**Example incident management plan for RDS**

**1. Incident Identification and Alerting**

* Define and implement monitoring and alerting mechanisms for AWS RDS instances, including key performance metrics, latency, CPU utilization, storage, and replication status.
* Set up CloudWatch Alarms or other monitoring tools to trigger alerts when thresholds are breached or critical events occur.
* Ensure that the alerts are properly routed to the incident management team through communication channels like email, chat, or incident management platforms.

**2. Incident Triage and Initial Response**

* When an alert is triggered or an incident is reported, the first responder (on-call personnel) acknowledges the incident and starts the triage process.
* Gather information about the incident, including the affected RDS instance, error messages, and any recent changes or deployments.
* Verify the scope and severity of the incident and determine its impact on the business and users.

**3. Escalation and Team Activation**

* If the incident requires escalation, involve relevant stakeholders and escalate to senior members or management as necessary.
* Activate the incident response team and establish clear communication channels for real-time updates and coordination.

**4. Incident Investigation and Diagnosis**

* Conduct a thorough investigation to identify the root cause of the incident. Check AWS RDS logs, CloudTrail logs, and any other relevant logs or metrics.
* Compare the current behavior of the RDS instance with historical performance to gain insights.
* Analyze recent changes to the RDS configuration, software updates, or schema modifications that might have contributed to the incident.

**5. Mitigation and Temporary Remediation**

* Implement temporary workarounds or mitigations to restore the service to an acceptable level of performance or availability.
* Consider scaling up the RDS instance, optimizing queries, or applying other performance improvements if appropriate.

**6. Communication and Status Updates**

* Maintain clear and consistent communication with all stakeholders throughout the incident lifecycle.
* Update the incident management platform, if used, with incident status, findings, and actions taken.
* Provide regular updates to relevant teams, management, and customers, informing them about the incident and its progress.

**7. Permanent Resolution and Post-Incident Review**

* Implement permanent fixes to prevent the incident from recurring.
* Document the incident, including the root cause, actions taken, and lessons learned.
* Conduct a post-incident review (postmortem) with the incident response team to identify areas of improvement and develop action items.

**8. Incident Closure**

* Once the incident is fully resolved, communicate the resolution to all stakeholders.
* Update the incident management platform and any status pages if used, indicating that the incident is closed.

**9. Continuous Improvement**

* Use the lessons learned from the incident to improve processes, documentation, and prevention strategies.
* Schedule regular reviews of incident management procedures to ensure they stay up-to-date and effective.

Remember that each organization's incident management plan may vary based on its specific requirements, team structure, and scale of AWS RDS usage. The playbook should be periodically tested, refined, and updated to adapt to changing conditions and technologies.