# Table 1: Payroll Fraud

1. What are the different types of payroll fraud?
   1. Employees submitting fraudulent timesheets for their work-times. This can result from over-reporting overtime and under-reporting vacation/sick leave. Additionally, employees have attempted to edit their timesheets after before being sent to payroll.
   2. Employees have attempted to create fake personnel with the idea of pocketing their paychecks.
2. What is the probability of payroll fraud (in terms of high, medium, low)? What is the potential impact of payroll fraud threats (in terms of high, medium, low)? Explain. Refer to [2].
   1. Fraudulent work times.
      1. Probability: Medium. While there are measures in place to protect against submitting erroneous work times, all it takes is a supervisor to check-off on the times.
      2. Impact: Low. Some revenue may be lost, but it shouldn’t be an extremely large amount (at one time, at least).
   2. Fraudulent gain of benefits.
      1. Probability: Medium. Similar to 2.1.1.
      2. Impact: High. It would be possible for employees to retire early, which would have an impact on ongoing revenue.
   3. Creating fake users.
      1. Probability: Low. Only a sysadmin can create new users.
      2. Impact: High. If it did happen, HGA would basically be paying a non-existent employee (until the error was found and corrected).
3. According to the Risk-Level Matrix in [2], determine the risk scale of payroll fraud threats.
   1. Fraudulent work times (Low Risk).
      1. 0.5 (probability) X 10 (impact) = 5
   2. Fraudulent gain of benefits (Medium Risk).
      1. 0.5 (probability) X 100 (impact) = 50
   3. Creating fake users (Low Risk).
      1. 0.1 (probability) X 100 (impact) = 10
4. What are the control measures currently in use to protect against payroll fraud?
   1. Only sysadmins can create accounts.
   2. Only employees and contractors have access to HGA systems.
   3. New users are presented with a copy of HGA’s security policies and procedures; new employees must attend a security awareness training session.
   4. Authorized users are assigned secret usernames and passwords (which are not to be shared). Failure to follow the security policies and procedures results in disciplinary action.
   5. Data must be entered via an interface (not directly).
   6. Sensitive information is only available based on job-need.
   7. Government-based and HGA-based security policies are used to protect the time and attendance application (payroll).
   8. The time and attendance application performs security checks by using the LAN server’s access control and identification and authentication (I&A) mechanisms. The application compares the data with an employee database. After fixing any errors, the application formats the time and attendance data into a report, which specifies anomalies.
   9. Department supervisors are responsible for reviewing the correctness of the timesheets of the employees under their supervision. If they find irregularities, they report their findings to the Payroll Office.
   10. Only users with access to Time and Attendance Supervisory functions may approve and/or submit time and attendance data. Supervisors cannot approve their own time and attendance data.
   11. Only the sysadmin can grant access control privileges. The system tries to identify bogus data.
   12. Data entry can only be performed on specific computers on the LAN, during normal working hours.
   13. Access controls protect against unauthorized data entry.
   14. The time and attendance application utilities a client/server architecture.
5. What are the vulnerabilities related to payroll fraud found by the risk assessment team?
   1. Falsified Time Sheets (Low risk; acceptable risk)
   2. Unauthorized Access (High risk; unacceptable risk)
   3. Bogus Time and Attendance Applications (Low risk; acceptable risk, with one exception)
   4. Unauthorized Modification of Time and Attendance Data (Medium risk; unacceptable risk if a practical solution can be found)
6. What’s the recommendation by the risk assessment team?
   1. Falsified Timesheets. Timesheets should continue to be reviewed and approved by a supervisor. Supervisors are not permitted to approve their own timesheets. Since clerks and supervisors work together when submitting data to the mainframe, the likelihood of data-tampering is reduced.
   2. Unauthorized Access. Implement a strong authentication system based on smart tokens to generate one-time passwords. One-time passwords eliminate the possibility that they can be used by someone for subsequent sessions.
   3. Bogus Time and Attendance Applications. Fix security-related bugs as they pertain to the server’s operating system and access controls. Ensure the server’s access controls are configured properly.
   4. Unauthorized Modification of Time and Attendance Data. Various safeguards are needed. Ensure all temporarily stored data is secure through physical security and access controls. Modify network topology, harden access to switches, or input data directly into the mainframe. Limit access to the mainframe. Alternatively, employ digital signatures based on public key infrastructure.
7. What are the final decisions made by HGA management? Justify their decisions based on cost benefit analysis.
   1. The risk of falsified timesheets is acceptable. No changes were made related to the risk of falsifying timesheets.
   2. The risk of unauthorized access is unacceptable. The Computer Operations Group (COG) was directed to investigate the costs and procedures associated with using one-time passwords for Time and Attendance Clerks and supervisor sessions on the server. Users performing less sensitive tasks will continue to use password-based authentication.
   3. The risk of bogus time and attendance applications are acceptable, with one exception. The COG was directed to monitor the server’s access control configuration, and their responsiveness to vendor security reports and bug fixes.
   4. The risk of unauthorized modification of time and attendance data is unacceptable if a practical solution can be found. Management decided that digitally signed times and attendance information was practical and cost-efficient. The Computer Operations Group was directed to implement the solution.

# Table 2: Payroll Errors

1. What are the different types of payroll errors?
   1. Errors in entry of time and attendance data
   2. Failure to enter information describing new employees, terminations, and transfers in a timely manner
   3. Accidental corruption or loss of time and attendance data
   4. Errors in integrity coordination and processing of personnel transfers
2. What is the probability of payroll errors (in terms of high, medium, low)? What is the potential impact of payroll errors (in terms of high, medium, low)? Explain. Refer to [2].
   1. Errors in entry of time and attendance data
      1. Probability: Low
         1. Time and attendance data are entered twice; if the two entries match, they are considered correct
      2. Potential Impact: Low
         1. Could cause employee’s last paycheck for the year to be less due to repayment of erroneous overpayment of time record.
   2. Failure to enter information describing new employees, terminations, and transfers in a timely manner
      1. Probability: Medium
         1. Failure to notify the proper data entry agents upon hiring, terminating, or transferring new personnel when the event occurs
      2. Potential Impact: Medium
         1. Terminated employees would still have access to business systems until they have been removed from the system
         2. New and transferred employees do not have access to required systems when they begin employment
   3. Accidental Corruption or loss of time and attendance data
      1. Probability: Low
         1. Data storage is redundant and backed up nightly to prevent this from occurring.
      2. Potential Impact: Low
         1. Time, attendance, and payroll are temporarily calculated based on information from prior pay periods.
   4. Errors in integrity coordination and processing of personnel transfers
      1. Probability: Medium
         1. Inefficient incentives to managers to ensure timely processing of transfers
      2. Potential Impact: Low
         1. Transferred employees would not have access to relevant systems until transfer was processed successfully
3. According to the Risk-Level Matrix in [2], determine the risk scale of payroll errors.
   1. Errors in entry of time and attendance data (Medium Risk)
      1. 0.1 (Probability) X 10 (Impact) = 1
   2. Failure to enter information describing new employees, terminations, and transfers in a timely manner (Medium Risk)
      1. 0.5 (Probability) X 50 (Impact) = 25
   3. Accidental corruption or loss of time and attendance data (Low Risk)
      1. 0.1 (Probability) X 10 (Impact) = 1
   4. Errors in integrity coordination and processing of personnel transfers (Medium Risk)
      1. 0.5 (Probability) X 10 (Impact) = 5
4. What are the control measures currently in use to protect against payroll errors?
   1. Time and Attendance clerks enter each time sheet into the time and attendance application twice.
   2. A supervisor must review the reports for accuracy and are approved by running another server program to check the validity of the data.
   3. Manager of the Payroll Office is responsible for establishing and maintaining controls to ensure that the amounts of pay, leave, and other benefits reported on pay stubs and in permanent records are accurate and consistent
   4. Similar mechanisms for protecting against fraudulent modification are used to protect against accidental corruption - Access-control features of the server and mainframe systems
   5. Nightly backups of the server disks protect against data loss
   6. Copies of all time and attendance data are kept on the server for one year then archived and kept for 3 years
   7. Integrity of data maintained by digital signatures
   8. WAN protocols protect against data loss during transmission from server to mainframe
   9. Payroll application includes an application that runs 24 hours before paychecks and pay stubs are printed and prints a report for missing time and attendance data
   10. If time and attendance data is not received, pay, leave, and other benefits are calculated based on estimated information from previous pay periods
5. What are the vulnerabilities related to payroll error found by the risk assessment team?
   1. Late submission of personnel paperwork
   2. Managers are not providing sufficient incentives for compliance
   3. Significant amounts of data are stored on personal PCs instead of on the servers where the information is backed up automatically
6. What’s the recommendation by the risk assessment team?
   1. Need to establish incentives and penalties for compliance with payroll safeguards
   2. Director of Personnel must conduct quarterly compliance audits and report the findings
   3. Digital signature plan for fraud protection could also be used to provide protection against errors due to accidental corruption
   4. Automated program on the LAN server that will send quarterly reminders to all PC users to remind them to backup their hard disks
   5. Regular backup services for 5 percent of PCs based on the information stored on them
7. What are the final decisions made by HGA management? Justify their decisions based on cost benefit analysis.
   1. The risk of errors in entry of time and attendance data is acceptable. No changes were made to the entry of time and attendance data.
   2. The risk of failure to enter information describing new employees, terminations, and transfers in a timely manner is unacceptable. The Director of Personnel is tasked to conduct quarterly compliance audits to ensure data is entered in a timely manner.
   3. The risk of accidental corruption or loss of time and attendance data is acceptable. The same digital signature process used to prevent payroll fraud is to be used to protect against accidental corruption of data. The Mainframe service contingency plan was assessed and a request from HGA to the mainframe company to resolve the issues has been made.
   4. The risk of errors in integrity coordination and processing of personnel transfers is unacceptable. Compliance incentives and punishments were instituted to prevent future breakdowns of untimely data input.

# Table 5: Network Threats

1. What are the different types of network threats? Give a scenario where HGA had experienced a network related attack.
   1. Unauthorized disclosure or modification of information. Attempted have been made from the outside to gain access to HGA’s systems. Those that succeeded did so by learning/guessing account passwords. During those attempts, attackers deleted/corrupted a large amount of data (that was later restored using backups). Logs were not being audited.
   2. Unauthorized use of services and assets. By means of an e-mail utility bug, an attacker was able to gain sysadmin privileges. While no evidence of malicious conduct was found from the breach, the attack was not discovered until two days later.
   3. Unauthorized denial of services. It’s possible that a disgruntled employee/outsider may seek to disrupt time-critical processing (such as payroll). Such attempts may prevent time and attendance data from being processed/transferred to the mainframe before payroll deadline.
2. What is the probability of network threats (in terms of high, medium, low)? What is the potential impact of network threats (in terms of high, medium, low)? Explain. Refer to [2].
   1. Unauthorized disclosure or modification of information.
      1. Probability: Low. In the past, the only occurrences were through guessing/engineering passwords.
      2. Impact: Low/Medium. Data has been damaged/corrupted in past attacks. While it’s difficult to gauge exactly what impact data corruption may cause, back-ups are in place if such an event happens.
   2. Unauthorized use of services and assets.
      1. Probability: Low. It’s fairly unlikely that someone can gain elevated privileges without the sysadmin’s knowledge.
      2. Impact: High. However, if a malicious user did gain elevated privileges, it could potentially be devastating to HGA.
   3. Unauthorized denial of services.
      1. Probability: Low/Medium. While HGA hasn’t suffered an external attack to date, the possible of an attack is ever-present.
      2. Impact: High. An external DOS could impede the day-to-day operation of HGA.
3. According to the Risk-Level Matrix in [2], determine the risk scale of network threats.
   1. Unauthorized disclosure or modification of information (Low Risk).
      1. 0.1 (probability) X 30 (impact) = 3
   2. Unauthorized use of services and assets (Low Risk).
      1. 0.1 (probability) X 100 (impact) = 10
   3. Unauthorized denial of services (Low Risk).
      1. 0.1 (probability) X 100 (impact) = 10
4. What are the control measures currently in use to protect against network threats?
   1. External network interactions only travel through two interfaces that filter out unauthorized traffic.
      1. Only e-mail and data transfers from the server to mainframe are allowed by specific applications.
   2. Dial-in access via public-switched networks is restricted.
   3. Access controls are provided by the server’s operating system have been configured for dial-in sessions; only the e-mail utility can be executed.
   4. The server’s access controls have been configured so that the WAN interface device is only accessible to programs that posses a special access-control privilege.
      1. Only the sysadmin can assign privileges to server programs and certain special-purposes applications.
5. What are the network-related vulnerabilities found by the risk assessment team?
   1. Lack of assurance associated with the server’s access controls.
   2. The email utility allows users to attach a copy of any accessible file in an outgoing message.
   3. Copies can be mailed to any host on the Internet
   4. WAN service provider may rely on microwave stations or satellites as relay points that may expose information to eavesdropping.
6. What’s the recommendation by the risk assessment team?
   1. A stronger I&A for dial-in access should be used or, use of a restricted version of the mail utility be provided for dial-in, to prevent a user from including files in outgoing mail messages;
   2. Replace current modem pool with encrypting modems, and provide each dial-in user with an encrypting modem
   3. Work with the mainframe agency to on similar encryption capability for server-to-mainframe communications over the WAN
7. What are the final decisions made by HGA management? Justify their decisions based on cost benefit analysis.
   1. HGA’s policy on handling time and attendance information was clarified, strengthened, and elaborated. The hope is that implementing this new policy would help reduce risks related to the Internet and dial-in eavesdropping.
      1. A revised policy was issued informing employees that it was their responsibility to ensure they do not transmit disclosure-sensitive info outside HGA facilities (whether they are on-site or dialing-in).