ACFE
Association of Certified Fraud Examiners

Fraud Risk Assessment

Module # 3 – Physical Controls to Deter Employee Theft and Fraud

The physical controls assessment questions are designed to assess the probability of a fraudulent event occurring within the organization based on:

- Physical controls in place to control access to accounting records and information
- Physical controls in place to protect the assets of the organization

Questionnaire Key

1. Does the organization conduct pre-employment background checks to identify previous dishonest or unethical behavior?

Before offering employment to an applicant, a company should conduct a pre-employment background check.

2. Are there policies and procedures that address dishonest or unethical behavior?

The company should document and implement policies and procedures that describe (1) unethical conduct, (2) punishment for engaging in unethical conduct, and (3) how to report unethical conduct.

3. Does management support the ethics and anti-fraud policies?

Senior management sets the tone for ethical conduct throughout the organization. The tone should signal that fraud will not be tolerated.

4. Does the organization educate employees about the importance of ethics and anti-fraud programs?

All employees should receive training on the ethics and anti-fraud policies of the company. The employees should sign an acknowledgment that they have received the training and understand the policies.

5. Does the organization provide an anonymous way to report suspected violations of the ethics and anti-fraud policies?

Organizations should provide a system for anonymous reporting of suspected violations of the ethics and anti-fraud policies.

6. Does the organization restrict access to areas containing sensitive documents (such as invoices, receipts, journals, ledgers, and checks) and maintain a system for providing an audit trail of access?

Access to areas containing sensitive documents should be restricted to those individuals who need the information to carry out their jobs. Also, an audit trail of access should be maintained.

7. Does the organization restrict access to computer systems with sensitive documents (such as accounting software, inventory, and payroll) and create a system to provide an audit trail of access?

Access to computer systems should be restricted to those individuals who need the information to carry out their jobs. Also, an audit trail of access should be maintained.

8. Does the organization restrict access to areas with high value assets, such as shipping, receiving, storerooms, and cash?

Organizations should restrict access to areas with high value assets and should maintain a log of persons accessing such areas.

9. Does the organization use CCTV and recording equipment to monitor entries, exits, areas with sensitive or high value assets, and sales areas?

Entries, exits, areas with sensitive or high value assets, and sales areas can be monitored using CCTV and recording equipment.

10. Does the organization conduct random, unannounced audits of inventory, cash, expense, purchasing, billing, and other accounts by internal or external auditors?

Random, unannounced audits help prevent fraud perpetrators from having time to alter, destroy, and misplace records and other evidence of their offenses.

11. Does the organization use professional loss prevention or security personnel to monitor physical controls?

Professional loss prevention or security personnel can be used to monitor physical controls.

12. Does the organization promptly investigate incidents of suspected or reported fraud?

Promptly investigating incidents of suspected or reported fraud can minimize losses.

Physical Controls to Deter Employee Theft and Fraud			
	Yes	**No**	**N/A**
Does the organization conduct pre-employment background checks to identify previous dishonest or unethical behavior? **Comments:**	☐	☐	☐
Are there policies and procedures that address dishonest or unethical behavior? **Comments:**	☐	☐	☐
Does management support the ethics and anti-fraud policies? **Comments:**	☐	☐	☐
Does the organization educate employees about the importance of ethics and anti-fraud programs? **Comments:**	☐	☐	☐
Does the organization provide an anonymous way to report suspected violations of the ethics and anti-fraud policies? **Comments:**	☐	☐	☐

Physical Controls to Deter Employee Theft and Fraud

	Yes	No	N/A
Does the organization restrict access to areas containing sensitive documents (such as invoices, receipts, journals, ledgers, and checks) and maintain a system for providing an audit trail of access? **Comments:**	☐	☐	☐
Does the organization restrict access to computer systems with sensitive documents (such as accounting software, inventory, and payroll) and create a system to provide an audit trail of access? **Comments:**	☐	☐	☐
Does the organization restrict access to areas with high value assets, such as shipping, receiving, storerooms, and cash? **Comments:**	☐	☐	☐
Does the organization use CCTV and recording equipment to monitor entries, exits, areas with sensitive or high value assets, and sales areas? **Comments:**	☐	☐	☐
Does the organization conduct random, unannounced audits of inventory, cash, expense, purchasing, billing, and other accounts by internal or external auditors? **Comments:**	☐	☐	☐

ACFE
Association of Certified Fraud Examiners

Fraud Risk Assessment

Physical Controls to Deter Employee Theft and Fraud			
	Yes	No	N/A
Does the organization use professional loss prevention or security personnel to monitor physical controls? **Comments:**	☐	☐	☐
Does the organization promptly investigate incidents of suspected or reported fraud? **Comments:**	☐	☐	☐