TRAC2 5.2.1

5.2.1 - The repository shall maintain a systematic analysis of security risk factors associated with data, systems, personnel, and physical plant.

Introduction

Comprehensive, systematic risk assessment is essential to the long-term security and reliability of SP and its archived information. Risk assessment helps the repository identify and evaluate threats that could disrupt normal operations or impair its ability to meet its Mandatory Responsibilities and contracted obligations. SP began formally documenting and analyzing risks in the fall of 2011. The participants included key personnel from SP, OCUL, and the University of Toronto Libraries. In many cases, the risk analysis documented threats that librarians, systems administrators, and programmers had already addressed in the design and implementation of the repository.

At present, SP does not employ a third-party code of practice for risk analysis. Instead, SP reviewed risk assessment practices used by a variety of revelant institutions and organizations in order to avoid being 'locked in' to a particular code of practice. Following the review, SP designed a risk analysis model that suited the repository's operating conditions and technical environment.

Please see the Risk Analysis and Management Strategies document for details. This document identifies threats, assesses their probability and potential impact, and provides an overview of the repository's risk-minimization and prevention strategies.

Responsibility

Digital Preservation Policy Librarian

OCUL Executive Director

OCUL Library Directors

Potential Risks

The chief risks associated with risk analysis are (1) failure to review and update the analysis in a timely and consistent manner and (2) failure to acknowledge and analyze foreseeable risks. To minimize the first risk, SP has monitoring commitments in place (see Monitoring Commitments below). To minimize the second risk, SP uses a comprehensive typology of threats as a model for identifying foreseeable and relevant risks (described in the Risk Analysis and Management Strategies document).

Monitoring Commitments

The repository will assess its risk analysis 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.

Future Plans

SP recognizes that formal security audits and third-party vulnerability assessments could be valuable.

Relevant Document

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