by the 3rd party to assess configuration of the DNS server, the network infrastructure surrounding the DNS server, the patch management process for the DNS server and the implementation of DNSSEC
				DNS Open Resolver Configurations should be prevented or limited, based on the business need	NA	DNS Security	DNS open resolvers are vulnerable to multiple malicious activities, including the following: DNS cache poisoning attacks Denial of Service (DoS) or Distributed DoS (DDoS) Resource utilization attacks Some of the improvements could be to: 1. Permit Queries and Recursion only from Trusted Sources 2. Perform Randomization for UDP Source Port and Transaction Identifier 3. Segregate Authoritative and Recursive Resolvers 4. Set Maximum Cache Length and Maximum Cache Size

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
DNS server must be patched regularly, based on the criticality of the vulnerability and the patch management policy	NA	DNS Security	Vulnerabilities could be discovered by the periodic vulnerability testing exercises, alerts issued by vendors and Security forums. The vulnerabilities should be patched based on their criticality and patch management policy
DNSSEC should be implemented to counter vulnerabilities inherent in the DNS	NA	DNS Security	The major objective for DNSSEC is to provide the ability to validate the authenticity and integrity of DNS messages in such a way that tampering with the DNS information can be detected TLDs should have a strategic plan for implementing DNSSEC
Network infrastructure surrounding the DNS servers should be adequately managed and configured, in order to protect from DNS-specific threats and the information in transit	NA	DNS Security	Configurations of the Routers, Firewalls, Switches, Load-balancers etc., which are serving DNS traffic, should be assessed by the 3rd party to verify whether such network devices are configured to protect against DNS-specific threats. These network devices should also be configured to logically segregate the network containing DNS servers, so that network traffic traversing such a network can be better managed Further, the above mentioned network devices should be managed only by relevant personnel via 2-factor authentication or by using a separate management network with source-IP authentication

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
				DNS Infrastructure should be adequately monitored for the health of the systems and also, to alert respective personnel about DNS-specific events	NA	DNS Security	DNS Infrastructure (Network devices, servers etc.) should be configured to alert the respective personnel about any health and security related events. Further, monitoring systems (e.g. IDS) and event correlation tools should be configured to alert the relevant personnel about any events or trends that may affect the DNS infrastructure
		1.1.10	Information security policies and procedures are established and periodically reviewed and approved by a designated individual or group. Security policies are relevant documents are communicated to authorized users and personnel.	An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties.	ISO 27002 - 5.1.1	Security Policy	
				The information security policy should be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.	ISO 27002 - 5.1.2	Security Policy	
				Management should actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.	ISO 27002 - 6.1.1	Organization Of Information Security	
				Information security activities should be coordinated by representatives from different parts of the organization with relevant roles and job functions.	ISO 27002 - 6.1.2	Organization Of Information Security	
				All information security responsibilities should be clearly defined.	ISO 27002 - 6.1.3	Organization Of Information Security	
				A management authorization process for new information processing facilities should be defined and implemented.	ISO 27002 - 6.1.4	Organization Of Information Security	

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified and regularly reviewed.	ISO 27002 - 6.1.5	Organization Of Information Security	
Appropriate contacts with relevant authorities should be maintained.	ISO 27002 - 6.1.6	Organization Of Information Security	
Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained.	ISO 27002 - 6.1.7	Organization Of Information Security	
The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) should be reviewed independently at planned intervals, or when significant changes to the security implementation occur.	ISO 27002 - 6.1.8	Organization Of Information Security	
The risks to the organization's information and information processing facilities from business processes involving external parties should be identified and appropriate controls implemented before granting access.	ISO 27002 - 6.2.1	Organization Of Information Security	
All identified security requirements should be addressed before giving customers access to the organization's information or assets.	ISO 27002 - 6.2.2	Organization Of Information Security	

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
				Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities should cover all relevant security requirements.	ISO 27002 - 6.2.3	Organization Of Information Security	
		1.1.11	Procedures exist to safeguard secured assets through the use of employee roles, background validations, and security awareness training for employees, contractors, and thrid party users. Upon termination of employment, contract or agreement; personnel access to sensitive information is revoked.	Security roles and responsibilities of employees, contractors and third party users should be defined and documented in accordance with the organization's information security policy.	ISO 27002 - 8.1.1	Human Resources Security	
				Background verification checks on all candidates for employment, contractors, and third party users should be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.	ISO 27002 - 8.1.2	Human Resources Security	
				As part of their contractual obligation, employees, contractors and third party users should agree and sign the terms and conditions of their employment contract, which should state their and the organization's responsibilities for information security.	ISO 27002 - 8.1.3	Human Resources Security	
				Management should require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization.	ISO 27002 - 8.2.1	Human Resources Security	

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
				All employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.	ISO 27002 - 8.2.2	Human Resources Security	
				There should be a formal disciplinary process for employees who have committed a security breach.	ISO 27002 - 8.2.3	Human Resources Security	
				Responsibilities for performing employment termination or change of employment should be clearly defined and assigned.	ISO 27002 - 8.3.1	Human Resources Security	
				All employees, contractors and third party users should return all of the organization's assets in their possession upon termination of their employment, contract or agreement.	ISO 27002 - 8.3.2	Human Resources Security	
				The access rights of all employees, contractors and third party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change.	ISO 27002 - 8.3.3	Human Resources Security	
		1.1.12	Physical locations containing the entity's information systems infrastructure are designed to be secure and protected in	Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) should be used to protect areas that contain information and information processing facilities.	ISO 27002 - 9.1.1	Physical And Environmental Security	

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria
			accordance with defined policies.

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	ISO 27002 - 9.1.2	Physical And Environmental Security	
Physical security for offices, rooms, and facilities should be designed and applied.	ISO 27002 - 9.1.3	Physical And Environmental Security	
Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster should be designed and applied.	ISO 27002 - 9.1.4	Physical And Environmental Security	
Physical protection and guidelines for working in secure areas should be designed and applied.	ISO 27002 - 9.1.5	Physical And Environmental Security	
Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.	ISO 27002 - 9.1.6	Physical And Environmental Security	
Equipment should be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	ISO 27002 - 9.2.1	Physical And Environmental Security	
Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities.	ISO 27002 - 9.2.2	Physical And Environmental Security	
Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage.	ISO 27002 - 9.2.3	Physical And Environmental Security	

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
				Equipment should be correctly maintained to ensure its continued availability and integrity.	ISO 27002 - 9.2.4	Physical And Environmental Security	
				Security should be applied to off-site equipment taking into account the different risks of working outside the organization's premises.	ISO 27002 - 9.2.5	Physical And Environmental Security	
				All items of equipment containing storage media should be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.	ISO 27002 - 9.2.6	Physical And Environmental Security	
				Equipment, information or software should not be taken off-site without prior authorization.	ISO 27002 - 9.2.7	Physical And Environmental Security	
		1.1.13	Procedures exist to provide for backup, secure transport to offsite storage, and secure destruction of media which are consistent with related security policies.	Back-up copies of information and software should be taken and tested regularly in accordance with the agreed backup policy.	ISO 27002 - 10.5.1	Communications And Operations Management	
				There should be procedures in place for the management of removable media.	ISO 27002 - 10.7.1	Communications And Operations Management	
				Media should be disposed of securely and safely when no longer required, using formal procedures.	ISO 27002 - 10.7.2	Communications And Operations Management	
				Media containing information should be protected against unauthorized access, misuse or corruption during transportation beyond an organization's physical boundaries.	ISO 27002 - 10.8.3	Communications And Operations Management	

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
1.2	TLD services are available for use per contract or commitment.	1.2.1	Procedures exist to protect against potential risks (such as, environmental risks, natural disasters, labor disputes, and routine operational errors and omissions) that might disrupt system operations and impair system availability.	A managed process should be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity, while taking in to consideration the up time required for name resolution service to continue running in the case of an event	ISO 27002 - 14.1.1	Business Continuity Management	Business Continuity Plan should be developed and maintained
				Events that can cause interruptions to business processes should be identified, along with the probability and impact of such interruptions and their consequences for information security and the up time required for name resolution service to continue running in the case of an event.	ISO 27002 - 14.1.2	Business Continuity Management	Risk Assessment and BIA should be performed, and the availability requirements for name resolution service to continue running in the case of an event should be considered. The Risk Assessment and BIA should be performed periodically to accommodate for changes in business environment
				Plans should be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.	ISO 27002 - 14.1.3	Business Continuity Management	Disaster Recovery Program for restoring IT Operations should be developed and exercised periodically
				A single framework of business continuity plans should be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.	ISO 27002 - 14.1.4	Business Continuity Management	The BC Plans should not be developed for different business units in Isolation and the initial scope under consideration should be the whole organization, so that all risks to the business can be looked at comprehensively. The scope can then be broken down in to projects and a timeline can be associated with each one of them
				Business continuity plans should be tested and updated regularly to ensure that they are up to date and effective.	ISO 27002 - 14.1.5	Business Continuity Management	Leading practice is to test the BC and DR Plans at least annually. One could consider more frequent exercises for Registry Operations

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
		1.2.2	The entity is required to monitor and provide reports to relevent parties of service level metrics in accordance with specifications defined within the Registry Agreement.	The Service Level Agreement (SLA) should provide metrics and methods to measure performance of the HSTLD registry operator and/or backend registry service provider, and provide accredited and licensed registrars and/or registration authority with credits for certain substandard performance by the registry operator and/or backend registry service provider	NA	Service level agreements	
				The SLA should: 1. Define the terms used in the agreement 2. Define the responsibilities of the parties involved 3. Terms for providing credit to affected registrars and/or registration authority 4. Terms of dispute resolution 5. Use an Addendum for Miscellaneous/Additional items	NA		
				The HSTLD registry operator and/or backend registry service provider's Whois service should be available for free public query-based access at all times, unless availability requirements are specified as part of the Registry Agreement	NA	Whois service availability	
				The Registry Agreement should clearly specify the Whois performance requirements expected from the HSTLD registry operator and/or backend registry service provider and/or backend registry service provider.	NA	Whois service performance level	

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
				The HSTLD registry operator and/or backend registry service provider should provide ICANN with a Monthly (or periodic) Report, which should include: 1. The number of Whois queries during the reporting month 2. The amount of time for which the Whois service was available during the reporting month 3. Root cause for any Whois service interruptions observed during the reporting month 4. Additional performance requirements should be reported on, based on the specifications in the Registry Agreement	NA		
				The Registry Agreement should include provisions for conducting Whois performance tests by an independent, 3rd party. These provisions should include: 1. Providing the HSTLD registry operator and/or backend registry service provider with an advanced notification and the opportunity to evaluate the testing tools and procedures to be used by the independent, 3rd party 2. Written notification to the HSTLD registry operator and/or backend registry service provider containing the results of any testing within an agreed upon timeframe, including the method used for testing and the location of testing	NA		

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
The HSTLD registry operator and/or backend registry service provider should monitor and report on the response times for the Whois queries, based on performance specifications mentioned in the Registry Agreement	NA	Whois service response times	
The Registry Agreement should clearly specify the Whois performance requirements with respect to service response times expected from the HSTLD registry operator and/or backend registry service provider	NA		
The Registry Agreement should include provisions for conducting performance tests by an independent, 3rd party to measure and report on the Whois response times	NA		
HSTLD registry operator and/or backend registry service provider's Whois service should be the authoritative Whois service for all second-level Internet domain names registered in that HSTLD and for all hosts registered using those names	NA	Whois accuracy and completeness	
HSTLD registry operator and/or backend registry service provider should provide access to up-to-date data concerning domain name and nameserver registrations maintained by registry operator and/or backend registry service provider according to the requirements of the registry agreement. The specification of the content and format of this data, and the procedures for providing access, shall be according to the Registry Agreement	NA		

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
				HSTLD registry operator and/or backend registry service provider's Whois service and the Name Server infrastructure should be monitored for availability at all times by the HSTLD registry operator and/or backend registry service provider	NA	Availability monitoring	
				Appropriate monitoring tools should be configured and deployed to adequately serve the monitoring needs, and alert the relevant personnel on account of any events	NA		
				An escrow account should be established to deposit all data identified in the Registry Agreement between ICANN and the HSTLD registry operator and/or backend registry service provider	NA	Registration and transaction data escrow including escrow schedule, specifications, transfer, and Security Verification	
				The HSTLD registry operator and/or backend registry service provider should store in escrow a complete set of Data in an electronic format with Data Escrow Provider, to meet the Data Escrow requirements outlined in the Registry Agreement	NA		
				Data Escrow Provider should verify that the data is complete, accurate, and delivered in the intended format	NA		
				The escrow deposit verification process should validate completeness and integrity (accuracy) of the data as well as validate that the file format sent is the format received by Data Escrow Provider (correctness)	NA		

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
				Data should be securely and electronically transmitted at regular intervals, as outlined in the Registry Agreement	NA		
				Changes to the schedule, content, format, and procedure may be made only with the mutual written consent of ICANN and the HSTLD registry operator and/or backend registry service provider	NA		
				Escrow Agent/Provider should certify that it is allowed to receive the Deposit under the applicable Laws/Acts	NA		
1.3	Information owned, managed or transferred through the HSTLD has been assigned the appropriate level of classification, based on the HSTLD registry operator and/or backend registry service provider's classification scheme, and is protected as committed or agreed. Personal information collected by the HSTLD registry operator and/or backend registry service provider is collected, used, retained, disclosed, and destroyed appropriately, in line with relevant data protection laws per the jurisdiction of the HSTLD registry operator and/or backend registry service provider.			NOTE: The criteria topics and associated controls under this objective are covered by objective #1.1. The proposed criteria topics and associated controls under objective #1.1 will be updated and tailored for this purpose, based on the input from the HSTLD Advisory Group			
Principle#2: The Registry maintains effective controls to provide reasonable assurance that the processing of core Registry functions are authorized, accurate, complete, and performed in a timely manner in accordance with established policies and standards. The identity of participating entities is established and authenticated.				**Principle #2 Illustrative Control Examples**			

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
2.1	Registry operator and/or backend registry service provider credentials are made available to substantiate the identity of the legal entity that operates the TLD	2.1.1	Procedures exist to verify the validity of registry operator and/or backend registry service provider candidates according to defined requirements.	The HSTLD Sponsor should verify whether the background of the principals for the candidate registry operator and/or backend registry service provider are made available on the website or on request	NA	Background of principals	The background of principals could be maintained on the Entity's website and could also be provided separately on request. The background should include: 1. Summary of experience 2. Employment/Professional history 3. Professional accreditations 4. Professional associations
				The HSTLD Sponsor should identify and verify the background of at least one Principal Individual associated with the candidate registry operator and/or backend registry service provider (owners, partners, managing members, directors or officers)	WebTrust EV 1.1		
				The HSTLD Sponsor should verify whether the identified Principal Individual for the candidate registry operator and/or backend registry service provider (owners, partners, managing members, directors or officers) is not located in a country where it is prohibited from doing business	WebTrust EV 1.1		
				The HSTLD Sponsor should verify the physical address of the Place of Business for the candidate registry operator and/or backend registry service provider	WebTrust EV 1.1	Verifiable address	The physical address of the Place of Business could be maintained on the Entity's website and could also be provided separately on request.

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
The HSTLD Sponsor should obtain reasonable assurance about the physical existence and business presence of the candidate registry operator and/or backend registry service provider	WebTrust EV 1.1		
The HSTLD Sponsor should verify that the candidate registry operator and/or backend registry service provider's Place of Business is not in a country where it is prohibited from doing business	WebTrust EV 1.1		
The HSTLD Sponsor should verify the candidate registry operator and/or backend registry service provider's email address, and validate whether it is monitored and designated as the main email address for the candidate registry operator and/or backend registry service provider's business	NA	Verifiable e-mail address	The email address could be maintained on the Entity's website and could also be provided separately on request.
The HSTLD Sponsor should verify the candidate registry operator and/or backend registry service provider's phone number, and validate whether it is designated as the main phone number for the candidate registry operator and/or backend registry service provider's business	WebTrust EV 6.2	Verifiable telephone numbers	The telephone number could be maintained on the Entity's website and could also be provided separately on request.
The HSTLD Sponsor should verify whether the documentation of the business entity of the candidate registry operator and/or backend registry service provider specify: 1. The purpose of the organization 2. Organization's name 3. Place of business 4. Key officers	NA	documentation of the business entity	

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
				The HSTLD Sponsor should verify whether the candidate registry operator and/or backend registry service provider is a legally recognized entity whose existence was created by a filing with the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration	WebTrust EV 1.1		
				The HSTLD Sponsor should verify whether the candidate registry operator and/or backend registry service provider has designated with the Incorporating or Registration Agency either a Registered Agent, a Registered Office (as required under the laws of the jurisdiction of Incorporation or Registration), or an equivalent facility	WebTrust EV 1.1		
				The HSTLD Sponsor should verify whether the candidate registry operator and/or backend registry service provider is designated as an inactive, invalid, non-current organization or equivalent in records of the Incorporating Agency or Registration Agency	WebTrust EV 1.1		

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
				The HSTLD Sponsor should verify the certificate of formation for the candidate registry operator and/or backend registry service provider and validate whether it has been made available by the candidate registry operator and/or backend registry service provider. The HSTLD Sponsor should also verify whether the certificate of formation was filed in the office of the local in which the TLD operates, and sets forth: 1. The name of the Entity; 2. The address of the registered office 3. The address of the principal place of business 4. The name and address of each person executing the certificate of formation	NA	Certificate of formation	
				The HSTLD Sponsor should verify whether the organizational charter documents have been made available by the candidate registry operator and/or backend registry service provider and specify: 1. Statement of purpose 2. Organization's name 3. Affiliations 4. Principals (or Officers) 5. Criteria for the Principals (or Officers) for holding Office	NA	Charter documents	

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
The HSTLD Sponsor should verify whether the business license has been made available by the candidate registry operator and/or backend registry service provider, as applicable (Federal, State, Local). The license should be verifiable with the Registration Agency and should not be in a location (country) where the candidate registry operator and/or backend registry service provider is prohibited from doing business	NA	Business license	
The HSTLD Sponsor should verify whether the proof of a filed DBA has been made available by the candidate registry operator and/or backend registry service provider. The DBA certificate should be filed for in the county or local where the business is physically located	NA	Doing Business As (i.e., assumed name)	
The HSTLD Sponsor should verify whether the proof of Registration of trade name has been made available by the candidate registry operator and/or backend registry service provider. The trade name registration should provide a record of all owners of the Entity and should be filed with the appropriate governing body	NA	Registration of trade name	

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
				The HSTLD Sponsor should verify whether the following have been made available by the candidate registry operator and/or backend registry service provider: 1. Partnership agreements with other entities (relevant to registry operations) 2. Partnership agreements between the principals of the candidate registry operator and/or backend registry service provider The Partnership agreements should include the names of the relevant members/entities participating and cover the following, as applicable: a. Relevant dates b. Capital c. Profit and Loss sharing terms d. Salaries and Drawings e. Interest f. Management Duties and Restrictions g. Banking h. Termination i. Arbitration	NA	Partnership papers	

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
		2.1.2	The HSTLD sponsor should verify that the registry operator and/or backend registry service provider's insurance status or equivalent liability coverage is in accordance with defined local requirements.	The HSTLD Sponsor should verify whether the candidate registry operator and/or backend registry service provider maintains the minimum levels of Commercial General Liability Insurance and Professional Liability/Errors & Omissions insurance established by the local in which the TLD operates. The HSTLD Sponsor should also validate whether the proof of insurance coverage has been made available by the candidate registry operator and/or backend registry service provider	WebTrust EV 24	Insurance coverage	
				The HSTLD Sponsor should verify whether the providers of the Insurance coverage meet the ratings qualifications established in the local in which the TLD operates.	WebTrust EV 24		
				If the candidate registry operator and/or backend registry service provider self insures for liabilities, the HSTLD Sponsor should verify whether it maintains the minimum liquid asset size requirement established in the local in which the TLD operates.	WebTrust EV 24		
		2.1.3	The HSTLD sponsor should verify that the registry operator and/or backend registry service provider candidate's finanacial account status is in accordance with defined requirements.	The HSTLD Sponsor should verify whether a Financial Capability Review has been made available by the candidate registry operator and/or backend registry service provider. The Financial Capability Review should be performed by an independent, verified Accountant showing that the candidate registry operator and/or backend registry service provider's finances are sufficient to administer the objectives identified in the documentation of the business entity and Charter Documents	NA	Financial capabilities	

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
				The HSTLD Sponsor should verify whether the candidate registry operator and/or backend registry service provider has an active current Demand Deposit Account with a regulated financial institution OR whether the candidate registry operator and/or backend registry service provider has obtained a Verified Legal Opinion or a Verified Accountant Letter stating that it has an active current Demand Deposit Account with a Regulated Financial Institution	WebTrust EV 6.3		
		2.1.4	The HSTLD Sponsor should revalidate their registry operator and/or backend registry service provider candidates every two and a half years according to defined requirements.	The HSTLD Sponsor should require a revalidation of the candidate registry operator and/or backend registry service provider against of all the HSTLD Certification Program requirements every two and a half years	NA	Revalidation requirements	
		2.1.5	Procedures exist defining the screening and background verification process of employees and contractors in accordance with established requirements.	The HSTLD Sponsor should verify whether the following have been made available by the candidate registry operator and/or backend registry service provider: 1. The process employed to screen its employees before they are hired. 2. The training requirements for the employees after they are hired	NA	Screening processes for employees	

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
				The HSTLD Sponsor should verify whether the candidate registry operator and/or backend registry service provider has controls in place to: 1. verify the identity of each employee, agent, or independent contractors engaged in the TLD process 2. perform background checks of such person to confirm employment, check personal references, confirm the highest or most relevant educational degree obtained and search criminal records where allowed in the jurisdiction where the person will be employed	WebTrust EV 25.1		
				The HSTLD Sponsor should verify whether the personnel belonging to the candidate registry operator and/or backend registry service provider and performing the Registrar validation duties have received appropriate training that covers: 1. basic TLD knowledge, authentication and verification policies and procedures 2. common threats to the validation process including phishing and other social engineering tactics, and 3. the HSTLD Certification Program guidelines/principles/objectives	WebTrust EV 25.2		
				The HSTLD Sponsor should verify the records of employee training received by the relevant personnel belonging to the candidate registry operator and/or backend registry service provider	WebTrust EV 25.2		

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
				The HSTLD Sponsor should verify whether the personnel entrusted with validation duties meet minimum skills requirement that enables them to perform such duties satisfactorily for the candidate registry operator and/or backend registry service provider	WebTrust EV 25.2		
				The HSTLD Sponsor should verify whether the personnel entrusted with validation duties have attempted and passed an audit on the HSTLD Certification Program validation criteria/objectives outlined for the registrars and/or registration authority/Registrants	WebTrust EV 25.2		
2.2	The identity of the Registrar is designated and established prior to commencement of operations NOTE: 1. These are the proposed criteria topics and associated controls for performing Registrar Security Verification. The HSTLD Sponsor (or Community) may propose less or more stringent criteria and controls for a HSTLD registry operator and/or backend registry service provider to perform Registrar Security Verification 2. The HSTLD Sponsor (or Community) may also propose certain specific criteria and controls for Registrar Security Verification, depending on the HSTLD in question. E.g. HSTLD for financial institutions may have a	2.2.1	Information regarding the identity and location of the Registrar's Principle employees should be obtained and validated according to defined policy.	The Registrar shall provide a detailed background of its Principals, and make it available for review and validation	NA	Background of principals	The background of Principals could be maintained on the Registrar's website and could also be provided separately on request. The background should include: 1. Summary of experience 2. Employment/Professional history 3. Professional accreditations 4. Professional associations
				At least one Principal individual associated with the Registrar (owners, partners, managing members, directors or officers) should be identified and validated	WebTrust EV 1.1 and 5		The associated Principal individual (owners, partners, managing members, directors or officers) should not be located in a country where the Registrar is prohibited from doing business
				The Registrar shall maintain a physical address of the Place of Business, and make it available for review and validation	NA	Verifiable address	The physical address of the Place of Business could be maintained on the Registrar's website and could also be provided separately on request.

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria
	HSTLD for financial institutions may have a specific set of criteria and controls, whereas HSTLD for medical institutions may have a different set of criteria and controls		

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
The physical address provided must be verified as an address where the Registrar conducts business operations (e.g., not a mail drop or P.O. box), and is the address of the Registrar's Place of Business.	WebTrust EV 6.1		The Registrar's Place of Business should not be in a country where the Registrar/Registrant is prohibited from doing business Validation method TBD (refer to EV Certificate Guidelines Section 16)
The email address provided by the Registrar must be verified as the primary email address for the Registrar's business operations.	NA	Verifiable e-mail address	The email address could be maintained on the Registrar's website and could also be provided separately on request. Validation method TBD (refer to EV Certificate Guidelines Section 16(b))
The telephone number provided by the Registrar must be verified as a main phone number for the Registrar's Place of Business.	WebTrust EV 6.2	Verifiable telephone numbers	The telephone number could be maintained on the Registrar's website and could also be provided separately on request. Validation method TBD (refer to EV Certificate Guidelines Section 16(b))
The Registrar shall make their documentation of the business entity available for review and validation.	NA	documentation of the business entity	The following should be verified: 1. The purpose of the organization 2. Organization's name 3. Place of business 4. Key officers
The documentation of the business entity must be reviewed to validate that the Registrar is a legally recognized entity whose existence was created by a filing with the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration	WebTrust EV 1.1		

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
				The documentation of the business entity must be reviewed to validate that the Registrar has designated with the Incorporating or Registration Agency either a Registered Agent, a Registered Office (as required under the laws of the jurisdiction of Incorporation or Registration), or an equivalent facility	WebTrust EV 1.1		
				The organization should not be designated as inactive, invalid, non-current or equivalent in records of the Incorporating Agency or Registration Agency	WebTrust EV 1.1		
				The Registrar shall make the Certificate of Formation available for review and validation. The Certificate of Formation must be reviewed to validate that it was filed in the local in which the TLD operates, and sets forth: 1. The name of the Entity; 2. The address of the registered office 3. The address of the principal place of business 4. The name and address of each person executing the Certificate of Formation	NA	Certificate of Formation	
				The Registrar shall make their Charter documents available for review and validation. The Charter documents must be reviewed to validate the following: 1. Statement of purpose 2. Organization's name 3. Affiliations 4. Principals (or Officers) 5. Criteria for the Principals (or Officers) for holding Office	NA	Charter documents	

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
				The Registrar shall make the business license available for validation purposes., as applicable (Federal, State, Local). The license should be verifiable with the Registration Agency and should not be in a location (country) where the Entity is prohibited from doing business.	NA	Business License	
				If the Registrar has been in existence for less than three (3) years, as indicated by the records of the Incorporating Agency or Registration Agency, and is not listed in either the current version of one (1) Qualified Independent Information Source or a Qualified Governmental Tax Information Source, then additional evidence demonstrating the Registrar is actively engaged in business must be obtained by: - verifying that the Applicant has an active current Demand Deposit Account with a regulated financial institution, or - obtaining a Verified Legal Opinion or a Verified Accountant Letter that the Applicant has an active current Demand Deposit Account with a Regulated Financial Institution.	WebTrust EV 6.3		(See EV Certificate Guidelines Section 17 (a), (b))
				The Registrar shall make the proof of a filed DBA available for validation purposes. The DBA certificate should be filed for in the county or local where the business is physically located.	NA	Doing Business As (i.e., assumed name)	

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
				The Registrar shall make the proof of Registration of trade name available for validation purposes. The trade name registration should provide a record of all owners of the Entity and should be filed with the Secretary of State or equivalent entity	NA	Registration of trade name	
				The Registrar shall make the following available for validation purposes: 1. Any Partnership agreements with other entities (relevant to registrar operations) 2. Any Partnership agreements between the principals of the Entity If applicable, the Partnership agreements should include the names of the relevant members/entities participating and cover the following, as applicable: a. Relevant dates b. Capital c. Profit and Loss sharing terms d. Salaries and Drawings e. Interest f. Management Duties and Restrictions g. Banking h. Termination i. Arbitration	NA	Partnership papers	
		2.2.2	Information regarding accredidation status and renewal must be publicly provided.	The Registrar shall provide its current accreditation status, as of the time of the self-certification.	NA	Accreditation status as of the time of self-certification	

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
				The Registrar shall provide its date of accreditation expiry, as of the time of the self-certification.	NA	Notification of Accreditation expiry	
				The Registrar shall provide its planned date of accreditation renewal, as of the time of the self-certification.	NA	Notification of planned renewal	
		2.2.3	registrars and/or registration authority are revalidated periodically according to defined procedures.	The Registrar shall be subject to the entire vetting process for revalidation every two and a half years.	NA	Revalidation requirements	
2.3	TLD data is consistent and correct at the TLD Registry level.	2.3.1	Procedures exist to prevent abusive domain name registration practices by the entity's users and take appropriate actions when violations are discovered. Procedures must meet or exceed established abuse criteria standards.	The candidate registry operator and/or backend registry service provider should implement and adhere to any rights protection mechanisms (RPMs) that may be mandated from time to time by the HSTLD Sponsor (or Community)	Draft Applicant Guidebook, v3	Rights Protection Mechanisms	
				The candidate registry operator and/or backend registry service provider should develop and implement additional RPMs that discourage or prevent registration of domain names that violate or abuse another party's legal rights	Draft Applicant Guidebook, v3		

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
The candidate registry operator and/or backend registry service provider should include all the HSTLD Sponsor mandated and independently developed RPMs in the Registry-Registrar agreement entered into by the accredited registrars and/or registration authority authorized to register names in the HSTLD	Draft Applicant Guidebook, v3		
The candidate registry operator and/or backend registry service provider should perform a periodic check/audit on the accuracy and completeness of the Domain name registration data being provided by each of the accredited registrars and/or registration authority	NA	Accuracy of Domain name registration data from the registrars and/or registration authority	
The candidate registry operator and/or backend registry service provider should report on any inaccuracies discovered in the data being provided by any of the accredited registrars and/or registration authority and require the respective Registrar to take appropriate action within a proposed timeline	NA		
The candidate registry operator and/or backend registry service provider should periodically conduct audits to compare the Domain name registration data being provided by each of the accredited registrars and/or registration authority with the data recorded internally and report on, any inconsistencies noted	NA	Accuracy of Domain name registration data recorded internally by the Registry	
The candidate registry operator and/or backend registry service provider should identify the root cause behind the inconsistencies noted and introduce the appropriate solution to resolve them	NA		

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
				The candidate registry operator and/or backend registry service provider should provide the HSTLD Sponsor with the report on any inconsistencies noted, based on the periodic audits			
		2.3.2	The entity's public Whois data must be maintained, accurate, and complete in accordance with defined requirements. NOTE: Performance, Availability, Accuracy and Completeness of the Whois service and data are covered in Objective #1.2	The candidate registry operator and/or backend registry service provider should operate a registration data publication service available via both port 43 and a website, providing free public query-based access. The Query and Response formats for Domain Name Data, Registrar Data and Nameserver Data should be in accordance with RFC 3912	Draft Applicant Guidebook, v3	Whois service and query format	NOTE: Performance, Availability, Accuracy and Completeness of the Whois service and data are covered in Objective #1.2
				The candidate registry operator and/or backend registry service provider should enter into an agreement with any Internet user that will allow such user to access an Internet host server or servers designated by the candidate registry operator and/or backend registry service provider and download zone file data	Draft Applicant Guidebook, v3	Whois Zone File Access	
				The candidate registry operator and/or backend registry service provider should request each user to provide it with information sufficient to identify the user and its designated server. Such user information should include, without limitation, company name, contact name, address, telephone number, facsimile number email address and the Internet host machine name and IP address	Draft Applicant Guidebook, v3		

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
				The candidate registry operator and/or backend registry service provider should grant the User a nonexclusive, nontransferable, limited right to access registry operator and/or backend registry service provider's Server, and to transfer a copy of the top-level domain zone files, and any associated cryptographic checksum files to its Server	Draft Applicant Guidebook, v3		
				The candidate registry operator and/or backend registry service provider should permit user to use the zone file for lawful purposes; provided that, (a) user takes all reasonable steps to protect against unauthorized access to and use and disclosure of the data, and (b) under no circumstances will user use the data to: 1. allow, enable, or otherwise support the transmission by e-mail, telephone, or facsimile of mass unsolicited, commercial advertising or solicitations to entities other than user's own existing customers, or 2. enable high volume, automated, electronic processes that send queries or data to the systems of registry operator and/or backend registry service provider or any accredited Registrar	Draft Applicant Guidebook, v3	Integrity of public Whois data	
				The candidate registry operator and/or backend registry service provider should provide each user with access to the zone file for a pre-determined period of time	Draft Applicant Guidebook, v3		

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
				The candidate registry operator and/or backend registry service provider should periodically perform the vetting of access to zone file data by approved users/parties. Appropriate actions should be taken promptly to restrict or deny access, based on any findings	Draft Applicant Guidebook, v3		
				The candidate registry operator and/or backend registry service provider should continuously monitor and log the access to zone file data, and alert respective personnel/teams if unauthorized access is noted on reviewing the monitoring logs	Draft Applicant Guidebook, v3		
		2.3.3	The entity should monitor the information system infrastructure and resolves incidents in accordance with defined policy.	The candidate registry operator and/or backend registry service provider should deploy and document the processes and the solutions to monitor logical security, data integrity, system performance and availability across the Registry Operations infrastructure. Arrangements should be made for monitoring critical registry systems including, but not limited to: SRS, database systems, DNS servers, Whois service, network connectivity, routers and firewalls	Draft Applicant Guidebook, v3	Monitoring Logical security, Data integrity, System performance and Availability	NOTE: Strongly considering moving the Monitoring controls to Objective #1.1
				The candidate registry operator and/or backend registry service provider should deploy and document the Incident Management/Escalations processes and solutions across the Registry Operations infrastructure, in order to handle high-severity incidents effectively	Draft Applicant Guidebook, v3	Incident Management/Escalations	

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
				The candidate registry operator and/or backend registry service provider should deploy and document the processes and solutions for detecting threats and security vulnerabilities across the Registry Operations infrastructure, and taking appropriate steps to resolve them	Draft Applicant Guidebook, v3	Detecting threats and security vulnerabilities	
		2.3.4	Procedures exist to define the usage requirements of an Escrow Agent between the Registrar and the registry operator and/or backend registry service provider candidate.	Prior to entering into an escrow agreement, the Registrar should contact and inform the candidate registry operator and/or backend registry service provider as to the identity of the Escrow Agent, and provide with contact information and a copy of the relevant escrow agreement	Draft Applicant Guidebook, v3	Registrar data QA/quality review (and escrow data audit results)	
				Escrow Agent should be required to hold and maintain the Deposits in a secure, locked, and environmentally safe facility which is accessible only to authorized representatives of Escrow Agent	Draft Applicant Guidebook, v3		
				Escrow Agent should be required to protect the integrity and confidentiality of the Deposits using commercially reasonable measures	Draft Applicant Guidebook, v3		
				Escrow Agent should verify the format and completeness of each Deposit. The Registrar should regularly deliver to the candidate registry operator and/or backend registry service provider a verification report generated for the Deposits over a pre-determined period of time	Draft Applicant Guidebook, v3		

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
				The candidate registry operator and/or backend registry service provider should be provided the right to inspect Escrow Agent's applicable records upon reasonable prior notice	Draft Applicant Guidebook, v3		
				If the Escrow Agent receives a subpoena or any other order from a court or other judicial tribunal pertaining to the disclosure or release of the Deposits, the Registrar should promptly notify the candidate registry operator and/or backend registry service provider, unless prohibited by law	Draft Applicant Guidebook, v3		
				If the Registrar is notified by the Escrow Agent about any Deposit failing the verification procedures, the Registrar should notify the candidate registry operator and/or backend registry service provider of such nonconformity within a pre-determined duration from the time of discovery	Draft Applicant Guidebook, v3		
		2.3.5	Procedures exist to resolve disputes of the entity's registration of a domain name by other parties in an efficient and timely manner.	The candidate registry operator and/or backend registry service provider should adopt and implement dispute resolution mechanisms under which third parties may challenge registration of domain names by other parties	Draft Applicant Guidebook, v3	Dispute resolution process	
				The candidate registry operator and/or backend registry service provider should maintain and publish on its website a single point of contact responsible for addressing matters requiring expedited attention for dispute resolution	Draft Applicant Guidebook, v3		

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
				The candidate registry operator and/or backend registry service provider should maintain and publish on its website the procedure involved in a dispute resolution process	NA		
				The candidate registry operator and/or backend registry service provider must provide a timely response to abuse complaints concerning all names registered in the TLD through all registrars and/or registration authority of record, including those involving a reseller	Draft Applicant Guidebook, v3		
2.4	Establish effective controls to reduce malicious conduct by registrars and/or registration authority and Registrants	2.4.1	The entity secures administrative access to domain functionality through verified point of contact information, multi-factor authentication , and other security measures.	Verification of the point of contact information submitted by the registrant should be performed at registration and each time contact information is modified	Principle #3	Registration verification	This will be covered in Principle #3
				registrars and/or registration authority should enforce minimum length, maximum lifetime or complexity checks on passwords and protect against brute-force guessing attacks by limiting the number of incorrect login attempts.	APWG	Improve password-based authentication system	The predominant authentication method among registrars and/or registration authority is a simple username and password. Commonly accepted best security practices recommend that these measures should be present in any password based authentication system
				registrars and/or registration authority should require E-merchants and financial institutions to complement improved password systems by allowing a customer to register the personal computer (PC) or IP address from which he/she will administer an account	APWG	System Registration	

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to use a multi-factor authentication system for processing update, transfer and/or deletion requests. The registrars and/or registration authority in turn should require the Registrants to use a multi-factor authentication system for processing their requests	APWG	Multi-factor authentication	
The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to implement a challenge-response system for the Registrants as part of the cost/inconvenience of protecting domain names and preventing DNS configuration abuse. This could also be considered as an opt-in service for those Registrants who would accept the additional challenges as part of the benefit/inconvenience ratio	APWG	Challenge systems	
The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to offer a per domain access model to Registrants who seek greater protection. This could also be considered to be mandatory for all Registrants E.g. an opt-in feature would grant customers the ability to control which points of contact are able to make changes to contact and DNS confirmation information, initiate or authorize a domain transfer, etc.	APWG	Per domain access controls	

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
				The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to check for and request unique points of contact information from the Registrants. The Registrant as well as the Registrar can use unique points of contact to create a granular privilege model. This could also be considered to be an opt-in service for all Registrants interested in increased protection E.g. some organizations may want to ensure that only the registrant point of contact can transfer a domain, or that only the technical point of contact can change DNS configuration (other models exist, and these are presented here for illustrative purposes only).	APWG	Multiple, unique points of contact	
				The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to allow the Registrants to select which points of contact must be notified upon a request to change DNS configuration, or require that both the technical and administrative contact respond by phone or email before making a change requested by one party. This could also be considered to be an opt-in service for all Registrants interested in increased protection E.g. some organizations may want to ensure that only the registrant point of contact can transfer a domain, or that only the technical point of contact can change DNS configuration (other models exist, and these are presented here for illustrative purposes only).	APWG	Multiple change notifications or confirmations	Multiple confirmations improve an organization's defenses against impersonation: an attacker must socially engineer or impersonate not just one party, but two E.g. A situation where an employee designated as a point of contact has left the organization and the organization failed to change the contact information from this employee to his replacement. If the employee left disgruntled, he might attempt to claim the domain through a domain transfer. In the change confirmation scenario, other contacts are required to confirm the transfer and the transfer attempt could be blocked.

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
				The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to offer the Registrants the option to deliver critical notifications via telephone, fax, postal or courier services (in addition to email) for additional protection. This could also be considered to be mandatory for all Registrants	APWG	Multiple delivery methods for critical correspondence	

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
				The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to educate and encourage Registrants to: 1. Include point of contact information administration in the Employee Resource Management process to assure that when a terminated employee's credentials are rescinded, all domain registration point of contact information associated with that employee is changed as well 2. Impose a password change policy 3. Periodically verify contacts 4. Proactively monitor domain name registration 5. Assign email addresses for all registration points of contact from a different domain than the registered domain name. (Some registrants may want to create multiple domain registration accounts as an additional safeguard.) 6. Treat transfer attempts as a security event (check and re-check) 7. Use a separate domain for registration contact email accounts from domains used for other business purposes. For example, assign email addresses for example.info's points of contact from example.net 8.Create role accounts: e.g., domainadmincontact@example.com, domainregistrantcontact@example.biz, domaintechnicalcontact@example.net 9. Alias multiple recipients for a role account for notifications	APWG	Engaging the Registrant	

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to make efforts to communicate the kinds of security measures they provide to the Registrants	APWG	Informing the Registrant	
The candidate registry operator and/or backend registry service provider and its registrars and/or registration authority should collect emergency point of contact information from registrars and/or registration authority and Registrants respectively. This contact information should be for parties who are suited to assist in responding to an urgent restoration of domain name incident	APWG	Emergency point of contact	
The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to ensure that their resellers understand record keeping requirements of registrars and/or registration authority (and the HSTLD Sponsor), and improve compliance with these requirements	APWG	Reseller compliance	
The candidate registry operator and/or backend registry service provider should monitor DNS changes for anomalies or abuse	APWG	Monitoring DNS changes	Refer to Objective #1.1

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
				The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to share information with industry partners. E.g. 1. IPs associated with fraudulent domain registrations with respectable blacklists. 2. Full fraud reports with industry and law enforcement, such as those at the Internet Crime Complaint Center 3. Leading practices regarding accepting and managing domain registrations	APWG	Information sharing	
		2.4.2	The entity should periodically acquire determinations regarding information systems security from an independent third party.	The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to voluntarily have an independent security, anti-phishing and anti-malware audit performed on their operations as a component of their security due diligence	APWG	Independent Security, Anti-phishing and Anti-malware Audit	
				HSTLD Sponsor, candidate HSTLD registry operator and/or backend registry service provider and the registrars and/or registration authority should study whether registration services have generally improved and whether Registrants are benefitting from having an approved independent third party perform a security audit based on a prescribed set of security measures, at the request of the registrars and/or registration authority	APWG	Evaluate benefits of performing independent security audit	
		2.4.3	The entity should provide metrics of malicious activity and their resolutions within the SLA.	The candidate registry operator and/or backend registry service provider should include in the SLA with the registrars and/or registration authority on consequences of malicious domain registrations, based on a unit of measure.	NA	SLA based on percent of malicious domains per ”unit measure” of registrations (e.g., 1000, 5000, 10,000 domains)	E.g. Registrar to pay monetary fine for every 'X' number of malicious domain registrations etc.

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
		2.4.4	Procedures exist to resolve identified orphan name servers.	The candidate registry operator and/or backend registry service provider should enforce and document a policy to proactively identify and correct orphan name servers	NA	Proactive identification	
				Refer to Rapid Domain Suspension controls in this Objective below	APWG	Glue records for deleted domain	
		2.4.5	The entity has established an abuse response department and published relevant contact information.	The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to have a dedicated abuse department that has published contact information, including both phone and email, on both the registrar's website and WHOIS records	APWG	Abuse points of contact with a documented response process that is timely and auditable	Also, refer to Objective #2.3
		2.4.6	Policies defining activities constituting 'Malicious use' are defined and communicated between the entity and their clients.	The candidate registry operator and/or backend registry service provider should define as to what activities constitute 'Malicious use' in the Code of Conduct, in order for all the registrars and/or registration authority to have a common interpretation and understanding	NA	Definition of malicious use (conduct)	
				The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to explicitly mention about the prohibition of malicious conduct in Registrar-Registrant terms of service agreement and obtain an acknowledgement of the same from the Registrants. Refer to controls listed in Objective #4.2 for Code of Conduct	NA	Explicit prohibition of malicious conduct in registrant terms of service agreement	

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
		2.4.7	Procedures exist to prevent, identify, and expedite removal of domains and their records involved in phishing actvities.	The candidate registry operator and/or backend registry service provider should ensure that glue records for an invalid or deleted domain are removed, even if those glue records are in use in conjunction with other domains or cooperation between the TLDs should be implemented	APWG	Glue records for an invalid/deleted domain	
				The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to remove domain records of invalid or malicious domains within a pre-determined period of time (E.g. 3 hours)	APWG	Response time	
				The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to establish expedited channels and contact information for law enforcement and community partners	APWG	Law enforcement and Community partners	
				The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to work within the Registrar and Law enforcement community to establish a data exchange format for all fraudulent DNS registrations and associated information.	APWG		
				The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to collect IP Whois information from the Registrants in order to contact the Internet Service Provider hosting the phish site	APWG	Evidence Preservation for Investigative Purposes	Whois information on IP addresses is much more complete and accurate than Whois information for domains. Maintaining this resource would have a huge positive impact on the anti-phishing efforts

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
				The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to use criminal pattern tracking in the Whois database to quickly shut down and even pre-empt launches of phishing attacks	APWG	Proactive Fraud Screening	E.g. The domains used could be registered in batches over several days in different months, utilizing a dozen or more registrars and/or registration authority, but all with a very small set of unique registrant names and administrative Whois contact credential sets that include a rotated set of names, addresses and phone numbers, as well as specific email addresses created to be used specifically for the phishing attacks
				The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to not accept obfuscated Whois information, as it may directly interfere with phishing site shut down and increase the number of potential victims of a phishing crime	APWG		E.g. The recent widespread adoption and marketing of domain “privacy" services, which has created a method for scammers to hide illicit registrations.
		2.4.8	Controls exist to prevent phishing and spoofing activities within the entity's domain.	Refer to Anti-phishing and anti-spoofing controls for new TLDs and the Proactive Fraud Screening controls above in Objective #2.4	NA	Thick Whois process and support	
		2.4.9	Controls exist for the entity to deploy DNSSEC and IPv6 within their infrastrucutre.	Refer to Objective #1.1	NA	DNSSEC & IPv6 deployment plan	
		2.4.10	Real-time domain monitoring solutions have been implemented which alert relevant personnel in the event	The candidate registry operator and/or backend registry service provider should enable the configuration to allow specific events to be written to the DNS Events Log	NA	Event logging configuration	

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
			personnel in the event of security incidents.	The candidate registry operator and/or backend registry service provider should monitor for specific DNS events and alert relevant personnel. Some examples could be: 1. Monitoring account activity for anomalous activity such as unusual volumes of logins, password modification, transfers, withdrawals, etc. 2. Monitoring recent domain registrations and taking action against parties registering domain names deceptively similar to existing legitimate domain names Refer to controls listed in Objective #2.3 under 'Integrity of public Whois data'	NA	Event monitoring configuration	Some companies offer a registration monitoring service that will detect registration of a potential spoof domain and monitor any site activity while pursuing action against the registrant
		2.4.11	Malicious activity is tracked by the Registrant and documented in a monthly report that is communicated to the entity.	The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to provide a monthly report on malicious activity with respect to the domains registered through them. The monthly report should consist of the number of occurrences of malicious activity for every 'X' number of domains registered during the candidate month. The malicious activities should also be classified by their nature for trending purposes.	NA	Monthly reports of malicious activity reported to registry (such as phishing and botnets)	

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria
Principle#3: The Registry shall maintain effective controls to provide reasonable assurance that the processing of core Registrar functions by Registration Authorities are authorized, accurate, complete, and performed in a timely manner in accordance with established policies and standards. The identity of participating entities is established and authenticated.			
3.1	Registrant identity is verified and established prior to provisioning of domain name by the Registration Authority.	3.1.1	Information regarding the identity and location of the Registrant's Principle employees or subscribing individuals should be obtained and validated according to defined policy.

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
Refer to the control for 'SLA based on percent of malicious domains', mentioned above in Objective #2.4	NA	Commitment to address if malicious activity is high (relative to other registrars and/or registration authority who do business with this registry)	
Principle #3 Illustrative Control Examples			
The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to verify whether the background of the principals for the Registrant are made available on the website or on request	NA	Background of principals	The background of principals could be maintained on the Entity's website and could also be provided separately on request. The background should include: 1. Summary of experience 2. Employment/Professional history 3. Professional accreditations 4. Professional associations
The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to identify and verify the background of at least one Principal Individual associated with the Registrant (owners, partners, managing members, directors or officers)	WebTrust EV 1.1		
The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to verify whether the identified Principal Individual for the Registrant (owners, partners, managing members, directors or officers) is not located in a country where it is prohibited from doing business	WebTrust EV 1.1		

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to verify the physical address of the Place of Business for the Registrant	WebTrust EV 1.1	Verifiable address	The physical address of the Place of Business could be maintained on the Entity's website and could also be provided separately on request.
The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to obtain reasonable assurance about the physical existence and business presence of the Registrant	WebTrust EV 1.1		
The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to verify that the Registrant's Place of Business is not in a country where it is prohibited from doing business	WebTrust EV 1.1		
The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to verify the Registrant's email address, and validate whether it is monitored and designated as the main email address for the Registrant's business	NA	Verifiable e-mail address	The email address could be maintained on the Entity's website and could also be provided separately on request.
The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to verify the Registrant's phone number, and validate whether it is designated as the main phone number for the candidate Registrant's business	WebTrust EV 6.2	Verifiable telephone numbers	The telephone number could be maintained on the Entity's website and could also be provided separately on request.

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
				The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to verify whether the documentation of the business entity of the Registrant specify: 1. The purpose of the organization 2. Organization's name 3. Place of business 4. Key officers	NA	documentation of the business entity	
				The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to verify whether the Registrant is a legally recognized entity whose existence was created by a filing with the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration	WebTrust EV 1.1		
				The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to verify whether the Registrant has designated with the Incorporating or Registration Agency either a Registered Agent, a Registered Office (as required under the laws of the jurisdiction of Incorporation or Registration), or an equivalent facility	WebTrust EV 1.1		
				The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to verify whether the Registrant is designated as an inactive, invalid, non-current organization or equivalent in records of the Incorporating Agency or Registration Agency	WebTrust EV 1.1		

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
				The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to verify the certificate of formation for the Registrant and validate whether it has been made available by the Registrant. The candidate registry operator and/or backend registry service provider should also require the registrars and/or registration authority to verify whether the certificate of formation was filed in the office of the local in which the TLD operates, and sets forth: 1. The name of the Entity; 2. The address of the registered office 3. The address of the principal place of business 4. The name and address of each person executing the certificate of formation	NA	Certificate of formation	
				The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to verify whether the organizational charter documents have been made available by the Registrant and specify: 1. Statement of purpose 2. Organization's name 3. Affiliations 4. Principals (or Officers) 5. Criteria for the Principals (or Officers) for holding Office	NA	Charter documents	

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
				The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to verify whether the business license has been made available by the Registrant, as applicable (Federal, State, Local). The license should be verifiable with the Registration Agency and should not be in a location (country) where the Registrant is prohibited from doing business	NA	Business license	
				The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to verify whether the proof of a filed DBA has been made available by the Registrant. The DBA certificate should be filed for in the county or local where the business is physically located	NA	Doing Business As (i.e., assumed name)	
				The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to verify whether the proof of Registration of trade name has been made available by the Registrant. The trade name registration should provide a record of all owners of the Entity and should be filed with the approriate legal authority	NA	Registration of trade name	

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
				The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to verify whether the following have been made available by the Registrant: 1. Any Partnership agreements with other entities 2. Any Partnership agreements between the principals of the Registrant If applicable, the Partnership agreements should include the names of the relevant members/entities participating and cover the following, as applicable: a. Relevant dates b. Capital c. Profit and Loss sharing terms d. Salaries and Drawings e. Interest f. Management Duties and Restrictions g. Banking h. Termination i. Arbitration	NA	Partnership papers	NOTE: This may not be a necessary control for the Registrant vetting procedure
		3.1.2	Registrants are revalidated periodically according to defined procedures, notwithstanding a registrant will be re-validated should a transfer of the TLD occur.	The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to perform a revalidation of the Registrant against of all the HSTLD Certification Program requirements every two and a half years	NA	Revalidation requirements	

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
		3.1.3	Prior to registering a domain name, the Registrar and the Registrant should validate approval.	The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to validate that the transaction has been approved by both the technical and administrative (and possibly more) contacts at the Registrant organization before completing the process of domain name registration	NA	Authority of Registrant to register in the TLD	
		3.1.4	Procedures exist to validate exemptions of Registrants to allow proxy/anonymous registration.	The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to not accept proxies/anonymous registrations from the Registrants, unless a valid justification has been provided to and approved by the candidate registry operator and/or backend registry service provider and the HSTLD Sponsor	NA	Restrict Proxies/Anonymous Registrations	
				The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to seek sufficient proof from the commercial Registrants for justifying proxy/anonymous registration	NA	Commercial users exempt from Proxies/Anonymous Registrations must provide proof that the applicant is a natural person, organization must show cause or justification for anonymity	Refer to control for 'Absence of Proxies' under Objective #4.1

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
3.2	Data is consistent and correct at the Registrar level.	3.2.1	Procedures exist to authenticate an entity's new Registrant.	The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to honor the HSTLD Sponsor mandated and independently developed RPMs in the Registry-Registrar agreement	Draft Applicant Guidebook, v3	Rights Protection Mechanisms	NOTE: The following contributing controls/objectives/criteria have already been incorporated: 1. **Objective #3.1** lists all proposed controls for vetting the Registrant organization 2. **Objective #2.4** lists all proposed controls for contact verification, System Registration and multiple, unique points of contact 3. **Objective #2.3** lists the proposed control for including all the HSTLD Sponsor mandated and independently developed RPMs in the Registry-Registrar agreement
		3.2.2	Procedures exist to verify registration information from new Registrants are complete and accurate.	The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to ensure the accuracy and completeness of data provided by the respective Registrant, based on the controls listed in Objectives #2.4 and #3.1, before approving the Domain Name Registration application from the respective Registrant	NA	Registrar confirmation that registration data are accurate and complete	
		3.2.3	The entity should periodically verify the completeness and accuracy of a Registrant's registration information.	The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to proactively and continuously monitor the accuracy and completeness of registration data provided by the respective Registrants, based on the controls listed in Objectives #2.4 and #3.1, even after the Domain Name Registration application has been approved by the Registrar	NA	Registrar monitoring registration data for accuracy and completeness	

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
		3.2.4	Registrant transaction data is authenticated against registered DNS information.	The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to authenticate any transactions being made by the Registrants in order to: 1. Validate that the transaction is being made by an individual authorized by the respective Registrant for that particular domain name 2. Validate that the transaction is being made from a system that had been registered by Registrant 3. Validate that the transaction has been approved by both the technical and administrative contacts at the Registrant organization E.g. Registrant trying to make a change in the DNS configuration	NA	Registrar authentication of registration data for each transaction	NOTE: Refer to Objective #2.4 for details
		3.2.5	The Registrant should notify the entity of any changes to the Registrant's registration data.	The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to notify the respective Registrant of any transactions being made to the Registrant's registration data. Notifications should be sent to multiple points of contact at the Registrant organization about the completed transaction via multiple delivery methods	NA	Registrar confirmation of change in registration data	NOTE: Refer to Objective #2.4 for details

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
		3.2.6	Procedures exist to revoke service to Registrants in the event that registration information is inaccurate.	The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to reject/suspend the domain registration application from the respective Registrants, if: 1. The registration data is inaccurate/false, based on controls listed in Objective #3.1 2. The points of contacts provided by the candidate Registrant cannot be verified 3. The candidate Registrant organization is listed in respectable blacklists 4. The candidate Registrant organization has failed an independent security, anti-phishing and anti-malware audit 5. The candidate Registrant has not provided all the requested information by the Registrar for the domain name registration process	NA	Rejection/suspension of registration data with cause (incomplete, false/inaccurate)	NOTE: Refer to Objectives #2.4 and#3.1 for details
		3.2.7	Controls exist to prevent phishing and spoofing activities.	Refer to Anti-phishing and anti-spoofing controls for new TLDs and the Proactive Fraud Screening controls above in Objective #2.4	NA	Thick Whois	
		3.2.8	Procedures exist to proactively identify and remove non-active registration data.	The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to proactively identify and remove registration data for Registrants or Domains that are inactive or invalid	NA	Registrar removal of registration data	

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
		3.2.9	Procedures exist to monitor the Registrar's critical operational systems for performance levels, security vulnerabilities, and availability. Incidents and event resolutions are documented.	The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to deploy and document the processes and the solutions to monitor logical security, data integrity, system performance and availability across the Registrar's Operations infrastructure. Arrangements should be made for monitoring critical Registrar systems including, but not limited to: Database systems, Domain name registration systems, Whois systems, network connectivity, routers and firewalls	Draft Applicant Guidebook, v3	Monitoring Logical security, Data integrity, System performance and Availability	
				The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to deploy and document the Incident Management/Escalations processes and solutions across the Registrar Operations infrastructure, in order to handle high-severity incidents effectively	Draft Applicant Guidebook, v3	Incident Management/Escalations	
				The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to deploy and document the processes and solutions for detecting threats and security vulnerabilities across the Registrar Operations infrastructure, and taking appropriate steps to resolve them	Draft Applicant Guidebook, v3	Detecting threats and security vulnerabilities	

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
		3.2.10	Periodic verification of registration data is performed by the Registrar and communicated to the registry operator and/or backend registry service provider.	The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to perform a periodic check/ internal audit on the accuracy and completeness of the Domain name registration data being provided by Registrants	NA	Accuracy of Domain name registration data from the Registrants	
				The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to report on any inaccuracies and inadequacies discovered in the data being provided by any of the Registrants, and require the respective Registrar to take appropriate action within a proposed timeline	NA		
				The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to periodically conduct audits to compare the Domain name registration data being provided by the Registrants with the data recorded internally	NA	Accuracy of Domain name registration data recorded internally by the registrars and/or registration authority	
				The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to identify the root cause behind the inconsistencies noted and introduce the appropriate solution/measures to resolve them	NA		
				The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to provide a report on any inconsistencies noted, based on the periodic audits	NA		

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
		3.2.11	Procedures exist to expidite the suspension and removal of inaccurate Domain registration information.	Refer to Rapid Domain Suspension process controls listed in Objective #2.4	NA	Domain suspension	
Principle#4: Registrants in a High Security Zone are expected to maintain current and accurate information, and to commit to refrain from activities designed to confuse or mislead the Internet-using public.				**Principle #4 Illustrative Control Examples**			
4.1	Registrants provide current and accurate identity and locative information	4.1.1	Candidate Registry (and/or Registry Service Provider) affirms that Registrants will be notified of existing rules and policy with respect to their obligations to provide accurate and current registrant information at the time of the registration, transfer, or renewal of a domain name. Registrars within HSTLD will agree to make these notices to registrants or allow registry to provide said notice to registrants directly	The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to educate the Registrants about the importance of accurately providing the Whois data and the consequences of inaccurate/false information leading to suspension of the domain registration process The Registrants should also be required to proactively communicate changes to the Whois data	NA	WHOIS data	This should be included in the Code of Conduct communicated to the Registrants by the registrars and/or registration authority

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria	Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
				The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to communicate to the Registrants about the need for providing their accurate location information to the candidate registry operator and/or backend registry service provider, as a part of the domain name registration application	NA	Registrant locative information provided to registry	NOTE: The registrars and/or registration authority are already required to verify the Registrant's location/place of business, as a part of the controls listed under Objective #3.1. So, the registrars and/or registration authority can themselves provide such information to the candidate registry operator and/or backend registry service provider after vetting it
				The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to communicate to the Registrants about the need for providing their accurate contact information to the candidate registry operator and/or backend registry service provider, as a part of the domain name registration application	NA	Contact information provided to registry	NOTE: The registrars and/or registration authority are already required to verify the Registrant's contact information, as a part of the controls listed under Objective #3.1. So, the registrars and/or registration authority can themselves provide such information to the candidate registry operator and/or backend registry service provider after vetting it
		4.1.2	Procedures exist to disallow proxies/anonymous registration from Registrants.	The candidate registry operator and/or backend registry service provider should not accept proxies/anonymous registrations from the Registrants	NA	Absence of proxies	
4.2	Registrants will explicitly commit to abiding by ICANN's policies, as well as any additional obligations created through the application of HSTLD standards	4.2.1	Continous acknowledgement of defined HSTLD Code of Conduct obligations and the consequences for any violations are to be obtained from the Registrant by the Domain Registrar	The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to obtain an explicit commitment from the Registrants stating that the Registrants will abide by the HSTLD Sponsor's policies and any obligations considered as necessary by the HSTLD community (Code of Conduct)	NA	Explicit commitment	

This document is a working draft and has not been tested for consensus. The HSTLD AG continues to discuss all elements of this document, including all Principles, Objectives, Criteria, Illustrative Control Examples and Comments. The document contents will be modified as the HSTLD AG continues to make progress on this working draft.

HSTLD Standards

HSTLD Objective No	HSTLD Criteria Objective	HSTLD Criteria No	HSTLD Criteria
			Domain Registrar:

HSTLD Illustrative Control Examples

NOTE: Oranizations may elect to adopt their own equivalent controls

Illustrative Control Examples NOTE: Organizations may elect to build equivalent controls of their own	Illustrative Control Example Source Reference	Illustrative Control Example Control Element	Illustrative Control Example Comments
The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to obtain an acknowledgement from the Registrants on the consequences of violating the Code of Conduct (mentioned above)	NA	Consequences of violation	
The candidate registry operator and/or backend registry service provider should require the registrars and/or registration authority to communicate the Code of Conduct periodically (or when updated) to the Registrants as a means of continuously educating them about their commitments and any changes introduced to the Code of Conduct	NA	Ongoing communication	

Standards Breakdown		
Principles		4
Objectives		11
Criteria		57

Illustrative Control Activities Breakdown		
Industry Specific Controls		100
Draft Applicant Guidebook Controls		28
Webtrust EV Controls		34
APWG Controls		26
ISO 27002 Controls		119
Total Controls		307