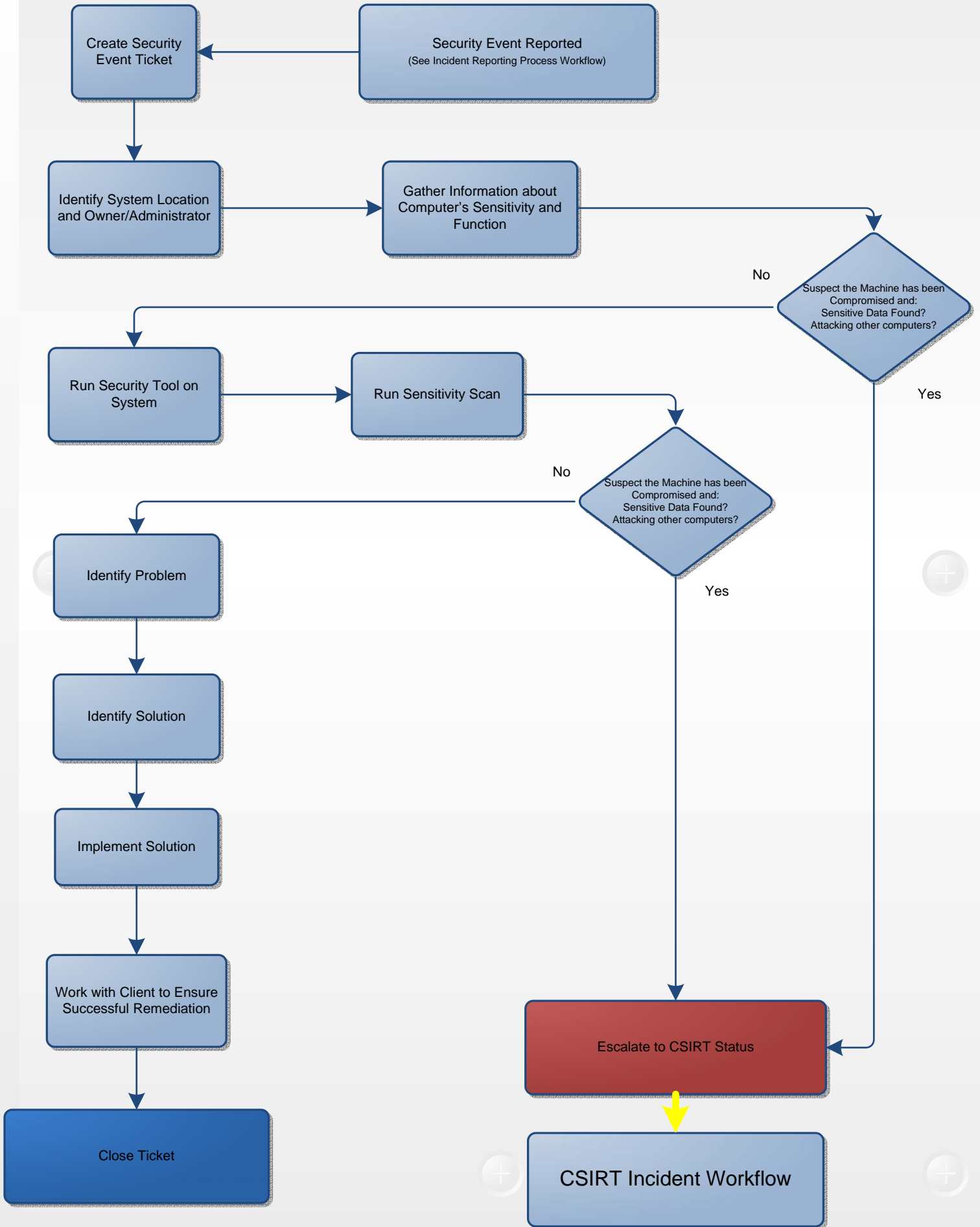


Security Event Workflow



CSIRT Incident Workflow

Security Event Workflow

CSIRT Incident Reported

Create or Escalate Incident Ticket
Contact Exec. Dir.,
Exec Dept. CIO, CIO

Sensitive Data Found?

Run Security Tool

Has Volatile Memory been Captured?

Police Involvement Necessary?

Unplug Power Cord and Confiscate Machine

Make Copies and Images of Hard-Drive(s)

Analyze Image and/or Throwing Copy of Hard-Drive

Initial Report Construction

Sensitive Data Found?

Clear and Reformat Hard-Drives

Report Sensitive Data Findings to Appropriate Person(s)

Police Involvement Necessary?

Return Machine to User

Is there a Reason to keep Forensic Copy of Hard-Drive?

Clear Forensic Copy of Hard-Drive

Keep Forensic Copy of Hard-Drive in Safe

Close Ticket

Final Report Construction

Present Final Report

Escalate Incident to Police Department