

Information Security Framework: Phase II

Executive Leader: Helen Patton **Project Manager:** Amber Buening **Technical Management:** Gary Clark, Jim Herbeck
Project Sponsors: Michael Hoffher (Chief Information Officer), Gates Garrity-Rokous (Chief Compliance Officer)

OVERVIEW

University groups know that Information Security is important – a top risk at the University – but it’s hard to know where to focus time and effort. The Information Security Framework provides Ohio State with the tools to organize, measure, and manage information risk.

RATIONALE

The Information Security Framework provides the University with the tools to organize, measure, and manage information risk through an innovative, standards based, functionally organized structure. During FY14, Enterprise Security partnered with campus units to create the Information Security Standard, Information Security Control Requirements, and the first University-wide survey of information risk at Ohio State. This work provided the foundation for Phase II of the Information Security Framework Project.

This year, in Phase II, the project will focus on the three risk management stages - Assess, Implement and Verify. Through this work, Enterprise Security will be able to demonstrate that university units combined efforts have had a positive effect, reducing information risk at the University.

Information Security Framework



RESULTS

This project will create base processes, job aides, training and tools to facilitate the ongoing operation of the OSU Information Security Management System (ISMS) through the following deliverables:

Assess:

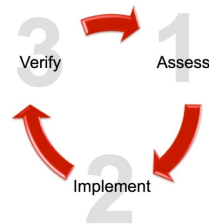
- **Milestone** - Completion of the 2nd Information Risk Survey & completion/submission of units' updated Risk Management Strategies.

Implement:

- **Milestone** - Create 31 priority 1 job aides to help organizations implement Framework & reduce risk;
- **Milestone** - Development & delivery of Framework specific training & awareness materials;
- **Milestone** - Automation of data analysis, management and reporting.

Verify:

- **Milestone** – Work with Internal Audit to create joint testability requirements;
- **Milestone** - Developing information security self-assessments (ISSA)for organizations to start performing self assessment;
- **Milestone** – Complete mapping of the Framework to HIPAA requirements.



End results

Each project milestone will complete according to the FY15 agreed activities. Completion of the entire Phase II project will be September 30, 2015. Future program efforts will extend into FY16 and 17.

RESOURCES

People and their roles

Executive Sponsor: Helen Patton
 Program Owner: Gary Clark
 Tech Lead: James Herbeck

Enterprise Security

- Accountable for ensuring the design and execution of this project.

Partnership with the following groups is also required:

- Unit Security Liaisons – for feedback to the FY15 Assessment questions, and collaboration on job aids
- OCIO Communications – for Security Awareness activities
- Internal Audit – for creation of Audit testability requirements
- OSUWMC Security Team – for HIPAA mapping
- Unit Subject Matter Experts (SME’s) – for feedback and review of developed job aides and processes

Other resources

The Information Security Advisory Board will maintain oversight over these activities serving as a steering committee, reporting to the Board of Trustees.

RISKS

- Resource conflicts due to operational/project priorities
 - Mitigation: Weekly resource alignment touch points

REPORTING

Documentation: <https://ocio.osu.edu/itsecurity>

Bi-weekly Plan/Roadmap:

- Monthly status report to Executive Leader (to be shared with Project Sponsors)
- Monthly status report to the Office of Compliance and Integrity
- Reporting to the Information Security Advisory Board on an as needed basis

REVIEW

Project wrap-up and review: October 2015

Measuring & Managing Information Risk Program Years 0 to 3

