INFO 7374 - Cybersecurity Audit and Compliance
Week 8 Assignment

Group Members:
Krisha Lakhani – 002334794
Nisarg Sheth - 002308269

I. Risks Identification

1. Fraudulent Payroll Processing

- Unauthorized employees or outside attackers could manipulate payroll transactions.
- Fraudulent payment to the employee could bring some financial misstatements.

2. Wrong Calculations in the Payroll

- Inaccuracies in tax deductions, overtime pay, and benefits calculations may mean either under-or overpayment.
- Punishment for breach of law in taxes and benefits and employee dissatisfaction are possible.

3. Late Payroll

- System failure, human error, or network failure delays the payroll.
- It would cause the employees not to receive salaries on time and would lead to legal and reputational issues.

4. Lack of Segregation of Duties

- Increased risk in fraud or unintended errors on the payroll, if one person is looking after both payroll processing and approval as well.
- There may be some unauthorised payment detection because of the absence of independent verification.

5. Data Security and Confidentiality Breach

- Payroll contains personal employee details like Social Security numbers and bank details.
- Identity theft, reputational harm, and lawsuits would follow after the data leaks.

II. Control Objectives

To mitigate the identified risks, PaySecure Inc. should implement the following control objectives:

1. Ensure Payroll Transactions are Authorized and Secure

- Only authorized personnel should have access to payroll processing systems.

INFO 7374 - Cybersecurity Audit and Compliance
Week 8 Assignment

Group Members:
Krisha Lakhani – 002334794
Nisarg Sheth - 002308269

- Access should be regularly reviewed and updated to prevent unauthorized usage.

2. **Ensure Accuracy in Payroll Calculations**

- The system should automatically validate tax deductions, overtime calculations, and benefits allocation.
- Periodic reconciliation should be conducted to verify payroll accuracy.

3. **Ensure Timely Payroll Processing and Compliance**

- Payroll should be processed according to a predefined schedule.
- Alerts and notifications should be provided to detect and address processing failures.

4. **Establish Proper Segregation of Duties**

- Different individuals should handle payroll data entry, approval, and disbursement.
- Access logs should be reviewed regularly to ensure compliance.

5. **Implement Robust Security Controls for Payroll Data**

- Sensitive payroll data should be encrypted at rest and in transit.
- Security audits should be conducted to identify and mitigate vulnerabilities.

III. Controls Design

To address each objective of control, the following controls should be designed:

1. **Access Control Mechanisms**

- Implement role-based access control (RBAC) to ensure that only authorized employees can access payroll systems.
- Use multi-factor authentication (MFA) to prevent unauthorized logins.
- Conduct quarterly access reviews to revoke unnecessary permissions.

2. **Automated Payroll Validation and Reconciliation**

- Integrate automated validation checks to flag anomalies in tax and benefits calculations.

INFO 7374 - Cybersecurity Audit and Compliance
Week 8 Assignment

Group Members:
Krisha Lakhani – 002334794
Nisarg Sheth - 002308269

- Conduct biweekly reconciliation of payroll records against accounting reports.
- Implement error-handling workflows for correction and reprocessing.

3. **Scheduled Payroll Processing with Monitoring**

- Establish a fixed payroll schedule with backup processing options.
- Set up automated alerts for delayed or failed payroll runs.
- Maintain a disaster recovery plan for payroll continuity.

4. **Dual Authorization for Payroll Approval**

- Require two independent approvers for payroll disbursement.
- Implement system logging to track and audit approval activities.
- Introduce real-time alerts for unauthorized payroll modifications.

5. **Data Encryption and Security Audits**

- Use AES-256 encryption for payroll data storage.
- Conduct annual penetration testing to detect security vulnerabilities.
- Establish employee security awareness training to prevent phishing attacks.

IV. Testing Methods

1. **Access Control Testing**

- **Review user access logs** to verify that only authorized personnel can process payroll.
- **Test multi-factor authentication** by attempting unauthorized access scenarios.
- **Check access review records** for timely permission updates.

2. **Payroll Calculation Accuracy Testing**

- **Review a sample of payroll transactions** to confirm correct tax and benefits calculations.
- **Verify compliance with federal and state tax regulations** using official tax rates.
- **Test system alerts for payroll discrepancies** by inputting incorrect data.

3. **Timeliness of Payroll Processing**

INFO 7374 - Cybersecurity Audit and Compliance
Week 8 Assignment

Group Members:
Krisha Lakhani – 002334794
Nisarg Sheth - 002308269

- **Examine payroll processing schedules and logs** to ensure adherence to deadlines.
- **Simulate a system failure** to verify the effectiveness of backup processing.
- **Check notification systems** to ensure alerts trigger upon payroll delays.

4. **Segregation of Duties Testing**

- **Review system access rights** to confirm that payroll processing and approval are handled separately.
- **Analyze approval logs** to verify independent verification of payroll transactions.
- **Attempt unauthorized payroll changes** to check if system restrictions work effectively.

5. **Data Security Testing**

- **Perform penetration testing** to identify potential vulnerabilities.
- **Review encryption policies** to ensure compliance with data protection standards.
- **Audit security awareness training records** to confirm employee participation.

V. Example Audit Findings

Control That Passed: Multi-Factor Authentication

- Observation: Payroll system logins require MFA.
- Audit Testing: Unauthorized access attempts were blocked.
- Conclusion: Effective in preventing unauthorized access.
- Recommendation: Continue quarterly security reviews.

Control That Failed: Segregation of Duties

- Observation: One employee had both payroll processing and approval access.
- Audit Testing: Logs showed self-approved payroll transactions.
- Conclusion: Increases fraud risk.
- Recommendation: Implement dual authorization and system alerts.