Comprehensive Audit Report

Executive Summary

This audit report consolidates findings from multiple audits conducted across various domains, including access control, transaction limit compliance, change management, and policy compliance. The purpose of this report is to provide a structured overview of the audit findings, highlight key risks, and recommend actionable steps to address identified issues.

Audit Background

The audits were conducted to ensure compliance with organizational policies, regulatory requirements, and best practices. The scope of the audits included: - **Access Control**: Review of user access levels against the authorized access matrix. - **Transaction Limit Compliance**: Analysis of transactions against authorized approval limits. - **Change Management**: Verification of audit trail records against change tickets based on the change management SLA. - **Policy Compliance**: Evaluation of transactions against organizational purchase policies.

Aggregated Statistics

- **Access Control**: 17 users with discrepancies, 4 users with no discrepancies.
- **Transaction Limit Compliance**: 5 transactions exceeded user approval limits, 9 transactions were compliant.
- **Change Management**: 14 audit trail records with potential change management violations, 5 records were compliant.
- **Policy Compliance**: 4 transactions with policy violations, 1 transaction was compliant.

Detailed Findings

Access Control Findings

Observation The following users have discrepancies between their actual access levels and the authorized access matrix:

- **USER001**: `system_b_access` should be `checker` but is `maker`.
- **USER002**: `system_b_access` should be `read-only` but is `maker`.
- **USER003**: `system_a_access` should be `read-only` but is `maker`.
- **USER005**: `system_b_access` should be `checker` but is `maker`.
- **USER006**: `system_c_access` should be `read-only` but is `maker`.
- **USER008**: `system_c_access` should be `checker` but is `read-only`.
- **USER009**: `system_a_access` should be `read-only` but is `checker`.
- **USER010**: `system_c_access` should be `checker` but is `maker`.
- **USER012**: `system_b_access` should be `checker` but is `maker`.
- **USER014**: `system_b_access` should be `read-only` but is `checker`.
- **USER016**: `system_b_access` should be `checker` but is `maker`.
- **USER017**: `system_a_access` should be `checker` but is `maker`.

- **USER021**: Unauthorized access to `system_a_access`, `system_b_access`, and `system_c_access`.
- **USER022**: Unauthorized access to `system_a_access`, `system_b_access`, and `system_c_access`.
- **USER023**: Unauthorized access to `system_a_access`, `system_b_access`, and `system_c_access`.
- **USER024**: Unauthorized access to `system_a_access`, `system_b_access`, and `system_c_access`.

Risk Rating

- **High**: Unauthorized access for users USER021, USER022, USER023, and USER024.
- **Medium**: Discrepancies in access levels for other users.

Risks

- Unauthorized access could lead to data breaches or misuse of sensitive information.
- Discrepancies in access levels could result in unauthorized actions or data manipulation.

Management Actions

1. **Immediate Revocation**: Unauthorized access for users USER021, USER022, USER023, and USER024 should be revoked immediately.
2. **Access Adjustment**: Adjust access levels for users with discrepancies to match the authorized access matrix.
3. **Periodic Reviews**: Conduct periodic access reviews to ensure compliance with the access matrix.

Transaction Limit Compliance Findings

Observation The following transactions were analyzed against authorized approval limits:

- **Transaction 0**: Exceeded approval limit for USER008.
- **Transaction 1**: Approved within the single approval limit of USER004.
- **Transaction 2**: Approved within the joint approval limit of USER001 and USER002.
- **Transaction 3**: Exceeded approval limit for USER009.
- **Transaction 4**: Approved within the joint approval limit of USER003 and USER004.
- **Transaction 5**: Approved within the single approval limit of USER007.
- **Transaction 6**: Approved within the joint approval limit of USER002 and USER003.
- **Transaction 7**: Exceeded approval limit for USER010.
- **Transaction 8**: Approved within the joint approval limit of USER001, USER002, and USER003.
- **Transaction 9**: Exceeded approval limit for USER005.
- **Transaction 10**: Approved within the joint approval limit of USER001 and USER004.
- **Transaction 11**: Approved within the single approval limit of USER008.
- **Transaction 12**: Approved within the joint approval limit of USER002 and USER003.

- **Transaction 13**: Approved within the single approval limit of USER006.
- **Transaction 14**: Exceeded the joint approval limit of USER001, USER002, and USER003.

Risk Rating

- **High**: Transactions exceeding user approval limits (Transaction 0, 3, 7, 9, 14).
- **Low**: Transactions within approved limits.

Risks

- Transactions exceeding approval limits could lead to financial losses or unauthorized expenditures.
- Non-compliance with approval limits could result in regulatory penalties.

Management Actions

1. **Immediate Review**: Transactions exceeding user approval limits (Transaction 0, 3, 7, 9, 14) should be reviewed and re-approved by authorized personnel.
2. **Limit Adjustments**: Consider adjusting approval limits for users who frequently exceed their limits (e.g., USER008, USER009, USER010, USER005).
3. **Periodic Reviews**: Conduct periodic reviews of transaction approvals to ensure compliance with authorized limits.

Change Management Findings

Observation The following audit trail records were analyzed against change tickets based on the change management SLA:

- **Audit Trail Record 0**: Potential change management violation by USER001.
- **Audit Trail Record 1**: Potential change management violation by USER004.
- **Audit Trail Record 2**: Compliant change by USER002 with change ticket CHG003.
- **Audit Trail Record 3**: Compliant change by USER007 with change ticket CHG004.
- **Audit Trail Record 4**: Compliant change by USER003 with change ticket CHG005.
- **Audit Trail Record 5**: Compliant change by USER005 with change ticket CHG006.
- **Audit Trail Record 6**: Potential change management violation by USER008.
- **Audit Trail Record 7**: Compliant change by USER006 with change ticket CHG008.
- **Audit Trail Record 8**: Potential change management violation by USER001.
- **Audit Trail Record 9**: Potential change management violation by USER004.
- **Audit Trail Record 10**: Unauthorized change by USER009 with change ticket CHG011.
- **Audit Trail Record 11**: Unauthorized change by USER002 with change ticket CHG012.
- **Audit Trail Record 12**: Unauthorized change by USER005 with change ticket CHG013.
- **Audit Trail Record 13**: Compliant change by USER003 with change ticket CHG014.
- **Audit Trail Record 14**: No related change ticket found.
- **Audit Trail Record 15**: No related change ticket found.
- **Audit Trail Record 16**: No related change ticket found.

- **Audit Trail Record 17**: No related change ticket found.
- **Audit Trail Record 18**: No related change ticket found.
- **Audit Trail Record 19**: No related change ticket found.

Risk Rating

- **High**: Unauthorized changes and potential change management violations.
- **Low**: Compliant changes.

Risks

- Unauthorized changes could lead to system instability or security vulnerabilities.
- Non-compliance with change management policies could result in regulatory penalties.

Management Actions

1. **Immediate Review**: Audit trail records with potential change management violations (Audit Trail Records 0, 1, 6, 8, 9, 10, 11, 12, 14, 15, 16, 17, 18, 19) should be reviewed and re-approved by authorized personnel.
2. **Process Improvement**: Consider enhancing the change management process to ensure all changes are properly documented and approved.
3. **Periodic Reviews**: Conduct periodic reviews of audit trail records to ensure compliance with change management policies.

Policy Compliance Findings

Observation The following transactions were analyzed against the organizational purchase policies:

- **Transaction T001**: Violation of Tax Compliance (Rule 6).
- **Transaction T002**: Violation of Vendor Restrictions (Rule 3) and Discounts (Rule 5).
- **Transaction T003**: Compliant with all policies.
- **Transaction T004**: Violation of Maximum Purchase Limit (Rule 1), Vendor Restrictions (Rule 3), Discounts (Rule 5), and Purchase Authorization (Rule 7).
- **Transaction T005**: Violation of Maximum Purchase Limit (Rule 1), Purchase Authorization (Rule 7), and Vendor Restrictions (Rule 3).

Risk Rating

- **High**: Transactions with multiple policy violations (T001, T002, T004, T005).
- **Low**: Compliant transaction (T003).

Risks

- Policy violations could lead to financial losses, regulatory penalties, or reputational damage.
- Non-compliance with purchase policies could result in unauthorized expenditures.

Management Actions

1. **Immediate Review**: Transactions T001, T002, T004, and T005 require immediate review and corrective action due to multiple policy violations.
2. **Process Improvement**: Enhance vendor approval processes and ensure all discounts above 15% are properly justified and approved.
3. **Training**: Conduct training sessions for staff to ensure compliance with purchase policies, especially regarding tax compliance and vendor restrictions.
4. **Periodic Audits**: Implement periodic audits to identify and address policy violations proactively.

Recommendations

1. **Access Control**:
   - Revoke unauthorized access immediately.
   - Adjust access levels to match the authorized access matrix.
   - Conduct periodic access reviews.
2. **Transaction Limit Compliance**:
   - Review and re-approve transactions exceeding user approval limits.
   - Consider adjusting approval limits for users who frequently exceed their limits.
   - Conduct periodic reviews of transaction approvals.
3. **Change Management**:
   - Review and re-approve audit trail records with potential change management violations.
   - Enhance the change management process to ensure all changes are properly documented and approved.
   - Conduct periodic reviews of audit trail records.
4. **Policy Compliance**:
   - Review and take corrective action on transactions with policy violations.
   - Enhance vendor approval processes and ensure proper justification for discounts.
   - Conduct training sessions for staff and implement periodic audits.

Conclusion

This report highlights discrepancies, unauthorized access, non-compliant transactions, and potential change management violations. Immediate action is required to address these issues and ensure future compliance with organizational policies, regulatory requirements, and best practices. “‘