



Los Angeles County **BOARD OF SUPERVISORS POLICY MANUAL**

Policy #:	Title:	Effective Date:
6.107	Information Technology Risk Assessment	07/13/04

PURPOSE

To ensure the performance of periodic countywide and departmental information security risk assessments for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

REFERENCE

Board of Supervisors Policy - Information Technology and Security Policy

POLICY

Security risk assessment is a mandatory activity, which encompasses information gathering, analysis, and determination of security vulnerabilities within the County's hardware and software environment, and information technology (I/T) business practices.

Security risk assessment is necessary to analyze and mitigate threats to the County information technology assets, which may come from any source including natural disasters, disgruntled employees, hackers, the Internet, equipment or service malfunction or breakdown.

Security risk assessments shall be conducted on all information systems including applications, servers, networks, and any process or procedure by which these systems are utilized and maintained. Risk assessment shall also be performed on facilities that house information technology resources.

A risk assessment program shall include an inventory of I/T assets, review of I/T policy and procedures, assessments and prioritization of data security vulnerabilities, and implementation of safeguards to mitigate identified

vulnerabilities.

County departments shall periodically conduct and document an information technology risk assessment in accordance with Auditor-Controller requirements.

Compliance

County departments must develop written procedures to comply with this policy. Review and remediation of risk assessment findings is the responsibility of each department.