

**American Bankers Association
BITS
Financial Services – Information Sharing and Analysis Center
Financial Services Technology Consortium**

6 August 2009

Mr. Rod Beckstrom, President and CEO, Rod.beckstrom@icann.org
Internet Corporation for Assigned Names and Number

Dear Mr. Beckstrom,

We want to thank The Internet Corporation for Assigned Names and Numbers (ICANN) for its willingness to engage the banking and finance sector in the public consultations regarding the Draft Applicant Guidebook. We particularly want to thank Greg Rattray, ICANN Chief Internet Security Advisor, with whom we met on several occasions as we developed our recommendations, and who was most cooperative and supportive of our efforts.

As we communicated to ICANN in our prior comment letters and discussions, the financial services industry has a variety of concerns about the proposed expansion of Generic Top Level Domains (gTLDs), including cost/benefit, trademark protection, scalability and security. Recognizing that ICANN is actively working most of these issues with other constituents, we focused our attention primarily on security, and we welcomed ICANN's invitation to contribute actively on that topic.

In Paul Twomey's June 21, 2009 letter, he directed his offer to engage the sector to the American Bankers Association (ABA), BITS, the Financial Services Information Sharing and Analysis Center (FS-ISAC), and the Financial Services Technology Consortium (FSTC). While those four associations collaborated in developing a response, we also reached out to a number of other organizations, including our member companies, several non-U.S. financial services trade associations, and select experts.

Our efforts concentrated on two objectives. The first was to identify potential process changes within the Guidebook that would allow ICANN and the sector to both identify and evaluate applications for new gTLDs where their use was primarily for offering financial services. The second objective was to identify a set of security, stability and resiliency requirements for these financial TLDs. Based on our discussions with Greg Rattray, we tried to keep these requirements at a higher level rather than a very detailed level.

We have attached two documents to this letter. The first, "Financial Associations Recommendations-gTLD Application Process (Final)," presents our proposed Guidebook process changes to address financial TLDs. The second, "Financial Associations Recommendations-gTLD Requirements (Final)," contains our security, stability and resiliency requirements for these gTLDs.

Based on our discussions to date, we understand that ICANN will review and evaluate this input, and then determine what to integrate into the next version of the Guidebook and how to integrate it. We certainly will be available to ICANN to answer any questions or discuss any concerns regarding our recommendations during these next steps.

American Bankers Association
BITS
Financial Services – Information Sharing and Analysis Center
Financial Services Technology Consortium

Our associations and members look forward to seeing and commenting on ICANN's incorporation of this input into the Guidebook. We also applaud ICANN's efforts to address our concerns outside of the security realm, and look forward to seeing the results of the consultations in those areas.

While we prefer to work all of these issues directly with ICANN, they are of great importance to our industry, and we are considering a number of options for managing the risks that they pose to our member institutions and their customers. We remain hopeful that, by partnering with ICANN, we will be able to resolve these issues and will not have to take other preventive or mitigating measures.

Again, we are grateful to ICANN for recognizing the need for high security within financial TLDs, for inviting the industry to communicate its requirements, and for ICANN's active collaboration as we developed and delivered the results. We look forward to continuing this dialog with the ICANN staff and with the broader ICANN community.

Sincerely,

Mr. Doug Johnson, Vice President, djohnson@aba.com
American Bankers Association

Mr. Leigh Williams, President, leigh@fsround.org
BITS

Mr. Bill Nelson, President and CEO, bnelson@fsisac.us
Financial Services-Information Sharing and Analysis Center

Mr. Dan Schutzer, President, dan@fsround.org
Financial Services Technology Consortium

Cc:

Mr. Doug Brent, Chief Operating Officer, ICANN, Doug.brent@icann.org
Mr. Kurt Pritz, Senior Vice President of Services, ICANN, Kurt.pritz@icann.org
Mr. Greg Rattray, Chief Internet Security Advisor, ICANN, Greg.Rattray@icann.org
Mr. Don Rhodes, Policy Manager, ABA, drhodes@aba.com
Mr. Paul Smocer, VP Security, BITS, pauls@fsround.org
Mr. John Carlson, SVP Regulatory, BITS, john@fsround.org
Mr. Andrew Kennedy, Project Administrator, BITS, andrew@fsround.org
Mr. Roger Lang, Managing Executive-Security SCOM, FSTC, roger@fsround.org

Attachments (2)

**Financial Services Industry
Recommendations for Process Changes to ICANN gTLD Application Process and Guidebook
In Support of Financial Services gTLDs**

gTLD Application Process Step	Party Responsible for Step	Proposed Process Additions	Subsequent Applicant Guidebook Changes	Notes
Application Submission	Applicant	<ul style="list-style-type: none"> • Establish a methodology to identify applications for gTLDs that will be used primarily for offering financial services 	<ul style="list-style-type: none"> • Inclusion of a checkbox used by applicant to identify use of gTLD to offer financial services, and • Add an attestation statement to the application wherein the applicant and its proposed registry services attest to their willingness to adhere to industry requirements if the gTLD will be used to offer financial services. (Will require updates to the application itself, as well as to Module 6 Top-Level Domain Applications – Terms and Conditions) • Inclusion of a section in the application for applicant to define proposed use of gTLD 	<ul style="list-style-type: none"> • Offering financial services defined to mean that the gTLD would be used primarily to perform financial transactions offered by recognized financial institutions including banks, saving associations, investment houses, and insurance companies. Financial transactions includes use to inquire about financial records of such institutions.

**Financial Services Industry
Recommendations for Process Changes to ICANN gTLD Application Process and Guidebook
In Support of Financial Services gTLDs**

gTLD Application Process Step	Party Responsible for Step	Proposed Process Additions	Subsequent Applicant Guidebook Changes	Notes
Administrative Completeness Check	ICANN	<ul style="list-style-type: none"> • Validate that applications whose proposed usage suggests financial services have properly marked the checkbox • Segregate applications for gTLDs whose primary purpose is the offering of financial services • Validate that applicant and its proposed registry services have attested to their plans to adhere to industry requirements and have submitted documentation supporting plans to conform 	<ul style="list-style-type: none"> • Expand explanation of Administrative Completeness Check (1.1.2.2) • Expand explanation of Initial Evaluation elements (1.1.2.3) 	

**Financial Services Industry
Recommendations for Process Changes to ICANN gTLD Application Process and Guidebook
In Support of Financial Services gTLDs**

gTLD Application Process Step	Party Responsible for Step	Proposed Process Additions	Subsequent Applicant Guidebook Changes	Notes
Objection Filing/Dispute Resolution	All	<ul style="list-style-type: none"> • Establish a formal Financial Services Panel for assessing financial service-oriented gTLD applications (enhancing the Community Objection principles noted in section 3.4.4) • Charge the above panel with: <ul style="list-style-type: none"> • Reviewing all filed gTLD applications to: <ul style="list-style-type: none"> ▪ Ferret out any applications overlooked as being financial service oriented in prior steps ▪ Identify applications for string names that could cause public confusion in inferring a core function of providing financial services (enhancing principles noted in section 4.2.3) • Reviewing applications for financially-oriented gTLDs to assure planned compliance with industry requirements • Provide preliminary endorsement to proceed through the rest of the application process, conditional endorsement or rejection of reviewed gTLD applications. 	<ul style="list-style-type: none"> • Need to update text regarding Objection Filing to recognize panel and its purpose (Sections 1.1.2.4, 3.1.1, 3.1.2, 3.1.2.4, 3.2.1, 3.2.3, 3.4.4, 4.2.3) 	<ul style="list-style-type: none"> • Financial Services Panel: <ul style="list-style-type: none"> • Potential members for this panel could consist of representatives from financial industry associations, financial regulatory authorities, data/identity protection organizations (e.g., the French Data Protection Authority (“CNIL”)) and civil society • Representatives should be drawn from at least three major geographic areas (e.g., Asia, Europe and North America) • As an alternative, would ICANN consider refining the concept of the expert panel (describing in 3.3.4) that contributes earlier in the application review process. • The existence of this panel does not obviate the concept currently stated in the AGB that “established institutions” in the financial services community have the right to object to any application. • The current DRSP for Community Objections is the International Center of Expertise of the International Chamber of Commerce (ICC). If the ICC has a role in financial gTLD reviews, it must have financial expertise.

**Financial Services Industry
Recommendations for Process Changes to ICANN gTLD Application Process and Guidebook
In Support of Financial Services gTLDs**

gTLD Application Process Step	Party Responsible for Step	Proposed Process Additions	Subsequent Applicant Guidebook Changes	Notes
Extended Evaluation	ICANN	<ul style="list-style-type: none"> • Require an Extended Evaluation in situation where: <ul style="list-style-type: none"> • The gTLD string could be associated with financial services • The application raises technical issues that may adversely affect the security of the financial services industry or its customers 	<ul style="list-style-type: none"> • Expand concept to include “if the applied for gTLD string or one or more proposed registry services raises technical issues that may adversely affect the security of the financial services industry or its customers” (1.1.2.5) 	
Dispute Resolution	ICANN	<ul style="list-style-type: none"> • No changes to proposed process assuming changes to Objection process noted earlier are acceptable 		
String Contention	ICANN	<ul style="list-style-type: none"> • No changes to proposed process 		

**Financial Services Industry
Recommendations for Process Changes to ICANN gTLD Application Process and Guidebook
In Support of Financial Services gTLDs**

gTLD Application Process Step	Party Responsible for Step	Proposed Process Additions	Subsequent Applicant Guidebook Changes	Notes
Transition to Delegation	ICANN or Approved "Auditor"	<ul style="list-style-type: none"> • Assure contract terms include industry-requirements for financial gTLDs • Ensure pre-delegation testing adequately tests control expectations set in industry requirements • Require an ongoing assurance that financial services gTLDs continue to operate according to industry requirements 	<ul style="list-style-type: none"> • Update Section 5.1 (Registry Agreement) to include requirements • Expand Section 5.2 (Pre-Delegation Testing) to include questions and criteria related to industry-specific requirements • Enlarge Section 5.4 (Ongoing Operations) to require periodic control reviews of financially oriented gTLDs 	<ul style="list-style-type: none"> • Section 5.4 currently states, "The registry agreement contains a provision for ICANN to perform audits to ensure that the registry operators remain in compliance with agreement obligations". If, as suggested earlier the industry requirements for financial gTLDs are incorporating into the agreement, this issue may be resolved. If not, then the section's text should be expanded to include audits of compliance with those requirements. In addition, we would need to assure that audits exist for registrars and registrants as well. • The suggested roles for the compliance audit environment would be: <ul style="list-style-type: none"> • ICANN certifies and selects audit firms • Registry operators, registrars and registrants engage certified firms.

Financial Services Industry Financial Services gTLD Control Requirements

This section addresses the control and security requirements the financial services industry believe should apply to any gTLD whose primary purpose is the offering of financial services.

This document provides a list of security and stability control requirements for any generic Top Level Domain (gTLD) whose purpose is to provide financial services. The financial services industry believes that such gTLDs should only exist in a highly secure environment given that banks, brokers, insurance, investment companies and others whose primary business is the offering of financial services will use such gTLDs to offer a myriad of such services to the public. The public expects their financial activities to be kept secure, and these financial institutions desire to provide these services in as secure an environment as is technically possible. Covered entities will be required to provide independent confirmation of their compliance with these standards. These standards are promulgated as of August 2009, and will be updated as necessary.

- Registry Operator Controls
 - Domain Name Registration/Maintenance (Create, Renew, Modify, Delete, Revoke/Suspend, Transfer)
 - *Shared Registration System (SRS) implemented to Internet Engineering Task Force's Extensible Provisioning Protocol (EPP) RFC standards with support for business rules and registry policies that are well defined and appropriate for any TLD offering primarily financial services*
 - *DNSSEC must be used for all DNS transactions from initial implementation of the domain*
 - Domain Records
 - Digital Certificate Requirements
 - *Each domain name should be linked to a digital certificate*
 - Encryption Requirements
 - *All traffic among registry operators, registrars and registrants must be encrypted*
 - *All domains must utilize HTTPS when the activity includes the display or entry of non-public personal information, the display of financial records, or the transacting of financial activities*
 - *All data related to authentication credentials associated with the interaction of registry operators, registrars and registrants must be encrypted in storage*
 - Defined Naming Conventions
 - *Registry must adhere to naming conventions endorsed by the Financial Services Panel and agreed to by any gTLD applicant*
 - Authentication Requirements
 - *Registry must require that Registrars accessing Registry services use strong, dual factor authentication to ensure only authorized access. The dual factor authentication methodology utilized at any given time should be at least at NIST Level 3 (or preferably Level 4).*
 - *Registry Operator must provide non-discriminatory access for all approved registrars*
 - Maintenance and Accuracy of Contact information (i.e., WhoIS data)
 - Ownership, Technical, Administrative
 - *While ICANN currently requires annual verification as a minimum, for financial gTLDs verification must be quarterly.*
 - *Proxy registrations will not be permitted within the financial gTLD environment.*
 - Resolution Services
 - *DNS lookup services must be available at all times with rapid response to all queries*

Financial Services Industry Financial Services gTLD Control Requirements

This section addresses the control and security requirements the financial services industry believe should apply to any gTLD whose primary purpose is the offering of financial services.

- *Registry operator must offer Thick Whois*
- Server Configuration/Maintenance Standards
 - *Server configuration and maintenance must be consistent with NIST Special Publication SP-800-123, "Guide to General Server Security"*
- Business Continuity Requirements/Backup And Disaster Recovery Capabilities
 - Planning
 - *Registry operations should be located in a geography with minimal exposure to natural disasters*
 - *Registry operations must provide sufficient physical redundancy to assure continuous operations of the domain in the event of a natural or man-made physical disaster. Planning should consider the requirements imposed on critical US financial institutions as embodied in "Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System issued by the Federal Reserve, the Department of the Treasury's Office of the Comptroller of the Currency, and the Securities and Exchange Commission.*
 - *Registry operators should plan for ability to withstand and quickly recover from a cyber attack including ability to recover from known attack scenarios including distributed denials of service and penetration attacks (i.e., those which take advantage of unfixed vulnerabilities)*
 - Testing/Simulations
 - *Registry operator must test its physical recovery capabilities at least annually*
 - *Registry operator must test its cyber attack recovery capabilities at least semi-annually*
 - *Registry operator must be willing to participate in at least one major industry-level physical disaster simulation and one major industry-level cyber attack simulation annually*
 - Auditing of Backup and Disaster Recovery Capabilities
 - *Registry operator must make its backup and recovery plans and test results available for third party verification by an industry-approved review service independent of the registry operator*
- Ongoing Monitoring Requirements
 - *Registry operator must be able to detect variations from expected "normal" state of IT operations*
 - *Registry operator must be able to detect actual and potential cyber attacks*
 - *Registry operator must have and monitor a reliable source to gather physical and cyber threat intelligence*
- Incident Management Process Requirements
 - *Mitigation of threats, be they physical, cyber or operational, must occur without degradation to ongoing operation and legitimate domain traffic*
 - *Registry operator must inform registrars and registrants of threat intelligence it identifies as a result of its own monitoring and must have capability to issue immediate alerts upon identification of critical or high-risk incidents*
- Change Management Process Requirements
 - *Registry operator must implement procedures related to environmental changes in hardware, software or operations that incorporate adequate pre-implementation*

Financial Services Industry Financial Services gTLD Control Requirements

This section addresses the control and security requirements the financial services industry believe should apply to any gTLD whose primary purpose is the offering of financial services.

planning and notification to parties potentially affected, adequate pre-implementation testing, post-implementation testing and adequate back-out contingencies

- Security
 - DNSSEC Requirements
 - *Top level gTLDs - must comply with industry standards and best practices for DNS signing*
 - *Registry operator must require DNSSEC for all domain names and sub-domains in the gTLD whose purposes include access to private information, financial information or the execution of financial transactions*
 - *DNSSEC must be employed minimally with NextSecure/NSEC (and preferably with NSEC3)*
 - Encryption
 - *Registry operator must require all traffic utilize a minimum of 128-bit encryption*
 - Key Management Controls for Signing Keys
 - *Registry operator must have adequate procedures to control the upgrade, replacement, retirement of encryption keys for both the TLD keys and domain name zones*
 - ◆ *An optional but value-added service would be for the registry to provide technical help, tools and services to assist registrars (and maybe registrants) with key management*
 - Other Security Requirements
 - *Registry operator must utilize commercially reasonable defense in depth protections including network and personal firewall protections, intrusion prevention, filtering to block malicious traffic, etc.*
 - *Registry operators must monitor their environment for security breaches or potential indicators of security issues utilizing commercially reasonable monitoring tools including IDS monitoring, etc.*
 - *Optionally, registry operator should offer distributed denial of service mitigation services to all sites within a financial services gTLD*
 - Periodic Security Testing Standards
 - ◆ *Registry operator must perform at least annual network penetration testing*
 - Certificate Issuance and Maintenance (Issue, Revoke, Modify)
 - *Registry operator must utilize Internal Registry Systems should be protected using PKI certificates for authentication and encryption of sensitive data*
 - *Registry operation must have written policies and procedures for key generation and storage, and aging and renewal of certificates (including alerting to certificate recipients of upcoming expirations)*
- Registrar Control (Undertaken by the Registry Operator)
 - Number of Registrars
 - *Registry operator should limit the number of registrars to the fewest possible to effectively serve any financial services gTLD*
 - ◆ *If permissible under ICANN rules, registry operator may also serve as the sole registrar for a financial gTLD*
 - Criteria for Vetting of Registrars
 - *Registrars associated with financially-oriented domains, prior to initial acceptance as a Registrar, must be subject to:*
 - ◆ *Extensive Financial Background Check (preferably at least 10 years back)*

Financial Services Industry Financial Services gTLD Control Requirements

This section addresses the control and security requirements the financial services industry believe should apply to any gTLD whose primary purpose is the offering of financial services.

- ◆ *Extensive Criminal Background Check (preferably at least 10 years back)*
- ◆ *Approval By the Financial Services Panel*
 - *Consideration should be given to performing these checks on Registrar principles and employees*
- *Registrars must be revalidated based on the above criteria at least quarterly. If the Registrant fails any of these checks during any post-initial acceptance revalidation, the Registry operator should suspend the Registrar.*
- *Registry operator must monitor registrar fraud activity looking for patterns indicative of inappropriate registrar controls*
- *Registry operator must have written policies and procedures for registering, suspending and terminating registrars*
 - ◆ *Registrar registration procedures must include processes to validate that registrar data provided is accurate*
 - ◆ *If the Registry Operator becomes aware of financial or criminal issues regarding an accepted Registrars or if the quarterly review reveals such issues, Registrar must be suspended or terminated*
 - ◆ *Registry Operator must possess the capability to transfer services between registrars with no disruption of service*
- **Data Escrow Requirements**
- **Auditing and Compliance Requirements**
 - *Registry operator must agree to having an annual, independent assessment of its compliance to all of the above industry requirements via a third party verification by an industry approved review service independent of the registry operator*
 - *Registry operator must agree to provide the results of the independent assessment to the Financial Services Panel (defined in process document) and agree that a summary of the report can be made publicly available.*

Financial Services Industry Financial Services gTLD Control Requirements

This section addresses the control and security requirements the financial services industry believe should apply to any gTLD whose primary purpose is the offering of financial services.

- Registrars
 - Authentication
 - *Registrars must provide strong, dual factor authentication to their Registrant facing portals to ensure only authorized access. Two factor authentication should be required for when adding, deleting or modifying any domain registration information and for account review or monitoring. The dual factor authentication methodology utilized at any given time should be at least at NIST Level 3 (or preferably Level 4).*
 - Sub-Domain Registration/Registrant Controls (Undertaken by the Registrars)
 - Initial Registration
 - *Registrars must evaluate all initial requests for domain name registrations. Evaluation must include:*
 - ◆ *Registrars must assure that any registrants in a financial gTLD are approved financial institutions as defined by the Financial Services Panel (i.e., Company Validation)*
 - *Possible methodologies include formal membership in a recognized and registered trade association, issuance of a formal charter by an in-country financial regulator, approval by an established financial community governance board.*
 - ◆ *Validation that the IP addresses associated with the domain names validly belong to the financial institution (i.e., IP Block Validation)*
 - ◆ *Validation that contacts associated with the registrant are valid employees of the financial institution before being granted access credentials (i.e., Credentials Validation)*
 - ◆ *Validation that the registrant possesses the legal right to use the domain name (i.e., Copyright, Trade Name Registration, Brand Name Registration Validation)*
 - *Registrars may complete the process for this brand-name protection validation in multiple ways. One possibility, in the context of the current IRT's suggestions, may involve financial institutions registering their protected names within an IP clearing house, which the registrar would then check.*
 - ◆ *Validation that the requesting party has the valid right to use the payment mechanism it is utilizing (i.e., Financial Validation)*
 - ◆ **N.B.** *Financial institutions often utilized third-party service providers or business partners to provide Internet services. Where that is the case, the Registrar must perform the above Company Validation on the financial institution utilizing the provider or partner. In addition, the financial institution must verify to the Registrar that the provider or partner has a current and active relationship with the institution. Once the institution completes that verification, the Registrar will complete the remaining validations on the provider or the partner. In these situations, the Registrar should reconfirm with the financial institution the continuing nature of these relationships annually.*

Financial Services Industry Financial Services gTLD Control Requirements

This section addresses the control and security requirements the financial services industry believe should apply to any gTLD whose primary purpose is the offering of financial services.

- *Registrars must establish SLAs for timely approval of domain name registrations and Registrants*
- **Renewal**
 - *Registrars must offer the option to allow automatic renewal of domain name registrations*
 - *Registration of domain names should last for an extended period of time before requiring renewal (e.g., a minimum of ten years)*
 - *Registrar must possess the ability to notify domain name holders of upcoming expirations of domain name registrations at least 180 days prior to such expirations.*
 - *Registrars must establish SLAs for timely renewal of domain name registrations and Registrants*
- **Registrar Standards for Monitoring Registrants**
 - *If a Registrar becomes aware that registrants and their registered domains are exhibiting patterns of inappropriate activity indicative that the registrant's domain(s) are being used as attack points for such activities as phishing, malware download, etc. and indications of fraudulent activity, the Registrar should notify the Registry Operator and the Registrant immediately so that both parties can investigate.*
- **Registrant Registration, Suspension and Termination Processes**
 - *Registrars must have rapid suspension or termination procedures to react to either direct requests from registrants for suspension or termination or to react to situations in which the Registrar's monitoring indicates an issue*
- **Auditing and Compliance Requirements**
 - *Registrars must agree to having an annual, independent assessment of its compliance to all industry requirements via a third party verification by an industry approved review service independent of the registrar*
 - *Registrars must agree to provide the results of the independent assessment to the industry through its governance committee (defined in process document) and agree that the report can be made available to any registrant served by the registrar*

Financial Services Industry Financial Services gTLD Control Requirements

This section addresses the control and security requirements the financial services industry believe should apply to any gTLD whose primary purpose is the offering of financial services.

- Registrants
 - Criteria for Registrant Behavior
 - *Registrants in a financial gTLD must be approved financial institutions as defined by the Financial Services Panel (i.e., Company Validation)*
 - ◆ *Possible methodologies for identifying “approved” financial institutions include formal membership in a recognized and registered trade association, issuance of a formal charter or validation by an in-country financial regulator, approval by an established financial community governance board. Regardless, the final approval criteria need to be standardized and applied consistently to the extent feasible across all financial gTLDs, but certainly within any particular financial gTLD.*
 - *In situations where the use of an in-country authority approval has consistently led to evidence of lax controls over entry of registrants coupled with resulting abuse by approved registrants, a method must exist to remove that authority from the list of approving authorities.*
 - Security Requirements
 - Authentication
 - Registrant to Registrar/Registry Operator Authentication
 - ◆ *Registrants must control authentication credentials associated with communication to Registrars and the Registry Operator, particularly those credentials associated with the ability to add, delete or modify the Registrant’s records*
 - Registrant Requirements for Users of Registered Domains
 - ◆ *Registrants must comply with the minimum authentication requirements for users of its domains required by its financial regulator, though Registrants are encouraged to utilize dual factor authentication for any activity involving display of private personal or financial information or conduct of financial transactions.*
 - Secure Web Browser Considerations
 - *Registrants are encouraged to have EV Certificates for all registered domains that they plan to use for the display or entry on non-public personal information, the display of financial records, or the transacting of financial activities*
 - *All confidential traffic (e.g., HTTPs, SMTP) should utilize NIST standard 128- bit encryption*
 - Audit and Compliance Requirements
 - *Registrants’ controls should be subject to review by its financial regulator, or if their financial regulator does not perform such reviews, by a third party verification by an industry approved review service independent of the Registrant.*

Future Considerations Financial Services gTLD Control Requirements

This section relates to future considerations regarding the financial services industry's requirements for any gTLD whose primary purpose is the offering of financial services.

- Requirements Definitions (Threat and Risk Assessments)
 - Environmental, control technique improvements and other factors will change over time and we need to keep our requirements up to date to reflect such changes. Given that, the Financial Services industry anticipates updating these requirements every two to three years. As with this version of the requirements, we will rely on the expertise of financial associations and their members and will engage with appropriate, external experts.