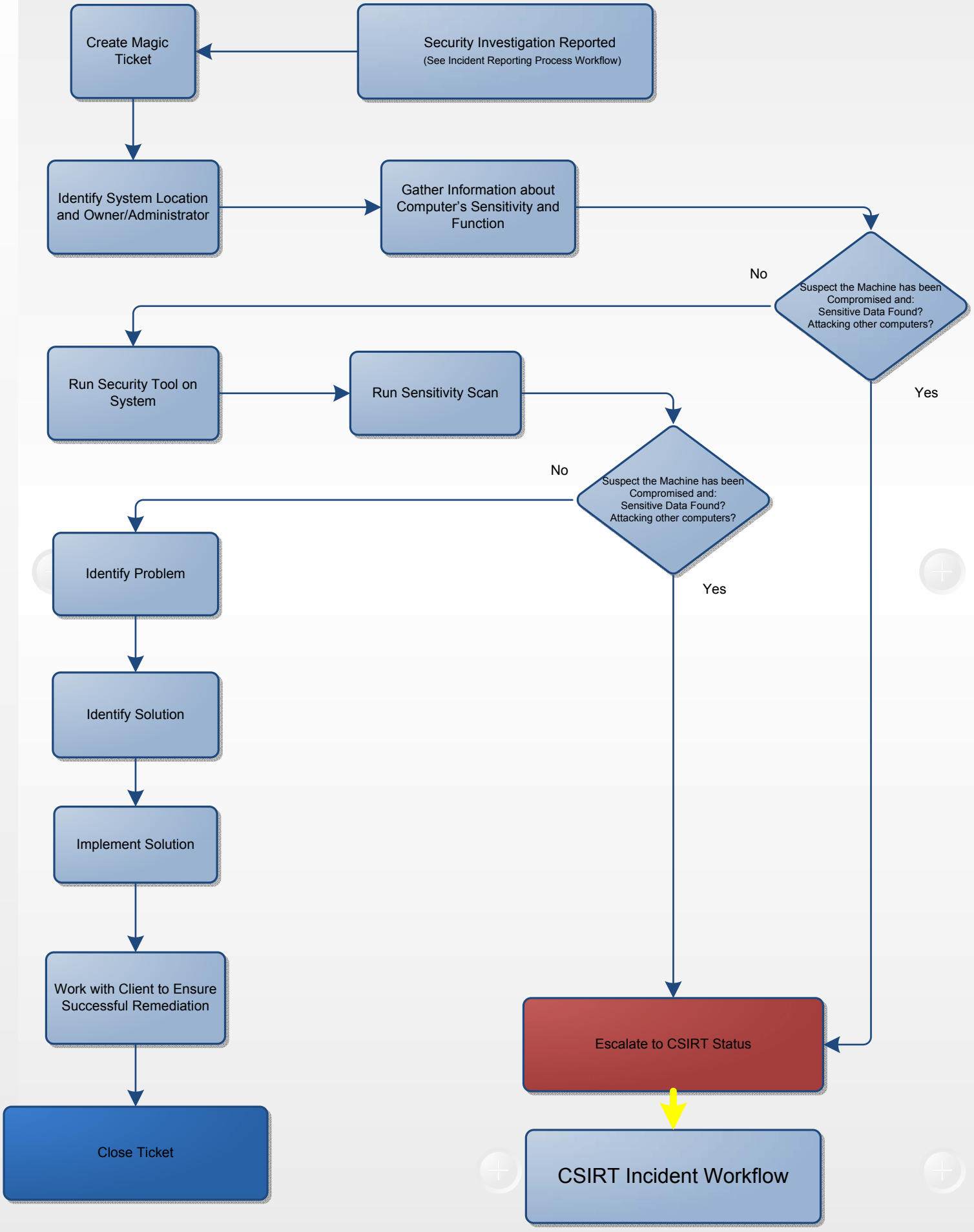
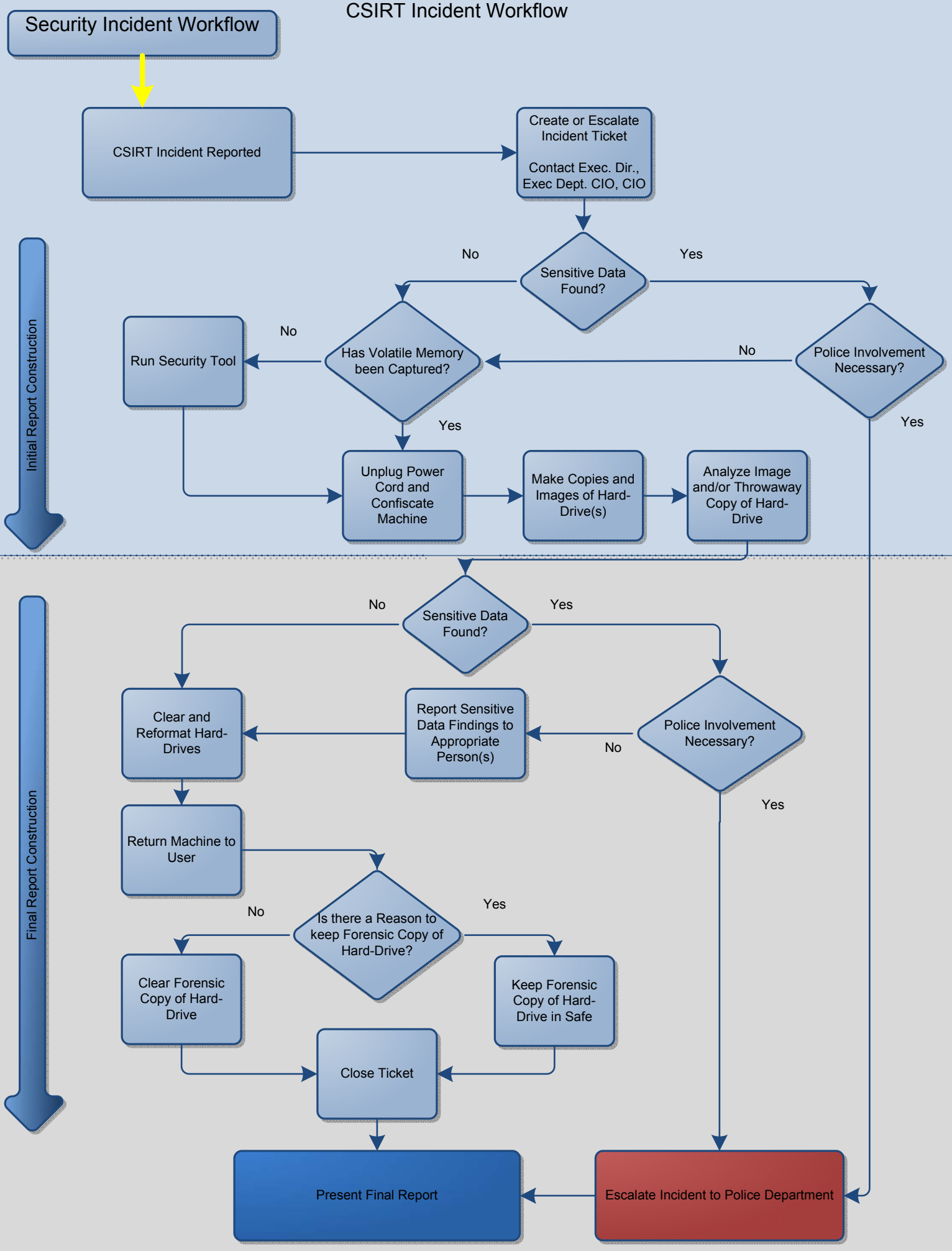
Security Investigatioin Workflow




CSIRT Incident Workflow
Security Incident Workflow
CSIRT Incident Reported
Create or Escalate Incident Ticket
Contact Exec. Dir., Exec Dept. CIO, CIO
Initial Report Construction
Sensitive Data Found?
No
Yes
Has Volatile Memory been Captured?
No
Run Security Tool
Police Involvement Necessary?
No
Yes
Yes
Unplug Power Cord and Confiscate Machine
Make Copies and Images of Hard-Drive(s)
Analyze Image and/or Throwaway Copy of Hard-Drive
Final Report Construction
Sensitive Data Found?
No
Yes
Clear and Reformat Hard-Drives
Report Sensitive Data Findings to Appropriate Person(s)
Police Involvement Necessary?
No
Yes
Return Machine to User
Is there a Reason to keep Forensic Copy of Hard-Drive?
No
Yes
Clear Forensic Copy of Hard-Drive
Keep Forensic Copy of Hard-Drive in Safe
Close Ticket
Present Final Report
Escalate Incident to Police Department