Information Security Assessment Overview

What is it?

The Assessment is an annual process through which the School CIOs and other senior IT leaders describe the School or unit status regarding University information security policy and related risk mitigation efforts.

How is it conducted?

The process has two phases:

1. Assessment Data Collection - in which School CIOs and senior IT leaders respond to questions aligned with policy and provide a cover letter describing their level of security assurance, disclose any gaps, and describe remediation plans.
2. Assessment Review Meetings – in which the University CISO meets with the School CIOs and IT leaders to review the report and discuss remediation activities.

When are the reports due?

* The Assessment is sent to the Schools and major IT units in June and responses are requested in September.

Why do we undertake this process?

1. It helps us to understand the security status of each School
2. It allows us to identify risk mitigation or policy implementation challenges
3. It supports a University level status report for the University CIO and the University Risk Management Committee
4. It provides input to School and University Risk Management process

Information Security Assessment - Annual Timeline

|  |  |  |
| --- | --- | --- |
| ***Month*** | ***Activity*** | ***Detail*** |
| June | CISO sends Assessment to CIOs  | Assessment includes template for cover letter and set of questions keyed to Requirements |
| June | CISO sends Assessment to HUIT MD’s | Units with complex, strategic, or critical University IT (e.g. enterprise systems) responsibilities provide sub-unit or practice-specific responses |
| July-August | CISO offers office hours to discuss process and answer questions | School security officers and others who contribute to the responses are invited |
| September | School, Central, and HUIT reports due |  |
| September | CISO reviews all data and develops School, University reports | School reports include additional detail regarding risk and vulnerability statistics |
| October-November | CISO meets with each School CIO and security officer | Discuss progress and develop mitigation plan based on remaining risk |
| November | CISO reviews University level report with UCIO and CIO Council |  |