Potential RDE Provider Risks & Conflicts: Iron Mountain

Please address, with detailed explanation, the following questions:

Potential Conflicts of Interest

1. Does the applicant own or is the applicant otherwise affiliated in ownership or management with an accredited registrar? Yes.

   If yes, please describe:
   (a) the nature of the relationship with an accredited registrar, including common management and/or control;

   Iron Mountain Information Management, Inc. owns an accredited Registrar – Iron Mountain Intellectual Property Management, Inc (also referred to as Intellectual Property Management or IPM) but does not operate currently as a fully-functioning registrar. IPM has two service lines – technology escrow and corporate domain name registration and management solutions. The registrar accreditation belongs to the Domain Name Management Services (DNMS) group which is separate from the "technology escrow" business. The IPM business reports into Iron Mountain Digital (IMD) which then in turn reports to the parent company Iron Mountain Incorporated. The technology escrow and DNMS business units operate from separate physical locations, have independent service delivery platforms, management and key personnel structures up to the Director level. Common management is at the IPM Vice President level inclusive of sales and service delivery. Vice Presidents do not have access to the front or backend systems which support Iron Mountain's RDE and registrar related businesses. Furthermore, IPM has managed its existing RDEA business under a sub group in the technology escrow group that provides Designated Third Party services and is described further below.

   (b) the policies and practices the applicant will utilize to avoid potential abuse of its position as ICANN's RDE provider (if retained by ICANN)?

   The following items summarize at a high level Iron Mountain's response to ICANN:

   The current RDEA business for registries is administrated out of the RDEA group in San Diego, CA and is contained within a group that specializes in "designated third party" services. The bulk of the work performed by this group today is to hold copies of electronically stored information of brokers and dealers under Rule 17a-4 of the Securities Exchange Act for the benefit of the Securities and Exchange Commission and self regulated organizations like the NASDAQ and NYSE for the protection of electronic records of broker-dealers in the United States. This group is highly audited by broker-dealers and self-regulating organizations and provides trusted services to regulated industries similar to ICANN's RDE requirements for registrars. It is here where the RDE business for ICANN and Registrars will be managed and delivered.

   The RDE and DNMS service delivery teams are housed in separate locations. The RDE service delivery team operates in San Diego, CA, US and the infrastructure team is in Collegeville and Boyers, PA, while the DNMS service delivery and infrastructure team operates out of Ashburn, VA. The hardware systems for both teams are completely separate and the teams utilize different software to complete their work. Each system requires a separate login to access and utilize the system. Logins are provided only to the service delivery team using that system. This means that neither team can login into the other's system and audits of these systems exist to support security protocols.

Additionally, the IT systems for both services are housed behind internal firewalls, as well as external firewalls, to protect the data from being accessed by unauthorized persons. Physical access to ALL Iron Mountain facilities, inclusive of these two, is controlled by access card and other physical security measures and protocols.

Iron Mountain Incorporated is a publicly traded company and is required to manage its business in accordance and in compliance with a variety of state and federal regulations such as Sarbanes-Oxley. Gramm-Leach-Bliley (in connection with services provided to financial institutions) and HIPAA (in connection with services provided to medical institutions), as well as its own Safety and Security standards. Iron Mountain is also SysTrust certified. SysTrust certification is a rigorous process developed by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) to provide independent assurances that an organization's systems are reliable and operate without material errors, faults, or failures. The Scope of the Current Certification Program is focused on four essential principles: (1) security, (2) availability, (3) processing integrity, and (4) confidentiality. Each principle is supported by well-defined and detailed criteria that encompass an organization's infrastructure, software, people, procedures and data. Iron Mountain engaged Ernst & Young (E&Y) to perform the SysTrust audit, which was most recently certified on March 23, 2007. The certification is located at the following link: https://cert.webtrust.org/ironmountain_systrust.html.

This certification process encompasses Iron Mountain's general IT infrastructure in North America, including: our production data center operations, server configuration and database administration, storage management systems and disaster recovery processes; as well as our network operations, system monitoring tools and processes, system security (both logical and physical), change management and common support processes.

Iron Mountain is willing to take additional steps to reassure ICANN as follows:

- Three Executive Level Control: Will require the VP of Operations, SVP of Operations, and President of Iron Mountain Digital to authorize any collocation of any data between the two groups with notification to ICANN within 48 hours. Notification to be initiated by the two Operational Managers of RDE and DNMS to be used only for:
    - Emergency Contingency and Disaster Recovery planning
    - Facilitation of Movement of assets (pre notification required)
- Specific briefing and notification to ICANN should any of the personnel in the above listed positions be changed.
- Annual auditing of our RDE operations as related to services contractually provided to ICANN

ICANN should note that IPM's business model of acting as a trusted neutral third party requires us to confidentially manage separately and on a routine basis, intellectual property (in forms of patents, trade secrets, copyrights and trademarks) competitive data, source code and proprietary information of companies that compete with each other, including at times Iron Mountain itself. Iron Mountain has its reputation to protect as a trusted services provider and more revenue and business is tied to this then what the ICANN RDE project represents. In other words, we have more to lose than just ICANN as a customer due to a material breach of our contractual obligations.

2. Does the applicant sell domain names or otherwise register domain names on behalf of others? Yes.

   If yes, please describe:
   (a) the nature of the relationship, including common management and/or control;

   Iron Mountain is an accredited Registrar and also acts as a reseller of domain names on behalf of its clients. Iron Mountain's DNMS is available to corporate clients (there is no retail model). The DNMS team registers, renews (also called manages) and modifies gTLD, sTLD and ccTLD domains for its clients. Currently the DNMS team registers and manages the majority of its clients' domain names through other registrars, partners or 3rd party providers and is not utilizing its registrar accreditation for the majority of its work.

   and

   (b) the policies and practices the applicant will utilize to avoid potential abuse of its position as ICANN's RDE provider (if retained by ICANN)? See 1(b) above.

3. Does the applicant own or is the applicant otherwise affiliated in ownership or management with a gTLD registry or ccTLD registry? No.

   If yes, please describe:
   (a) the nature of the relationship with the registry, including common management and/or control; N/A and

   (b) the policies and practices the applicant will utilize to avoid potential abuse of its position as ICANN's RDE provider (if retained by ICANN)? N/A

4. Does the applicant own or is the applicant otherwise affiliated in ownership or management with an internet hosting company, DNS provider, search engine, data collector/aggregator, SEO service provider, or other ISP? Iron Mountain does offer internal hosting on a defined limited basis to its DNMS clients. As a courtesy, the DNMS group offers to host the DNS of only its clients. The majority of DNMS clients host their own DNS. This service is not available to non-DNMS clients, and is not sold as a separate product.

   If yes, please describe:
   (a) the nature of the relationship, including any common management and/or control;
   See 2(a) above

   and

   (b) the policies and practices the applicant will utilize to avoid potential abuse of its position as ICANN's RDE provider (if retained by ICANN)? See 2(b) above.

5. Does the applicant hold other business interests related to domain names, including but not limited to those of a commercial registrant, intellectual property management company, law firm, or anti-spam/phishing organization? Yes.

   If yes, please describe:

(a) the nature of those business interests;

i. Iron Mountain does act as a commercial registrant in three ways; 1) to represent its own intellectual property (IP) protection and branding interests; 2) to assist its corporate clients in securing domain names anonymously to protect IP for various reasons (e.g., a new brand is launching and the corporate client wants to secure the domain name so no one else does, yet they don't want to make the new brand public knowledge until the official launch); and 3) to assist its corporate clients in securing ccTLD names in jurisdictions where the client cannot qualify.

ii. DNMS resells the online monitoring services, ULTRA, of a firm named Avestar, IP to our current clients to assist with identifying IP infringers in an automated fashion. The ULTRA technology uses algorithms to crawl the Internet searching for domain name registrations, webpage content, auctions, blogs, etc. which use the clients IP or a variation of it. ULTRA is not an anti-spam or anti-phishing product, but is similar in that it searches the internet looking for content or domain registrations that would be concerning to an IP owner and then delivers the results through an online interface.

and

(b) the policies and practices the applicant will utilize to avoid potential abuse of its position as ICANN's RDE provider (if retained by ICANN)?

i. See 1(b) above

ii. Avestar, IP has complete control over the ULTRA technology and we are merely a partner reseller. Our access to the tool is equivalent to the access our clients have – to log into the tool, view data, take action on that data, produce reports, etc. In order for data to be delivered via ULTRA a revenue-generating contract must be executed with Avestar, IP. Once a contract is executed, DNMS, Avestar and the client discuss the parameters which need to be set in order to receive the desired results and Avestar programs the backend of the solution.

6. Does the applicant have business relationships with affiliates, partners, or clients whose interests may be adverse to those of ICANN or registrar-depositors? Iron Mountain has over 100,000 corporate clients worldwide to whom we provide a variety of services around protection and management of information and corporate records. While we pride ourselves in providing total customer satisfaction and knowing our clients business we are unable to say with certainty that we do not store a box of records for someone whose interest or opinions differ from ICANN. We are not knowingly engaged with any companies whose interest may be adverse to ICANN.

If yes, please describe:
(a) the nature of the relationship(s); N/A
and

(b) the policies and practices the applicant will utilize to avoid potential abuse of its position as ICANN's RDE provider (if retained by ICANN)? Iron Mountain will respond in a timely manner to any request that ICANN makes if it believes a conflict exists. In our agreement we will also provide the ability for ICANN to terminate its relationship with Iron Mountain if sufficient assurances can not be provided to address any concerns.

7. Would the applicant have any other potential conflict of interest if selected to provide RDE services for ICANN? None that we are aware of. However, Iron Mountain has over 100,000 corporate clients worldwide and there are nearly 1000 registrars. It is possible that Iron Mountain provides services to companies whose interests are competitive to those of ICANN or registrar-depositors.

   If yes, identify the conflict(s) and describe the policies and practices the applicant will utilize to avoid potential abuse of its position as ICANN's RDE provider (if retained by ICANN)? N/A

8. What legal warranties is the applicant willing to make to ICANN and registrars with regard to abuse of deposited data or other information obtained through its position as ICANN's RDE provider (if retained by ICANN)? Iron Mountain shall provide all equipment and qualified personnel necessary to perform or provide the RDE services, including, without limitation, the Software, the System and the Support Services in a manner that will meet or exceed prevailing standards, practices and procedures applicable to these services. Iron Mountain will not use or disclose the deposited data except as required to perform or provide the RDE services.

9. If the applicant is an ICANN-accredited registrar, how will it satisfy its RDE obligations as a registrar in a way that allows for meaningful protection of registration data? Iron Mountain will satisfy its RDE obligations in a fashion which is mutually agreeable between itself and ICANN. There are three options which we feel would provide for meaningful protection of the data. They are:

   i. Iron Mountain can provide its RDE data to a TPP
   ii. Iron Mountain can deposit its data directly with ICANN by providing ICANN with the hardware necessary to receive the data. ICANN would already have and own the PERL scripts necessary to validate the data. If needed, Iron Mountain could assist and provide instruction on how to set up the systems, launch the PERL scripts, pull the periodic samples, and access the data in the event of an Iron Mountain registrar failure.

10. If the applicant is an ICANN-accredited registrar, would it terminate, assign, or otherwise divest itself of its accreditation?
    Iron Mountain does not believe that its accreditation in the DNMS business area is in conflict with its ability to perform the RDE services to ICANN and the registrars. We would request that ICANN refer to the responses in this document about the controls and separation of our business operations and our response on May 31, 2005 to Mr. Kurt Pritz about our approval for accreditation. The link to this letter on your website is http://www.icann.org/correspondence/johnson-to-pritz-31may05.pdf. Iron Mountain is willing to discuss this further with ICANN to understand its concerns but does not currently plan to terminate, assign or otherwise divest itself of its accreditation.

11. If the applicant is an ICANN-accredited registrar, what value, if any, might the accreditation add to the applicant's provision of registrar data escrow services? As stated previously, Iron Mountain does not operate these service lines jointly and therefore dialogue between the two groups is limited. On the surface, the accreditation could be considered a value add to the RDE service in that maintaining it allows Iron Mountain to keep-up with the latest changes and better anticipate changes to the market and technologies required to provide better and more secure escrow services to ICANN.

This operational awareness also ensures that we are kept up to date with local, state, national, and international regulations to better protect ICANN and Iron Mountain. This is not a two-way street as there would be no direct advantage to the DNMS business.

Other Potential Risks

1. Please describe the applicant's preparedness for business continuity risks set out below:

   A. Loss of key personnel
   B. Natural disaster or other destruction of physical property
   C. Hacking or other intentional disruption
   D. Hardware failure
   E. Connectivity disruption

   Iron Mountain maintains comprehensive Disaster Recovery Planning procedures. A summary that answers many of the questions below is included here for ICANN's review. ICANN should be aware that because of the proprietary nature of our disaster plan and the potential for compromise of our business recovery strategy, IM does not provide specific documents to customers or any other non-Iron Mountain personnel. If ICANN has additional questions a call with our Security and Safety team at our corporate offices can be arranged.

   Business continuity planning and vulnerability assessment at Iron Mountain is the responsibility of each potentially impacted department. To facilitate such planning at the local level, Iron Mountain maintains a comprehensive Disaster Planning/Business Recovery template. The philosophy behind these disaster plans is one of "prepare by disaster, recover by discipline." In order to ensure the appropriate recovery of customer assets, Iron Mountain maintains national account relationships with three international disaster recovery vendors. They are as follows: BMS Catastrophe, Munter's Moisture Control and Belfor Disaster Recovery Solutions. The specific methodology for recovery of an asset will depend upon the nature of the damage and the media involved. Wet paper records and media, for example, can be effectively recovered through the use of freeze drying and/or desiccant dehumidification. Magnetic media requires more careful handling and cleaning in addition to appropriate drying techniques.

   By policy, Disaster Recovery plans are to be tested annually by each District/Branch. Corporate guidance is issued relative to the testing methodology to be used and the resolution of any identified gaps in the plan.

   From an Information Technology perspective, Iron Mountain adheres to industry standard best practices by utilizing a multi-tiered approach in the management of all infrastructure hardware and software components. This applies to the following areas:

   - Daily Operations,
   - Disaster Recovery Preparedness,
   - Business Continuity.

   Within the Information Technology arena, specific recovery plans are developed based upon the individual systems/applications being hosted. These plans are typically developed by service offering to address the respective needs of our customers.

From a corporate offices standpoint, our business operations use redundancy and automated fail-over to provide high availability for critical processes via our divisional facilities in Collegeville, PA. Each functional department manager has the responsibility for ensuring that its critical processes are identified and that capability for recovery exists. The overall design of our disaster recovery effort utilizes our existing highly available infrastructure and diverse geographic locations to provide for immediate fail over of our critical business applications in the event of disaster. Iron Mountain's multi-tiered approach encompasses physical diversity of data centers/critical operations, redundant network connectivity over diverse Tier-1 services providers, and highly available secure ingress gateways.

The hallmark of Iron Mountain is in the value it places on the security of its customer's information assets. To that end, specific Iron Mountain Disaster Recovery plans are considered company propriety and not for disclosure. This ensures that we fulfill our obligations to protect our customers in all aspects of their records and information management needs.

Data Processing Continuity

Network Disaster Recovery/Business Continuity

Iron Mountain's network consists of three data centers interconnected by a redundant high-speed ATM backbone with diversified switching to provide a fault tolerant, high-capacity infrastructure. The network is engineered with high capacity connections to diverse ISPs providing redundant Internet connectivity. An Autonomous System Number permits the use of BGP to provide fault tolerant inbound access. Security of this network is achieved using firewall inspection modules running on scalable appliance solutions, providing fault tolerance and redundancy. The architecture has been engineered in accordance with industry best practices to support multiple DMZ networks allowing for secure redundant private connections to our customers and partners. These connections are facilitated via our private SONET ring network. Recent strategic alliances and business partnerships allow for bandwidth on demand through optical technologies to support both public and private connectivity requirements.

In addition to our existing data centers and in support of our Digital Services offerings, Iron Mountain has constructed a state of the art data center 200 feet underground in our 113-acre highly secure facility — National Underground Storage. This facility utilizes high capacity and redundant optical technology such as SONET terminals, ATM switches and optical IP routers. This engineering approach provides flexible and scalable growth with potentially unlimited capacity within one of the worlds most secure locations.

Iron Mountain exceeds industry standard best practices related to the management of all infrastructure hardware and software components, both in terms of their daily operations and in relation to disaster recovery preparedness and business continuity. Iron Mountain has on staff several CDRP (Certified Disaster Recovery Professionals) who are regarded in the industry as experts. The overall design of our disaster recovery effort utilizes our existing highly available infrastructure to provide for immediate fail over of our production database in the event of a disaster. We constantly run, in our recovery center, a standby version of our database infrastructure. Every 10 minutes archive logs are sent from our production site to our disaster recovery site over our secure private network. Copies of all production tapes are created daily and shipped offsite to a secure location. In the event of a disaster these tapes would immediately be shipped to our recovery site. The disaster recovery plan associated with the query and ingestion process for external access to our archive utilizes an implementation of TCP/IP and BGP. This implementation allows us automatically, within our private TCP/IP address space to redirect any network traffic to our disaster recovery site in the event of a disaster. This architecture affords us the ability to continuously ingest data and accept query traffic from our external customers.

Corporate Office Continuity

The need for comprehensive business continuity plans for the corporate offices has long been clearly understood as an essential function. As part of this recognition, Iron Mountain's corporate critical business operations have deliberately migrated towards full redundancy utilizing the technical infrastructure available at our Boston, MA; Collegeville, PA; Boyers, PA; and Renton, WA computing sites. The failover capability for all key operational processes to our alternate locations is an effective and best-practice recovery strategy for business. Such capability limits the reliance on specific written plans for each business process which require the intervention of a "human resource" to activate or implement.

Local Facility Continuity

Standard Disaster Recovery Planning Documentation

Since an identical business interruption scenario (for example, severe weather) can result in single or compound problems (for example, personal injury, transportation disruptions, power loss and building damage) remediation efforts will be dictated by the extent of the event. We have established the following priority for our disaster recovery efforts:

1. Saving of lives and first aid to the injured.
2. Reduction and/or prevention of further damage.
3. Restoration and recovery of damaged property.

In order to ensure the appropriate recovery of customer assets stored at its facilities, Iron Mountain maintains national account relationships with three international disaster recovery vendors. They are: BMS Catastrophe, Munter's Moisture Control and Belfor Disaster Recovery Solutions. The specific methodology for recovery of an asset will depend upon the nature of the damage and the media involved. Wet paper records and media, for example, can be effectively recovered through the use of freeze drying and/or desiccant dehumidification. Magnetic media requires more careful handling and cleaning in addition to appropriate drying techniques.

Iron Mountain is committed to the protection of its customer assets. Our relationship with these vendors is designed to provide our customers with the best emergency services available. While it remains our goal to do everything possible so that we never require the services of our disaster recovery partners, we take our responsibility to be prepared seriously.

The Cover Page and Table of Contents from our most recent Disaster Recovery/Business Resumption template are shown below to provide an overview of the extent of our emergency preparedness planning for local facilities.

Disaster Planning and Business Recovery

Table of Contents

Attachment A — Employee Emergency Roster
Attachment B — Emergency Telephone Directory
Attachment C — Evacuation Priority Listing
Attachment D — Emergency Equipment and Supplies
Attachment E — Treatment of Damaged Records
Attachment F — Facility Site and Floor Plan
Attachment G — Disaster Prevention/Response Resource List
Attachment H — Bomb Threat Telephone Card

Pandemic Planning

Iron Mountain takes business continuity planning very seriously. As such, we are constantly evaluating threats that could impact our ability to serve our customers. A pandemic influenza is one such threat.

Federal, state, and other local government agencies are working together to respond to pandemic influenza and to maintain essential health care and community services if an outbreak should occur. Led by the World Health Organization, governments all around the world are preparing for the possibility of a pandemic outbreak.

The current World Health Organization (WHO) pandemic status is level 3, which means that there is none, or very little human-to-human transmission. Our goal is to reduce the impact of any pandemic through prevention efforts and to respond appropriately to ensure minimal business interruption.

Iron Mountain's current efforts include:

- The assembly of an international assessment team, including representatives from HR, Safety & Security, Customer Response and Service Delivery/Operations.
- Issuance of educational and awareness material to our employees about pandemics, including guidance to reduce the risk of infection, such as:
    - Understanding pandemics
    - Manner of transmission of the flu
    - Personal Hygiene tips
    - Counseling to stay home if ill
- Monitoring situation globally utilizing a variety of resources at our disposal
    - Government/regulatory agencies
    - Professional organizations
    - Travel advisories
    - News
- Ensuring that our existing Business Continuity Plans have identified:
    - Roles and responsibilities for response
    - Communication strategies (internally and externally)
    - Use of Iron Mountain personnel from other locations or existing temporary labor agencies to support staff reductions
    - Issuance of appropriate Personal Protective Equipment (gloves/masks/hand sanitizing lotion)—especially to couriers

Iron Mountain's Safety & Security team continues to monitor the status through the WHO. Should the threat level be raised to 4 (showing increased human-to-human transmission), Iron Mountain is prepared to address the situation with contingency planning, such as acquisition and staging of personal protective equipment (gloves, masks, and hand sanitizers), labor deployment, etc. Iron Mountain will proactively communicate with our customers if and when this should occur.

Recovery Protocol Strategy

Iron Mountain has further refined its recovery process by the establishment of a formal recovery protocol strategy. Over twenty senior level Vice Presidents have been trained as Disaster Response Managers. These individuals coordinate all aspects of facility level recovery efforts from infrastructure to customer communication to DR Vendor management.

Summary

Iron Mountain is committed to the protection of its customer assets. Our infrastructure redundancy, our documented pre-planning and response efforts as well as our relationships with our Disaster Recovery vendors planning is designed to provide our customers with the best emergency services available. While it remains our goal to do everything possible so that we are never required to activate our Business Continuity Plans, we take our responsibility to be prepared seriously.

Because of the proprietary nature of our disaster plan and the potential for compromise of our business recovery strategy, do not provide these documents to customers or any other non-Iron Mountain personnel. If a prospect questions this policy, present it as essential to protect customers' assets entrusted to Iron Mountain.

F. Financial failure – Iron Mountain Incorporated is a publicly traded company with strong financial results since its IPO in 1995. The IPM group within Digital is a financially stable business unit. As a trusted third party service provider with recurring revenue streams this business no doubt would survive a financial failure of Iron Mountain as a corporate entity. Furthermore, as a trusted third party escrow agent, assets of our customers (RDE data) are not legally considered assets of the company and could not be tied up in bankruptcy dissolution proceedings by law.

2. What steps will the applicant take to mitigate or avoid the risks noted above if they have not already been addressed?

   Iron Mountain's internal audit performs routine audits on a three-year cycle designed to ensure that all risk areas are addressed in a systematic and risk-based manner.

   Internal Audit at Iron Mountain is an independent appraisal activity chartered to examine and evaluate the Company's activities as a service to the organization. The objective of Iron Mountain's Internal Audit Department is to assist Iron Mountain management in the effective discharge of their responsibilities by providing independent, objective assurance and consulting services designed to add value and improve the operations of our Company. Internal Audit accomplishes this by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of the business risk management, internal control, and governance processes.

Internal Audit has direct reporting responsibility to the Audit Committee of the Board of Directors, and is responsible for providing independent assessment and reporting on the companies' control environment. The department is staffed with trained internal auditors whose expertise is supplemented, as required, by the external accounting firms. All activities performed by the internal audit department are managed by the internal audit director, as required by SEC requirements. Iron Mountain's Internal Audit Director is a Certified Internal Auditor with over twenty years of experience, domestically and internationally.

District and Functional Reviews

The scope of internal audit work performed within the Iron Mountain companies includes audits of district-level financial, operational, and system processes, as well as functional process reviews within divisional and corporate offices. The internal audit department performs an annual risk assessment, which is aligned with the ERCC's Corporate Risk Assessment, to select district and functional processes for review. External auditors also perform analyses and testing of selected districts as part of the year-end audit

District level internal audits include analysis and testing of the following functions:

- Administrative processes
- Account initiation and retention
- Record center/vault library workflow
- Customer billing and revenue management
- Procurement and disbursement procedures
- Safety and security processes
- Fleet management
- Inventory and revenue system testing

Independent Assurance Reviews

Independent Assurance Reviews are occasionally referred to as SAS 70's reviews. We do not currently pursue this certification as it is not specific to our industry and does not relate to the services we provide to our customers. Instead, we pursue a more appropriate certification, SysTrust, which is based on criteria developed by the AICPA (American Institute of Certified Public Accountants) and the CICA (Canadian Institute of Chartered Accountants). This certification is conducted by an independent accounting services firm.

ICANN is welcome to further discuss how Internal Audit works with our Audit department.

3. How does the applicant propose to ensure continuity of ICANN's RDE services and maintenance of stored RDE data in the event of total business failure? See 11 (1) and 11 (2) above.