ICANN Security Questions for CIO

Please note that these questions also extend to the services, equipment and facilities provided by ICANN to PTI.

These questions are roughly based on the high level topic areas of ISO27001 ad are intended to start a dialogue between the SSR2 RT and the ICANN teams responsible for ICANN Orgs internal IT security. These questions are not intended to be encompassing of ICANN's role in the greater ecosystem but rather are focussed on internal IT applications, processes and policies at ICANN org.

- **Scoping Purposes**
  - Does ICANN has a formal service description of all provided services (internal and external)?
  - Has ICANN identified its stakeholders and interested parties and if so, could you provide us an overview?
  - Can you provide an overview of relevant divisions / departments for scoping purposes?

- **Information Security Management System**
  - Does ICANN utilise a formal ISMS (Information Security Management System)?
  - Are the general ISMS objectives compatible mapped to the ICANN strategic plan and ICANN's identified enterprise risks?
  - Is there a formal training plan in place to ensure all staff are aware of the policies and operating procedures of the ISMS?

- **Support and staffing**
  - Are adequate resources provided for all the elements of ISMS?
  - Are required competences defined, trainings performed, and records of competences maintained?
  - Are outsourced processes identified and controlled?
  - Are all relevant employees and contractors being trained to perform their security duties, and do the awareness programs exist?

- **Performance and Auditing**

    - Does an internal security audit program exist that defines the timing, responsibilities, reporting, audit criteria and scope?

- **Asset Management**
    - Is an Inventory of assets drawn up?
    - Does every asset in Inventory of assets have a designated owner?

- **IT System/Product Management**
    - Are security requirements defined for new information systems, or for any changes to them?
    - Are the rules for the secure development of software and systems defined?
    - Do formal change control procedures exist for making any changes to the new or existing systems?
    - Is the outsourced development of systems monitored?
    - Are the criteria for accepting the systems defined?

- **ICANN internal incident response, and vuln disclosure**
    - Does ICANN have a documented incident response plan, with processes and resources identified
    - Does ICANN maintain contracts with third parties to potentially assist in major incident responses
    - Is this incident response plan tested on a periodic basis?
    - Does ICANN have a vulnerability management process?
    - Does ICANN have a vulnerability disclosure policy?

- **ICANN Business Continuity Management**
    - Does the organization have a documented business continuity operational planning and control process?
    - Does the organization ensure that all personnel and/or teams that have been assigned roles and responsibilities in the BCMS especially business continuity procedures and arrangements, are competent and capable of performing their roles?
    - Has the organization established a training programme for all current employees that may be affected by and/or have to deal with a disruptive incident?

- Does the organization have a formal documented standard procedure and evaluation process for conducting a Business Impact Assessment
- Have the Recovery Time Objective (RTO) for each prioritised activity been identified and agreed?
- Does the organization have a documented exercise/testing programme and process for business continuity procedures, plans and arrangements?
- Has a business continuity disaster planning exercise been performed?
- Has the organization identified the dependencies and resources needed to maintain, restore, resume and/or recover each of its prioritised activities to an acceptable level of functionality and performance?
- Is there a documented Corporate (organization) BCM Strategy that has been signed-off by top management?

For risk department:

- **Information Risk Management**
  - Is there an information risk assessment process documented, including the risk acceptance criteria and criteria for risk assessment?
  - Are the risks identified, their owners, likelihood, consequences, and the level of risk; are these results documented?
  - Does Risk treatment plan define who is responsible for implementation of which control, with which resources, what are the deadlines, and what is the evaluation method?