Root Cause Analysis (RCA)

Description

Include a brief description of the incident

Timeline

Provide a thorough timeline of the incident from initial report to resolution including all troubleshooting steps, communication and major milestones of the incident investigation.

Investigative Team

Document all of the team members involved in response, communication, resolution, and analysis. Include any of your third party providers who were also involved.

Methods Used
What did you do to try to solve it? Include all of the methods used by the investigative team to troubleshoot the issue and manage the response through communication and other means.

Root Cause

This is the final verdict of the analysis. What did you find. Document in detail the cause of the outage or incident. Don't be shy here. You can't learn from it, if you hold back, or fail to share the true details. Of course, if there is proprietary knowledge, keep the distribution list small. You may even consider a code name for the "secret sauce".

Remedy

What did you learn? What are the steps taken to resolve the incident and prevent it in the future along with steps to strengthen the response and investigation process. This is where you include the new monitoring functions, or changes to the response plan. Document what you've learned.