Security Assessment Report

Comprehensive Security Control Assessment
Generated on 2025-07-30 03:12:18

Total Assessments	3
Generation Date	2025-07-30 03:12:18

Executive Summary

Executive Summary – Cybersecurity Audit Report

Overall Risk Assessment & Control Maturity Rating

The organization’s cybersecurity posture demonstrates moderate risk, reflecting a control maturity rating of **Developing**. While certain foundational controls are implemented, significant gaps exist in documented procedures, enforcement of least privilege access, and formal system sanitization processes.

Key Findings Summary

- • **Authentication & Authorization (PR.AA-02.01):** Medium Risk. The authentication mechanism is initiated but lacks demonstrable enforcement of authorization levels and user attribution to transactions. The system’s ability to track user roles during database access is not clearly evidenced in the log entries. Immediate action is required to implement audit logging for authorization levels and robust role validation. * **Access Control & Identity Management (EEE-035):** Critical Risk. A guest user account ('svc_guest_user') was accessed with insufficient privileges, presenting a significant vulnerability. Immediate implementation of multi-factor authentication for all accounts, coupled with strict adherence to the principle of least privilege, is critical. * **System Sanitization & Restoration (EEE-089):** Medium Risk. The current shutdown and cleanup procedures are preventative but do not satisfy the requirements for documented and executed system sanitization protocols. Formalized system sanitization and restoration processes, along with comprehensive documentation and record-keeping, are needed.

Critical Recommendations Requiring Immediate Attention

1. **Implement Multi-Factor Authentication (MFA) – Priority:** Implement MFA for all user accounts, including the ‘svc_guest_user’ account, to immediately mitigate the risk of unauthorized access. 2. **Enforce Least Privilege Access – Priority:** Conduct a thorough review and strictly enforce the principle of least privilege across all user accounts, limiting access to only the necessary resources. 3. **Formalize System Sanitization & Restoration – High Priority:** Develop and implement a documented system sanitization and restoration process, aligned with EEE-089, including procedures for secure data destruction, comprehensive record-keeping, and regular audits.

These recommendations represent immediate priorities to strengthen the organization's cybersecurity posture and reduce overall risk. Continued monitoring and ongoing audits are recommended to maintain a robust and resilient security environment.

Assessment Summary

Compliance Status Distribution

Status	Count	Percentage
PARTIALLY COMPLIANT	1	33.3%
NON-COMPLIANT	2	66.7%

Risk Level Distribution

Risk Level	Count	Percentage
MEDIUM	2	66.7%
CRITICAL	1	33.3%

Detailed Assessment Results

Assessment 1: Control Statement

PR.AA-02.01 Authentication of identity PR.AA-02.01: The organization authenticates identity, validates the authorization level of a user before granting access to its systems, limits the use of an account to a single individual, and attributes activities to the user in logs and transactions

Compliance Status	PARTIALLY COMPLIANT
Risk Level	MEDIUM

Log Evidence

Source File: auth.token

Relevant Log Entries:

```
2025-06-26 14:00:01,914 [INFO] auth.token - JWT authentication initialized for user: svc_report_user (role: reporter)

2025-06-26 14:00:02,032 [INFO] db.connector - Attempting connection to PostgreSQL (host=db.internal.net port=5432 dbname=corp_ledger)

2025-06-26 14:00:02,315 [INFO] db.connector - Connection established. User: svc_report_user, SSL: enabled, ConnID: b823fa1
```

Assessment Rationale

Why It Failed:

While JWT authentication is initialized and a connection to the database is established with the user 'svc_report_user' and the role 'reporter', the logs do not explicitly demonstrate the authorization level validation or user attribution to transactions, as stated in the control objective. The logs show authentication initiation and database connection, but not the enforcement of the authorization level or activity tracking.

Gap Analysis:

The evidence lacks details on how the 'reporter' role is validated before granting access to the database. It's unclear if the system is verifying the claimed role against a configured access control policy.

Impact:

A compromised 'svc_report_user' account with elevated privileges could lead to unauthorized data access or modification within the 'corp_ledger' database. The lack of explicit role validation presents a moderate risk.

Evidence Of Compliance:

JWT authentication is initialized and a connection is established. The log entry confirms user identification.

Effectiveness Assessment:

The JWT authentication is effectively initiated, but the system's ability to enforce and track user authorization is not clearly demonstrated in the provided log entries.

Improvement Recommendations

Mandatory Improvements:

- Implement audit logging to track the authorization level of users accessing the database.
- Review and update the JWT token schema to include a more robust representation of user roles and permissions.
- Configure the database access control to strictly adhere to the defined roles and access levels.

Enhancement Opportunities:

- Consider using a centralized identity management system for enhanced role-based access control.
- Implement multi-factor authentication for 'svc_report_user' to improve security.

Assessment 2: Control Statement

EEE-035: Access Control and Identity Management Documentation #authentication | #authorization | #credential_management | #identity_and_access_management | #multi_factor_authentication | #risk_management 072.166 PROTECT / Identity Management, Authentication, and Access Control / Authentication PR.AA-03.02 Access authorization PR.AA-03.02: Access authorization

Compliance Status	NON-COMPLIANT
Risk Level	CRITICAL

Log Evidence

Source File: db.auth

Relevant Log Entries:

```
2025-06-26 14:01:45,389 [ERROR] db.auth - Authentication failure for user: svc_guest_user from IP 10.18.25.44

2025-06-26 14:01:45,390 [CRITICAL] db.auth - Access denied to sensitive_table. Origin: Streamlit_app_01, Reason: insufficient privileges
```

Assessment Rationale

Why It Failed:

The log entry indicates an authentication failure for the user 'svc_guest_user' from IP address 10.18.25.44, resulting in access denied to the 'sensitive_table'. This directly reflects an insufficient privileges issue, contradicting the organization's need to strictly limit and closely manage privileged system access through multi-factor authentication.

Gap Analysis:

The absence of multi-factor authentication for the 'svc_guest_user' account and the resulting 'insufficient privileges' error demonstrates a critical gap in access control implementation, exposing a sensitive table to potential unauthorized access.

Impact:

Successful exploitation of this vulnerability could lead to data breaches, unauthorized modifications to sensitive data, and a significant disruption to the organization's operations. The use of a guest user account with overly permissive access rights poses a substantial security risk.

Evidence Of Compliance:

N/A - No evidence of compliance observed.

Effectiveness Assessment:

The authentication mechanism is failing to effectively restrict access, as demonstrated by the 'insufficient privileges' error.

Improvement Recommendations

Mandatory Improvements:

- Implement multi-factor authentication for all user accounts, including the 'svc_guest_user' account.
- Review and strictly enforce the principle of least privilege, ensuring that each user account has only the necessary permissions to perform their assigned tasks.
- Conduct a thorough audit of all user accounts and access rights, identifying and remediating any instances of overly permissive access.
- Establish clear and documented procedures for requesting and granting access to sensitive data.

Enhancement Opportunities:

- Consider leveraging identity governance and administration (IGA) solutions to automate access provisioning, deprovisioning, and ongoing access reviews.
- Implement continuous monitoring and alerting for authentication failures and unauthorized access attempts.
- Conduct regular penetration testing and vulnerability assessments to identify and address potential security weaknesses.

Assessment 3: Control Statement

EEE-089: System Sanitization and Restoration Documents - Procedures for the sanitization of systems and data to remove sensitive information securely before disposal or repurposing. - Restoration procedures detailing steps to return systems to operational status after an incident or maintenance. - Records of system sanitization and restoration activities, including dates, systems involved, and personnel responsible. - Training records for IT staff on proper sanitization techniques and restoration protocols. - Compliance reports or certifications demonstrating adherence to industry standards for data sanitization and system restoration

Compliance Status	NON-COMPLIANT
Risk Level	MEDIUM

Log Evidence

Source File: system.shutdown

Relevant Log Entries:

```
2025-06-26 14:05:32,778 [INFO] system.shutdown - Application gracefully disconnected from PostgreSQL (ConnID: b823fa1)

2025-06-26 14:05:32,779 [DEBUG] system.cleanup - Cleared memory cache, flushed log buffers, revoked temporary secrets
```

Assessment Rationale

Why It Failed:

The log entries indicate a graceful shutdown of an application and subsequent cleanup operations. However, there is no evidence of documented procedures for system sanitization or restoration (as mandated by EEE-089). The cleanup actions (clearing memory cache, flushing log buffers, revoking temporary secrets) are preventative measures but do not represent formal system sanitization procedures.

Gap Analysis:

The shutdown process lacks explicit documentation and control around the removal of sensitive data or the secure destruction of system components, directly contradicting the requirements of EEE-089.

Impact:

Failure to adhere to EEE-089 could lead to potential data breaches if systems are not properly sanitized prior to disposal or repurposing, creating a risk of unauthorized access to stored information. This could result in regulatory fines, reputational damage, and legal liabilities.

Evidence Of Compliance:

None - the logs confirm only shutdown and cleanup processes, not formal sanitization.

Effectiveness Assessment:

The cleanup actions are effective in maintaining system stability during shutdown, but they do not address the core requirement of documented and executed system sanitization protocols.

Improvement Recommendations

Mandatory Improvements:

- Implement and document a system sanitization and restoration process aligned with EEE-089.
- Establish clear procedures for data destruction (e.g., secure wiping of disks, physical destruction of media).
- Create and maintain records of all system sanitization and restoration activities, including dates, systems involved, personnel, and methods used.
- Conduct regular audits to verify compliance with sanitization procedures.

Enhancement Opportunities:

- Integrate the sanitization process into the change management workflow.
- Utilize automated tools for data sanitization to ensure consistency and accuracy.
