# Analysis Results

## Problem Management

Alignment result for Problem Management (Level 1): the alignment of the text to the criteria is moderate.   
  
the firm's cloud practice problems are somewhat integrated with the overall problem management practices. however, there are areas where this integration could be improved. for instance, while the firm uses itil-based incident management processes and tools like bmc and remedyforce, there is no formal cloud governance structure. the soc enforces security compliance when possible, but there are limited standardized alerts for permission changes within azure subscriptions. additionally, while root cause analysis is conducted for significant security breaches in azure, this documentation is not standard for all incidents.  
  
-bullet point 1: the firm uses itil-based incident management processes and tools like bmc and remedyforce, indicating some integration of cloud problems with overall problem management.  
-bullet point 2: there is no formal cloud governance structure, and there are limited standardized alerts for permission changes within azure subscriptions.  
-bullet point 3: root cause analysis is conducted for significant security breaches in azure, but this documentation is not standard for all incidents, suggesting a gap in the integration of cloud problems with overall problem management.

Similarity score for Problem Management capability: 0.37

Maturity Score for Problem Management capability: 0.0

### Recommendations for Problem Management capability

the business is currently at level 1 maturity, with a well-structured incident management process based on itil guidelines, and a robust toolset for infrastructure monitoring, event management, and ticketing. the security operations center (soc) is event-driven, identifying threats and initiating remediation. compliance is monitored continuously via azure security center and azure sentinel, with efforts aligned with the csa framework, cis benchmarks, and specific standards through security maturity initiatives. however, there is limited governance for azure permissions and remote access monitoring, and no formal cloud governance structure. the business is also lacking in cloud-specific playbooks and standardized alerts for permission changes within azure subscriptions. to achieve level 2 maturity, the business needs to proactively identify all possible candidates for problem resolution upon completion of root cause analysis.  
  
- implement a formal cloud governance structure to enhance security compliance.  
- develop cloud-specific playbooks to standardize response procedures.  
- establish standardized alerts for permission changes within azure subscriptions.

### Implementation Road for Problem Management