

SAM – INFORMATION SECURITY
(Office of Information Security)

INFORMATION SECURITY COMPLIANCE
(Revised 6/14)

5330

Policy: Each state entity shall validate compliance with statewide information security policy, standards, and procedures as set forth in this Chapter, and the state entity's internal information security policies to verify that security measures are in place and functioning as intended. Each state entity's validation processes shall include:

1. Ongoing assessments of key security measures and controls in both in-house and outsourced systems;
2. Completion of independent "pre-production" assessments of security controls in new systems or systems that are undergoing substantial redesign;
3. Adherence to the CISO reporting requirements;
4. Coordination of all IT audit and assessment work done by third-party auditors; and
5. Monitoring of third-party auditors' compliance to statewide information security requirements as set forth in this Chapter.

Implementation Controls: NIST SP 800-53: [Security Assessment and Authorization \(CA\)](#)