THREE AND GREEN IN 2018

LEADERS

This is being managed by colleges and units as an ongoing governance initiative overseen by the Board of Trustees, and as such, there is no need for a project manager.

TIMELINE: This project will end when the college/unit self-assessments show that risk areas are being managed to an acceptable level. Currently, units are predicting that this will occur by the end of FY18.

FUNDING: FY17: A mixture of Cash and PBA, both within the Enterprise Security team and within distributed colleges and units.

OVERVIEW

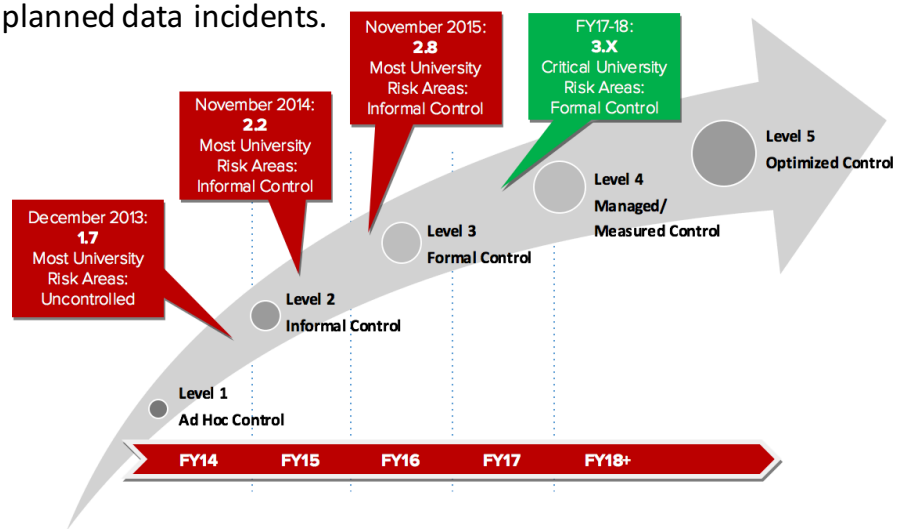
This effort continues the work started in FY15 to bring the university to acceptable levels of managing information risk, in order to address information security threats to our systems. It includes work such as: moving data centers to the SOCC, stopping email forwarding, addressing email retention, and consolidating networks.

WHY IT IS IMPORTANT

Not only do external regulators require that our health, financial, student and research data be securely managed, our students and partners have an expectation of data security that must be met.

WHAT SUCCESS LOOKS LIKE

This effort will ensure we can demonstrate that we are managing information risks according to regulatory requirements, and should result in fewer unplanned data incidents.



RISKS & BENEFITS

RISKS: Regulators can level fines for non-compliance, the university can incur significant additional unplanned expenses to remediate data incidents. Our ability to receive federal funding for student financing, or research, may be at risk.

BENEFITS: Positive outcomes include more efficient operations, lower costs for external audit response, decreased incidents, improved technology capabilities and demonstrating management of risk to regulators.