Management Controls for High Risk IT Resources

These documents define a “future state” framework of policies, management controls and objectives which may be eventually used in governing those IT Services operated IT systems and facilities that have been classified as “high risk”. These are collectively referred to as “High Risk IT Resources.” The scope of these policies and controls would be limited to those information systems, processes, and staff identified as having a direct and consequential role in the operation and management of High Risk IT Resources at The University of Chicago. Once implemented, these statements will be reviewed and revised at least bi-annually.

We recognize that not all management controls may be applied in equal measure on all platforms and configurations of systems and services. For example, the use of malicious code protection mechanisms (anti-virus) applies most directly to Windows based systems, secondarily to Linux and MacOS systems, and may have little or no relevance in the context of database transactions or management of network peripherals. So while the controls state a set of objectives, we recognize that the objectives will be realized only to a “commercially reasonable” extent within a specific context. Where useful, specific variations from the objectives will be noted in the documentation for the supporting practices.

These statements describe policies and controls that address the following operational areas as they apply to the operation and management of high risk systems:

1. Access Control
2. Training & Security Awareness
3. Audit & Accountability
4. Security Assessments and Authorization
5. Configuration Management
6. Contingency Planning
7. Identification & Authentication
8. Incident Response
9. Maintenance
10. Media Protection
11. Physical and Environmental Protection
12. Risk Assessment
13. System and Services Acquisition
14. System and Communications Protection
15. System & Information Integrity