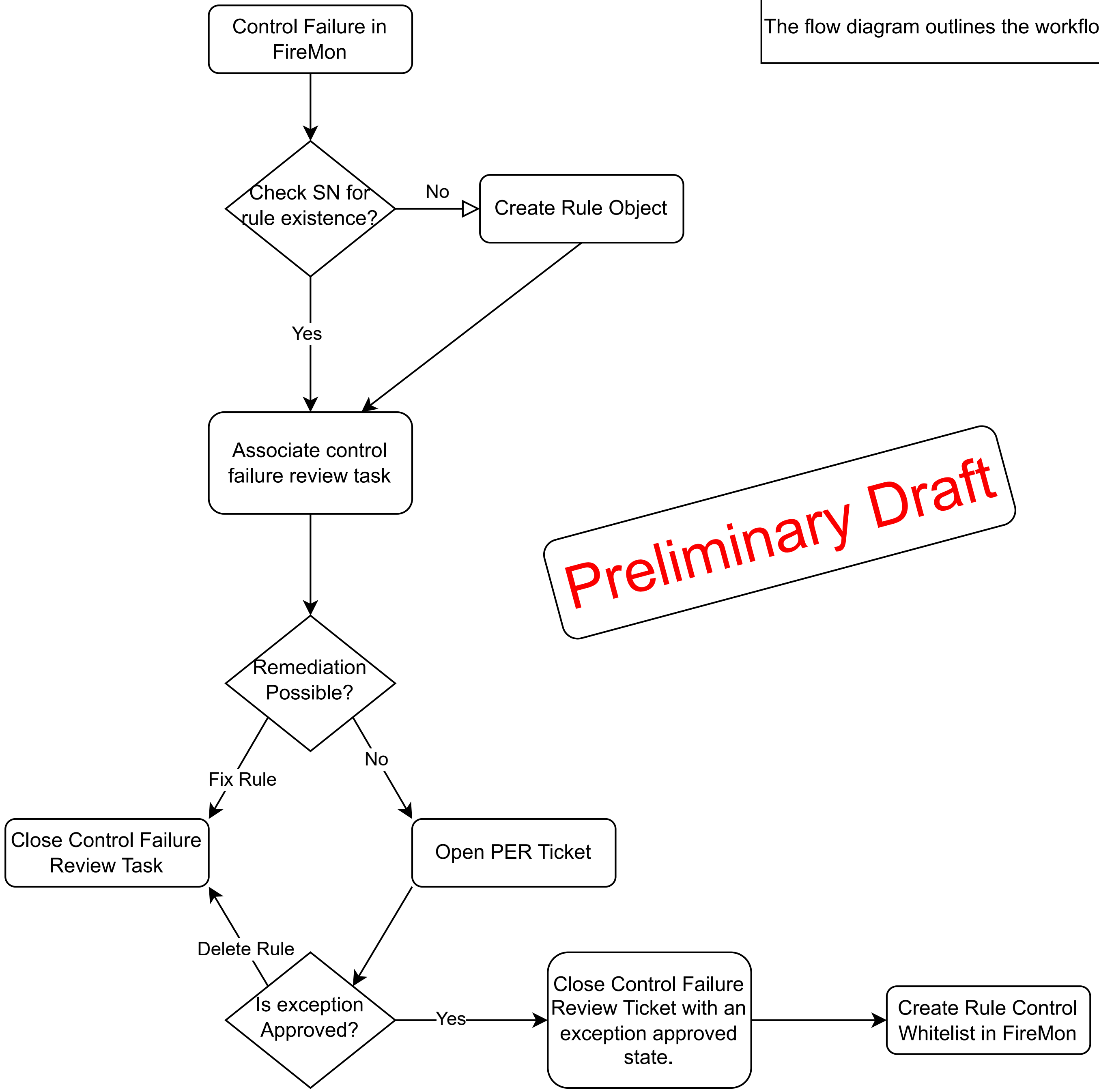
Rule Compliance and Remediation Automation

Control Failure

The flow diagram outlines the workflow automation to manage, document rule control failures to resolution: Fix, Exception or Delete.



Control Failure in FireMon
Check SN for rule existence?
No
Create Rule Object
Yes
Associate control failure review task
Remediation Possible?
Fix Rule
No
Close Control Failure Review Task
Open PER Ticket
Delete Rule
Is exception Approved?
Yes
Close Control Failure Review Ticket with an exception approved state.
Create Rule Control Whitelist in FireMon

Preliminary Draft

Need	Platform	Notes
Rule Object	SN	- Object type 'generic' - Relationship to Panorama? - Rule name, pa uuid, link to FireMon - Why create this? Multiple controls could fail on the same rule, this is a way of bundling the control failure tasks and having reporting visibility in Service Now (often record of truth) of all issues related to a rule. Also provides history of rule remediation related to specific rules.
Control Failure Task	SN	- Control ID, Control Name, Rule Object, Link to FireMon, - Close States: Fixed, Rule Deleted, Exception Approved - Remediation not possible > Open PER - PER approved > Create whitelist in firemon - PER denied > activate Delete Rule Lambda
Lambda Automation	AWS	- Reviews FireMon control failures daily - Creates Rule Object in SN if necessary - Control Failure Task lifecycle in SN - Delete Rule