THETA

The Higher Education Technology Agenda

How to mechanize the process of an IT Audit and complete an individual service/application risk assessment using ServiceView

When the words “IT Audit” are mentioned the response is usually a sea of cringing faces. It is well known that audits involve the seemingly endless interactions between an Audit Team and Stakeholders – time that many of us just don’t have. These same interactions seem to repeat themselves at re-occurring intervals and by the time the next audit rounds are due, so many factors have changed resulting in the audit wheel of time starting all over again.

This presentation shows how The University of Queensland uses ServiceView to:

- Ease (borderline automate) the IT Audit process,
- Complete Individual Risk Assessment on each Service to determine:

1. Its’ current level of protection and redundancy,
2. Its’ target level of protection and redundancy,
3. Any areas for potential improvement to assist in meeting these target levels.

The ServiceView application is primarily a single repository for Institutions IT Architecture. To effectively carry out a successful audit on IT Services, ServiceView focuses on the following 3 key risk factors (also commonly known as CIA classification/rating):

- The level of Confidentiality of the data used by the service.
- The level of Integrity of the data used by the service, and
- The level of Availability of the service.

To assist with determining a services CIA rating, each service is posed with a variety of relevant risk questions, such as:

- What level of confidentiality is required for the data being stored by the service e.g. Confidential, Private, For Office Use Only, or Public?
- What level of integrity is required for the data being stored by the service e.g. Some services may not necessarily require extremely accurate data whilst others, such as exam results, will require an extremely accurate level of data.
- What is the service uptime requirements e.g. 24-hours a day, or Business hours only?

These questions are specifically used to determine the level of protection and redundancy currently in place for each service. Once the questions are answered, ServiceView then conducts an assessment of the service by mapping each question to a CIA risk matrix and then provides the service with its CIA classification. A further enhancement of this feature, is that ServiceView not only provides the service with a CIA rating for where the service currently stands, but it also provides the service with a Target CIA rating.

Furthermore, ServiceView is also able to generate a report which shows areas of inadequate protection across the organisation and highlights areas of risk and areas for potential improvement. The CIA classifications and Risk Report provide users at a glance with the ability to see:

- How their service is currently managing risk:
  - Utilising the CIA “Actual” ratings, and
- If there are any potential areas to improve in minimising risk:
  - Reviewing the CIA Assessment report.

Alisha Pham and Chris Parker
University of Queensland