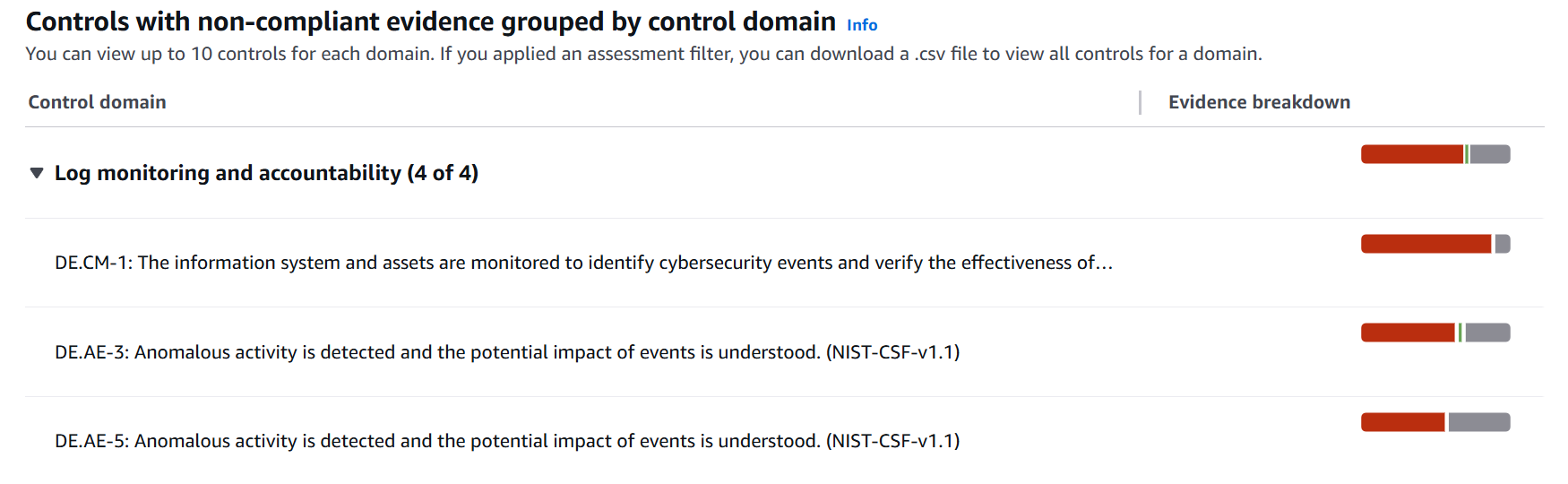
AWS Audit Manager Finding – Report

# 1. Before Screenshot

Screenshot showing non-compliant controls in the "Log monitoring and accountability" domain.



# 2. Vulnerability Overview

The 'Log monitoring and accountability' domain contains four non-compliant controls. These issues are related to log review and anomaly detection based on NIST-CSF-v1.1.

# 3. CVE ID (if applicable)

Not applicable (compliance control failure, not software vulnerability).

# 4. Severity

Moderate to High

# 5. CVSS Score

Not applicable

# 6. Risk Description

Without proper monitoring, cybersecurity events may go undetected, increasing the risk of breaches, data leaks, or delayed responses.

# 7. Analysis

- DE.CM-1: Log monitoring is not functioning effectively.  
- DE.AE-3 and DE.AE-5: Anomalous activity is not adequately detected or assessed.

# 8. Prioritization

High – foundational to detection and response capabilities.

# 9. Affected Resources

AWS CloudTrail, GuardDuty, CloudWatch, Security Hub.

# 10. Impact If Unresolved

- Undetected breaches  
- Delayed incident response  
- Compliance violations  
- Reduced threat visibility

# 11. Level of Effort to Fix

Low – mostly configuration of existing AWS services.

# 12. Resolution Action Taken

- Enabled CloudTrail logging in all regions  
- Activated GuardDuty  
- Verified CloudWatch alarms  
- Connected services to Security Hub

# 13. After Screenshot

[Insert updated screenshot here after resolution]

# 14. Recommendation

- Regularly audit monitoring tools  
- Use GuardDuty for automatic detection  
- Ensure CloudTrail and CloudWatch are enabled  
- Centralize alerts via Security Hub