DAAS Fraud Awareness and Prevention Guidelines

Definition of Fraud

Fraud is defined as a misrepresentation or concealment of material facts with intent to deceive and obtain unauthorized benefit. It involves deliberate and deceptive acts, such as forgery of any document, with intent to obtain benefits, such as money, property, or services. Misrepresentation could be false presentation, concealment, or non-disclosure but does not include expressing an opinion.

If there is no deception or misrepresentation, it may be a case of abuse or misuse of assets but not fraud. For example, untruthful statement by a staff member for obtaining allowances or benefits purely by mistake, without any intention to deceive the Organization, is not a fraud but constitutes grounds for severe disciplinary measures under the Human Resource Regulations and Rules of DAAS.

Types of Frauds

Most of the frauds can be classified into three major categories: Corruption, Fraudulent Statements and Asset Misappropriation. These can be further broken down into various sub-categories.

Corruption is the act of doing something with the intention of obtaining some advantage inconsistent with official duty. Corruption often occurs when fraudsters wrongfully use their influence in a transaction to benefit themselves or another party to whom the benefit is not due through:

a) Bribery: payment, receipt, or solicitation of a private favor for an official action.

b) Illegal gratuities: It is similar to bribery but of a lesser magnitude.

c) Economic extortion: the act of obtaining or compelling financial gain by illegal means.

Fraudulent statements generally involve falsification of financial statements, like overstating income, understating expenses and liabilities resulting in gain of personal benefit or loss of property or assets of the Organization.

These statements could be:

a) Financial

b) Non-financial

Asset misappropriations involve the outright theft of the assets of the Organization and covering up with falsified documents or through other schemes. Some examples are:

a) Cash theft

b) Inventory theft

c) Embezzlement

d) Billing for nonexistent material or work

e) Skimming (removing funds prior to recording)

f) Payroll for nonexistent employees

g) Expense re-imbursement schemes

h) Misrepresentation, forgery, alteration of official claim, certificates, documents, record, or accounts, including forgery of cheques, receipts, and other financial documents

i) Intentionally mishandling of contract obligations and relations with third parties, resulting in loss of property or assets of the Organization or gain of personal benefit.

The types of fraud listed above are not exhaustive as any similar or related inappropriate conduct or any act encouraging, concealing, conspiring, or colluding in any of the above actions are also considered as fraud.

Risk Assessment

DAAS offices are located in many countries with different cultures and working environments with varying types of vulnerabilities to fraud. Therefore, the chances of a particular type of fraud that might occur could be different in different locations. At some locations, the risk of misappropriation of assets could be higher and at others the risk of fraud through corruption may be more likely to occur.

It is important for managers to evaluate and assess the risk of potential fraud in relation to the country in which the manager is located.

Risk Impact and Prioritization

Managers should be aware that when assessing the impact of various risks, they should keep two aspects of risks in mind:

a) Impact – how much damage (maximum/minimum) can occur?

b) Probability – what is the likelihood of it occurring?

The identified risks should then be prioritized in terms of their possible impact on the operations and those with the likelihood of high impact should be addressed first.

Prevention Measures

In general, managers should be aware that there are various circumstances that could contribute towards fraudulent behavior, such as:

a) The perpetrator has sufficient knowledge to commit a fraud and has access to assets.

b) Perceived lax attitude at DAAS Offices in terms of compliance with rules, regulations, policies, or procedures of the Organization.

A preventive strategy to mitigate some of the above-mentioned circumstances would be to provide only appropriate access commensurate with delegated authority and demonstrated commitment towards adherence to rules and regulations by senior staff.

Risk assessment would help in determining probabilities of a specific fraud at a particular location, appropriate measures should be taken to mitigate and prevent such specific situations. For example:

i) If at one location it is found that the risk of misappropriation of inventory is the highest:

a) Level of inventory at hand should be minimized.

b) Inventory should be safeguarded in premises having two locks and each key to be held by a different person.

c) Adequate segregation of duties should be maintained - the person having the access, the person who is recording and the person who is authorizing the use are different.

d) Frequent verifications (physical inventory cross checked with the records) should be performed.

ii) At another location, if procurement is considered a high-risk area, then some of the measures that should be taken are:

a) In order to avoid potential collusion between the DAAS entity placing an order and the supplier, internal DAAS processes to establish the requirement of goods or services should be well defined / documented and coordinated. This will also prevent any persuasion from the suppliers.

b) A clear and unambiguous contract preventing delivery of sub-standard products

POLICY REVISION HISTORY:

Policy #	Date Reviewed (YYYY MM DD)	Summary of Changes	Changed by Whom
201909140001	2019/09/14	New Policy	Walter Phillips