BCNET

Shared IT Services for Higher Education & Research

Conference 2018

Building a Strategic Plan for Information Security

Hugh Burley Thompson Rivers University & ISO BCNET

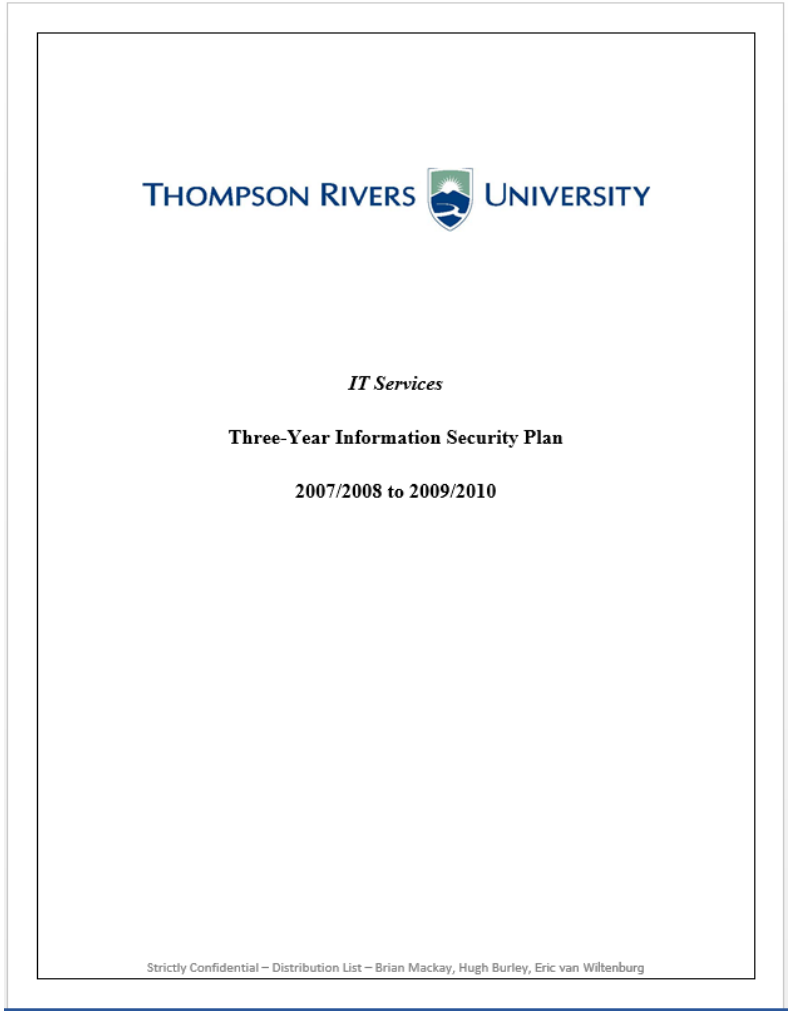
Who’s in the room today?

- CIO or Senior IT Director/Leader
- Information Security (Chief, Director, Manager, Analyst, Officer)
- Privacy (Chief, Manager, Analyst, Officer)
- Other executives (IT, Legal, Administrative)
- Other IT
- Faculty

What would you like to discuss?

- Does strategic planning for information security work?
- What needs to be in place?
- How do you get started?
- How much effort is required?
- What are the components?
- Approaches to delivering the message?
- Other?

Some History 2001- 2018



THOMPSON RIVERS UNIVERSITY

IT Services

Three-Year Information Security Plan

2007/2008 to 2009/2010

Strictly Confidential – Distribution List – Brian Mackay, Hugh Burley, Eric van Wiltenburg

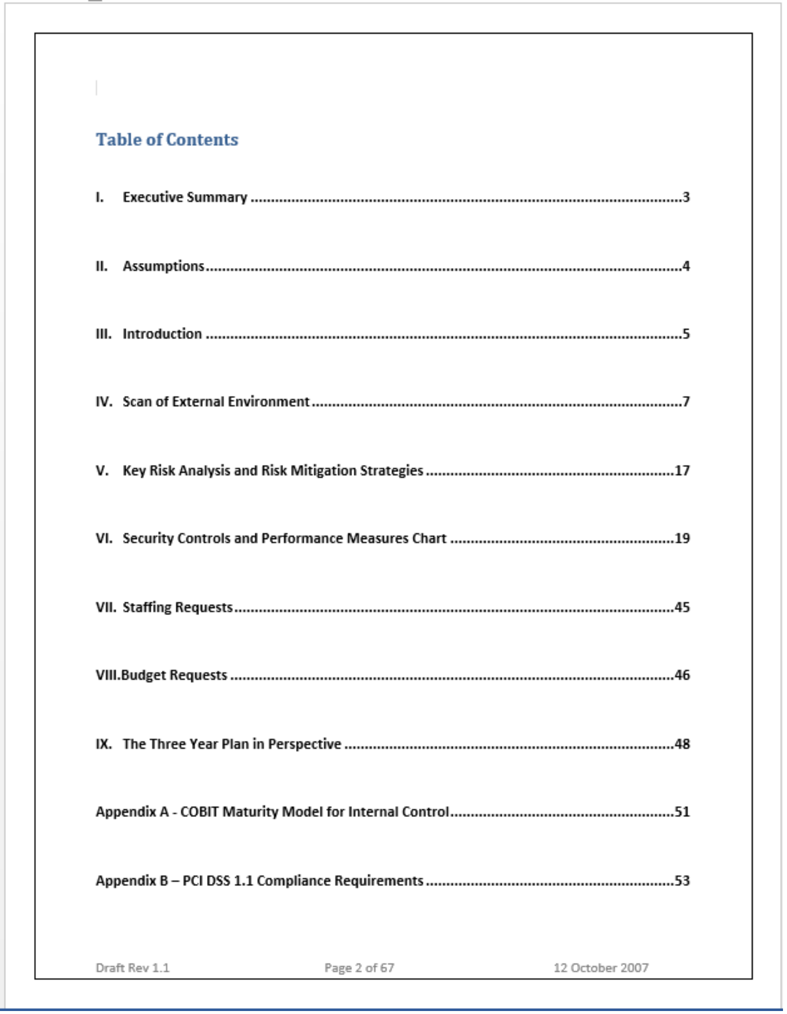
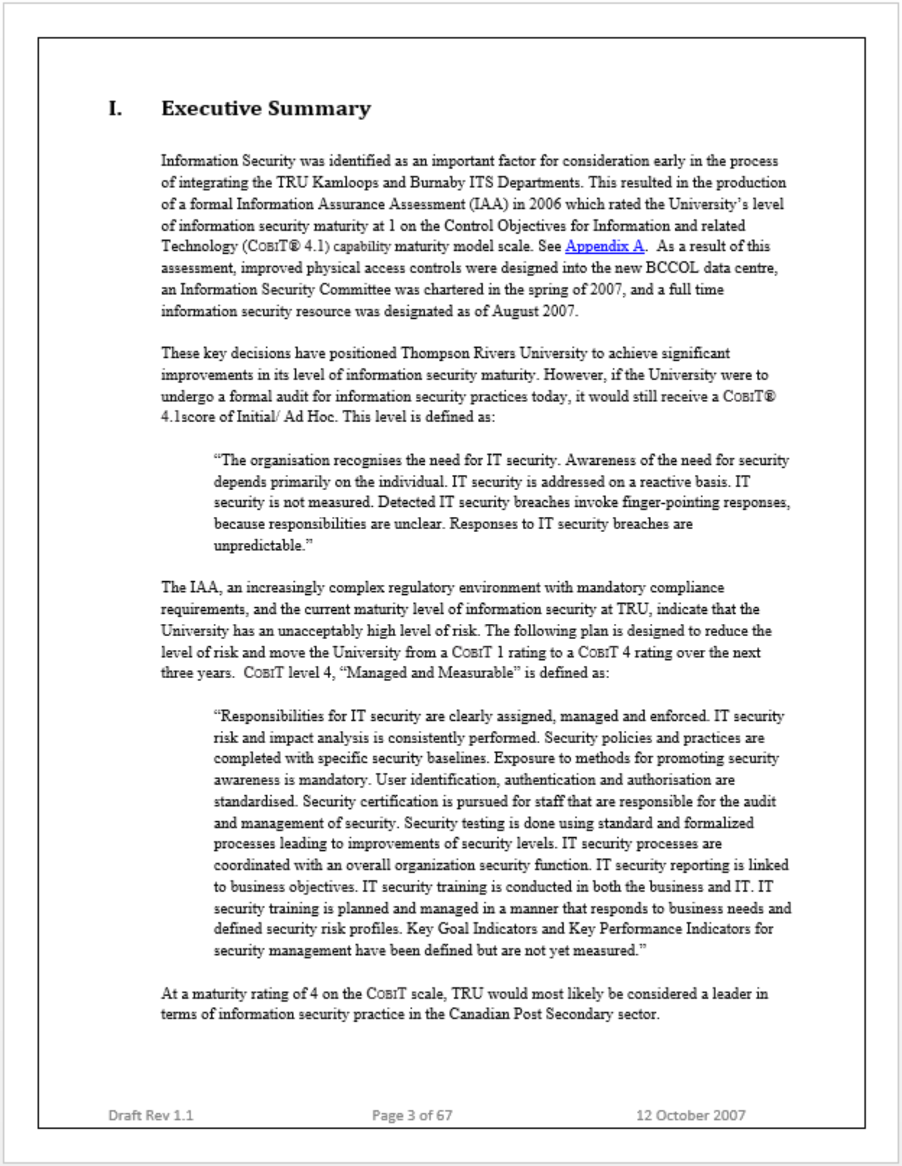


Table of Contents

Draft Rev 1.1 Page 2 of 67 12 October 2007

Some History



I. Executive Summary

Information Security was identified as an important factor for consideration early in the process of integrating the TRU Kamloops and Burnaby ITS Departments. This resulted in the production of a formal Information Assurance Assessment (IAA) in 2006 which rated the University's level of information security maturity at 1 on the Control Objectives for Information and related Technology (COBIT® 4.1) capability maturity model scale. See Appendix A. As a result of this assessment, improved physical access controls were designed into the new BCCOL data centre, an Information Security Committee was chartered in the spring of 2007, and a full time information security resource was designated as of August 2007.

These key decisions have positioned Thompson Rivers University to achieve significant improvements in its level of information security maturity. However, if the University were to undergo a formal audit for information security practices today, it would still receive a COBIT® 4.1score of Initial/ Ad Hoc. This level is defined as:

> "The organisation recognises the need for IT security. Awareness of the need for security depends primarily on the individual. IT security is addressed on a reactive basis. IT security is not measured. Detected IT security breaches invoke finger-pointing responses, because responsibilities are unclear. Responses to IT security breaches are unpredictable."

The IAA, an increasingly complex regulatory environment with mandatory compliance requirements, and the current maturity level of information security at TRU, indicate that the University has an unacceptably high level of risk. The following plan is designed to reduce the level of risk and move the University from a COBIT 1 rating to a COBIT 4 rating over the next three years. COBIT level 4, "Managed and Measurable" is defined as:

> "Responsibilities for IT security are clearly assigned, managed and enforced. IT security risk and impact analysis is consistently performed. Security policies and practices are completed with specific security baselines. Exposure to methods for promoting security awareness is mandatory. User identification, authentication and authorisation are standardised. Security certification is pursued for staff that are responsible for the audit and management of security. Security testing is done using standard and formalized processes leading to improvements of security levels. IT security processes are coordinated with an overall organization security function. IT security reporting is linked to business objectives. IT security training is conducted in both the business and IT. IT security training is planned and managed in a manner that responds to business needs and defined security risk profiles. Key Goal Indicators and Key Performance Indicators for security management have been defined but are not yet measured."

At a maturity rating of 4 on the COBIT scale, TRU would most likely be considered a leader in terms of information security practice in the Canadian Post Secondary sector.

Draft Rev 1.1 Page 3 of 67 12 October 2007

Choosing a framework or frameworks

- CoBiT (4.1 or 5)
- NIST
- ITIL
- ISO 27000
- PCI

Assessment (Where are we now?)

- CoBiT (4.1 or 5)
- NIST
- ITIL
- ISO 27000
- PCI

Determining future state

- Delivering Stakeholder Benefits
- Optimizing Risk
  - Institutional Risk Tolerance
  - Institutional Risk Program
- Optimizing Resources

Who is the audience for the plan?

- The senior information security practitioner
- Senior Risk Executive(s)
- The CIO, CDO
- The Information Security Committee
- The Board and Senior Executive
- ITS
- The broader institutional community
- BCNET and CUCCIO Membership

Trying to communicate

- Policies, Standards and Processes
- Awareness and Engagement
- 2009 information security mtg ppv1.2 2009.pptx
- 2011 ISCPrioritiesNov2011
- 2012 TRU Information Security Strategic Decisions 2012ver1.0
- 2013 ISC Risk Register 2013
- 2015 Audit Committee Presentation 2015

Putting it all together

- 2016-17 Information Security strategic plan 2016
- 2018 TRU - ITRG - Sec gap analysis tool   2018
- Standard Fusion