Next Generation Identity & Access Management (IAMNG)

WATERLOO
INFORMATION SYSTEMS
& TECHNOLOGY
ist.uwaterloo.ca

Program
Introduction

Program Goals

- Common definitions for core institutional roles
- Documented workflows for the efficient provisioning of accounts based on roles
- Well defined governance model for IAM, as part of a greater IT governance model
- A supportable and sustainable IAM system that supports current and future needs
- An IAM system that supports different security assurance levels (aligned with Security Architecture)
- Single Sign-on and centralized authorization for web-based applications.

Program Structure

- 3 Phases
- Each phase is dependent on previous phase
- Checkpoints at end of each phase ensure EA integration

Phase 1

- Institutional Roles/Lifecycles/Sponsors (identity management focus)
- Governance
- Access Control Framework (part of Security Architecture)

Phase 2

- Requirements Definition
- Assess what we have (Sun IDM, CAS, AD, etc…)
- Assess what we need
- RFI/RFP development
- Design next generation AD
- What will it take to get ‘er done?

Phase 3

- Implementation
  - Identity management first
  - Access Management second
- Shift to operational state

Timelines

- Phase I
  - Fall 2013/Winter 2014
- Phase II (Planning)
  - Winter/Spring 2014
- Phase III (Implementation)
  - Fall 2014 and beyond