

NEW MEXICO
OIL CONSERVATION COMMISSION

Form C-128

Well Location and/or Gas Proration Plat

Date January 13, 1956

Operator El Paso Natural Gas Company

Lease San Juan 30-6 Unit

Well No. 15 Section 29 Township 30N Range 7W NMPM

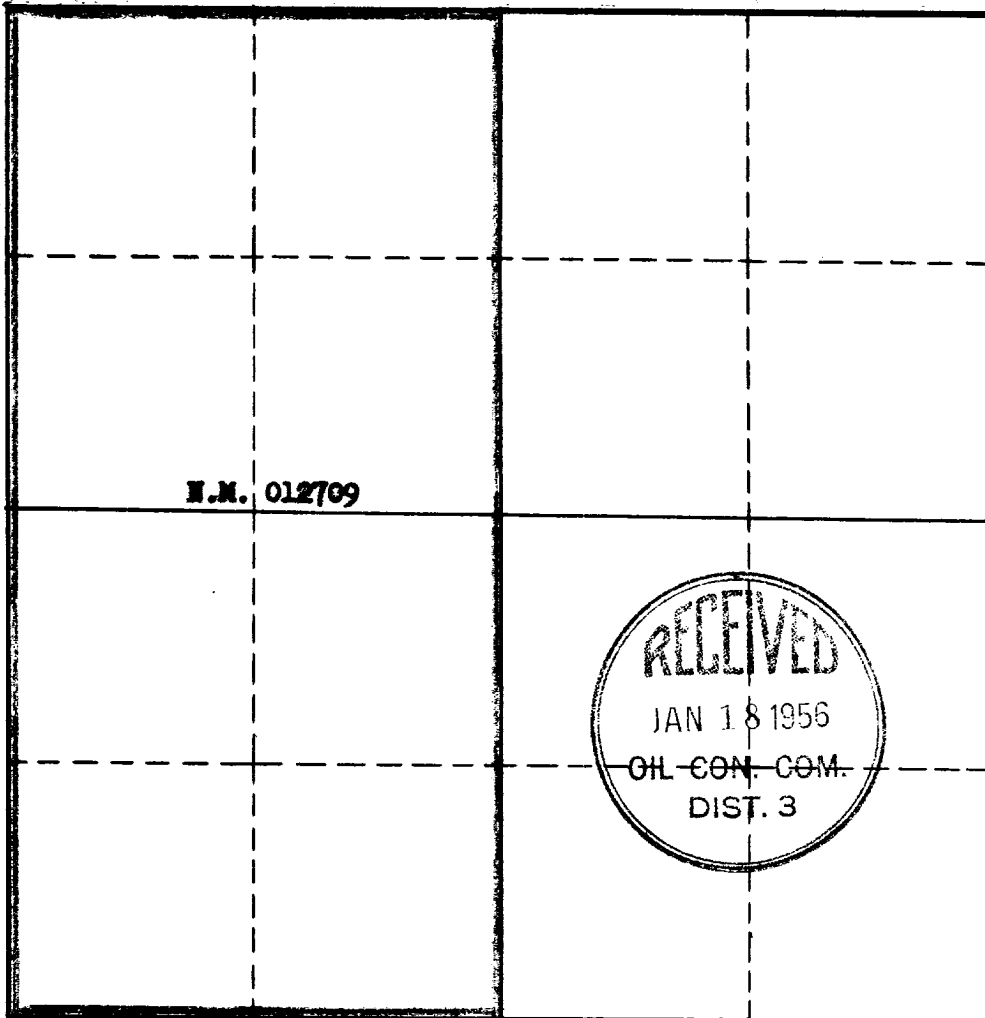
Located 1700 Feet From South Line, 900 Feet From West Line,

Rio Arriba

County, New Mexico. G. L. Elevation 6279

Name of Producing Formation Mesa Verde Pool Blanco Dedicated Acreage 320

(Note: All distances must be from outer boundaries of Section)



SCALE: 1"=1000'

1. Is this Well a Dual Comp.? Yes No X

2. If the answer to Question 1 is yes, are there any other dually completed wells within the dedicated acreage? Yes No

Name E. S. Oberly

Position Petroleum Engineer

Representing El Paso Natural Gas Company

Address Box 997, Farmington, New Mexico

This is to certify that the above plat was prepared from field notes of actual surveys made by me or under my supervision and that the same are true and correct to the best of my knowledge and belief.

Date Surveyed

Registered Professional Engineer and/or Land Surveyor

O-L CONSERVATION COMMISSION

ADAMS PATENT OFFICE

4

[illegible][illegible]

Journal of Management Education 36(7) 809-824

[illegible]

1. The first step is to identify the key components of the system. This includes understanding the hardware, software, and data involved. For example, in a web application, this might involve identifying the server, database, and client-side code.

2. The second step is to analyze the system's behavior. This involves observing how the system responds to different inputs and outputs. This can be done through manual testing or automated testing tools.

3. The third step is to identify potential vulnerabilities. This involves looking for weaknesses in the system that could be exploited by an attacker. This can be done through techniques such as code review, penetration testing, and vulnerability scanning.

4. The fourth step is to develop a plan to address the identified vulnerabilities. This involves determining the best way to fix the issues and implementing the fixes. This may involve updating software, changing configuration, or adding new security measures.

5. The fifth step is to test the system again to ensure that the vulnerabilities have been successfully addressed. This involves running the same tests as in step 2 to verify that the system is now secure.

6. The sixth step is to document the findings and the actions taken. This involves creating a report that details the vulnerabilities found, the steps taken to fix them, and the results of the final testing.

7. The seventh step is to implement the findings. This involves making any necessary changes to the system based on the recommendations in the report.

8. The eighth step is to monitor the system for any future vulnerabilities. This involves regularly checking the system for updates and security issues.

9. The ninth step is to provide training to the system administrators. This involves educating them on the importance of security and how to respond to potential threats.

10. The tenth step is to review the process and make improvements. This involves reflecting on the entire process and identifying areas where it can be made more efficient or effective.
