

SAM – INFORMATION SECURITY
(Office of Information Security)

AUDITABLE EVENTS
(Revised 12/13)

5335.2

Introduction: Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the right level of abstraction is a critical aspect of an audit capability and can facilitate the identification of root causes to events. Each state entity may determine that information systems must have the capability to log every file access, both successful and unsuccessful, but not activate that capability except for specific circumstances due to the extreme burden on system performance.

Policy: Each state entity shall ensure that information systems are capable of being audited and the events necessary to reconstruct transactions and support after-the-fact investigations are maintained. This includes the auditing necessary to cover related events, such as the various steps in distributed, transaction-based processes (e.g., processes that are distributed across multiple organizations) and actions in service-oriented architectures.

Implementation Controls: NIST SP 800-53: [Audit and Accountability \(AU\)](#); [Physical and Environmental Protection \(PE-1\)](#); [Risk Assessment \(RA\)](#)