TRAC2 5.2.2

5.2.2 -The repository shall have implemented controls to adequately address each of the defined security risks.

Introduction

SP has implemented controls to address and manage the security threats described in its Risk Analysis and Management Strategies document. The repository manages threats to its operations and content by using administrative procedures and technical controls recommended by the international digital curation community. SP manages some threats without external assistance and others in collaboration with staff from University of Toronto Libraries, OCUL administration, and/or OCUL members. Accordingly, the repository's risk management strategies include activities that involve SP staff only indirectly or not at all (e.g. fire prevention and suppression). These relationships are outlined in the Risk Analysis and Management Strategies document where relevant.

Please see the Risk Analysis and Management Strategies document for details. This document describes policies and procedures employed by SP, University of Toronto Libraries, and the Libraries' Information Technology Services to manage risks.

Responsibility

Numerous personnel are responsible for the design, implementation, and monitoring of security and risk controls. In general, the *Digital Preservation Policy Librarian* is responsible for overall risk management.

Potential Risks

The chief risks associated with security controls are (1) failure to employ controls that address the full scope and scale of the threat and (2) failure to review and update controls in a timely manner. To manage the first risk, SP conducted a thorough analysis of individual threats in order to design controls that address their full scope and scale. Please see 5.2.1 for more information. To manage the second risk, the repository has monitoring commitments in place (see Monitoring Commitments below).

Monitoring Commitments

SP will assess its Risk Analysis and Management Strategies document on a regular basis, according to the Review Cycle for Documentation Policy, or whenever there are major changes to its operating environment such as hardware refreshment, significant staffing level changes, or security incidents. Reassessment will in some cases lead to the adjustment of individual security controls.

Future Plans

SP recognizes that standardized codes of practice, such as ISO 27000, could provide a useful framework for designing and implementing security risk controls.

Relevant Document

1. Risk Analysis and Management Strategies
2. Review Cycle for Documentation Policy