FRAUD RISK ASSESSMENT

All agencies are subject to fraud risks and need to complete a fraud risk assessment for their agency at least every biennium. A detailed fraud assessment needs to be performed by division and/or function. Functions and services that need to be included in the assessment are Finance and Accounting, Human Resources Management (payroll), Purchasing and Contracting, and Information Technology. As a part of the assessment, agencies need to look at control environment and information technology as both have a significant effect on fraud risk for most functions.

CONTROL ENVIRONMENT AND INFORMATION TECHNOLOGY

The control environment includes management's attitude as to the importance of the establishment and maintenance of a strong internal control system; having organizational units clearly defined to perform the necessary functions of the agency; having qualified and properly trained personnel; delegation of authority or limitation of authority to provide assurances that responsibilities are effectively performed; having policies and procedures including a code of ethical conduct available to employees; and requiring background checks on personnel that have access to personal information, positions of accounting and financial oversight, and positions of trust.

PeopleSoft payroll and financial systems play a critical role in state agencies' financial operations. In addition, agencies have personal computers and many agencies have other computer systems that are essential. Some computer systems have controls built in which are a benefit to internal controls, such as segregation of accounts payable input and approval duties. However, agencies need to ensure that their users have the appropriate access and need to ensure that there is no unauthorized access.

A control environment assessment form and computer security assessment form that agencies should complete as part of their fraud risk assessment can be found at www.nd.gov/fiscal/forms. Any no answers to the questions on these forms would signal a weakness in the agencies controls to prevent fraud activity.

Agencies that have their own computer systems will need to do additional assessments of their systems.

FRAUD RISK ASSESSMENT

The following information was taken from the AICPA's "Managing the Business Risk of Fraud: A Practical Guide." Some changes were made to adapt this document to state agency business. This guide can be found at http://www.aicpa.org/forthepublic/auditcommitteeeffectiveness/auditcommitteebrief/downloadabledocuments/managing_the_business_risk_of_fraud.pdf.

A fraud risk assessment should be performed periodically to identify potential schemes and events that need to be mitigated. This document provides guidance for conducting a fraud risk assessment; however, agencies will need to make modifications to meet their individual needs and complexities.

An effective fraud risk management assessment should identify where fraud may occur and who the perpetrators might be. Therefore, control activities should always consider both the fraud scheme and the individuals within and outside the organization who could be the perpetrators of each scheme. If the scheme is collusive, [1]preventive controls should be augmented by detective controls, as collusion negates the control effectiveness of segregation of duties.

Fraud, by definition, entails intentional misconduct, designed to evade detection. As such, the fraud risk assessment should anticipate the behavior of a potential fraud perpetrator. It is important to design fraud detection procedures that a perpetrator may not expect, requires a skeptical mindset and involves asking questions such as:

- How might a fraud perpetrator exploit weaknesses in the system of controls?
- How could a perpetrator override or circumvent controls?
- What could a perpetrator do to conceal the fraud?

With this in mind, a fraud risk assessment generally includes three key elements:

- *Identify inherent fraud risk* — [2]Gather information to obtain the population of fraud risks that could apply to the organization. Included in this process is the explicit consideration of all types of fraud schemes and scenarios; incentives, pressures, and opportunities to commit fraud; and IT fraud risks specific to the organization.
- *Assess likelihood and significance of inherent fraud risk* — Assess the relative likelihood and potential significance of identified fraud risks based on historical information, known fraud schemes, and interviews with staff, including business process owners.
- *Respond to reasonably likely and significant inherent and residual fraud risks* — Decide what the response should be to address the identified risks and perform a cost-benefit analysis of fraud risks over which the organization wants to implement controls or specific fraud detection procedures.

Agencies should apply a framework to document their fraud risk assessment. The framework on the following page illustrates how the elements of fraud risk identification, assessment, and response are applied in a rational, structured approach. This example begins with a list of identified fraud risks and schemes, which are then assessed for relative likelihood and significance of occurrence. Next, the risks and schemes are mapped to the people and/or departments that may be impacted and to relevant controls, which are evaluated for design effectiveness and tested to validate operating effectiveness. Lastly, residual risks are identified, and a fraud risk response is developed.

---

1 A collusive scheme is one performed by two or more individuals working together.

2 The initial assessment of fraud risk should consider the inherent risk of particular frauds occurring in the absence of internal controls. After all relevant fraud risks have been identified; internal controls are mapped to the identified risks. Fraud risks that remain unaddressed by appropriate controls comprise the population of residual fraud risks.

Identified Fraud risks and Schemes	Likelihood	Significance	People and/or Department	Existing Anti-Fraud Controls	Controls Effectiveness Assessment	Residual Risks	Fraud Risk Response
Financial Reporting: Revenue Recognition -Recording receipts in Incorrect periods Expenditure Recognition -Holding bills -Improper coding of bills Misclassification of Balances Reporting more receivables and less cash to conceal misappropriation of receivable payments Misappropriation of Assets: Cash/Checks -At time of receipt Accounts Payable / Expenditures -Unauthorized Pcard transactions -Fictitious vendors -Inflated invoices from vendors Payroll -Unauthorized payroll adjustments Capital Assets/Inventory -Theft by employees -Theft by others Corruption: Kickbacks/Conflict of Interest -Contracts award improperly							

A fraud risk assessment example can be found in Appendix A. Note that this is a sample and does not encompass all possible fraudulent schemes and risks. This example is only to assist agencies to begin their assessment. Each agency needs to determine what its possible fraud risks are. A blank form of this framework above can be found at www.nd.gov/fiscal/forms.

In addition to the fraud risk assessment example, there is a listing of possible types of fraud an agency may encounter in Appendix B. For some of the risks listed, we have also given a brief explanation of the reason why the fraud may be committed. Again, this listing is not all-inclusive. It's just to help agencies get started with their own risk assessment.

Risk Assessment Team

A good risk assessment requires input from various sources. Ideally, management should identify a risk assessment team, even if the team would only be 2 individuals, to conduct the risk assessment. Individuals from throughout the organization with different knowledge, skills, and perspectives should be involved in the risk assessment. Such members of the risk assessment teams should include personnel such as:

- Accounting/finance personnel, who are familiar with the financial reporting process and internal controls.
- Nonfinancial business unit and operations personnel, to leverage their knowledge of day-to-day operations.
- Legal and compliance personnel, if agency has.
- Internal audit personnel, for agencies with internal auditors.

Management should participate in the assessment, as they are ultimately accountable for the effectiveness of the agency's fraud risk management efforts.

Fraud Risk Identification

The risk assessment team should go through a brainstorming activity to identify the agency's fraud risks. Brainstorming enables discussions of the incentives, pressures, and opportunities to commit fraud; risks of management override of controls; and the population of fraud risks relevant to the agency. Other risks, such as regulatory and legal misconduct risk, as well as the impact of IT on fraud risks also should be considered in the fraud risk identification process.

The agency's fraud risk identification information should be shared with the board or audit committee, if any, and comments should be solicited. If no board or audit committee, the information should be shared with senior management.

Incentives, Pressures, and Opportunities

Motives for committing fraud are numerous and diverse. The fraud risk identification process should include an assessment of the incentives, pressures, and opportunities to commit fraud.

Opportunities to commit fraud exist throughout organizations. These opportunities are greatest in areas with weak internal controls and a lack of segregation of duties. However, some frauds, especially those committed

by management, may be difficult to detect because management can often override the controls. If possible, such opportunities are why appropriate monitoring of senior management by a strong board and audit committee, supported by internal auditing, is critical to fraud risk management.

Risk of Management's Override of Controls

As part of the risk identification process, it is important to consider the potential for management override of controls established to prevent or detect fraud. Personnel within the agency generally know the controls and standard operating procedures that are in place to prevent fraud. It is reasonable to assume that individuals who are intent on committing fraud will use their knowledge of the agency's controls to do it in a manner that will conceal their actions. For example, a manager who has the authority to set up new vendors and approve invoices may create and approve a fictitious vendor and then submit invoices for payment. Hence, it is also important to keep the risk of management's override of controls in mind when evaluating the effectiveness of controls; an anti-fraud control is not effective if it can be overridden easily.

Population of Fraud Risks

The fraud risk identification process requires an understanding of fraud risks and the subset of risks specific to the agency. This involves understanding the agency's business processes and gathering information about potential fraud from internal sources by interviewing personnel and brainstorming with them and performing analytical procedures.

There are three general categories of fraud risk: fraudulent statements, misappropriation of assets, and corruption35. These categories should be used as a starting point but a more detailed breakout can be developed to produce an agency-specific fraud risk assessment. For example, potential fraud risks to consider in the three general categories include:

1) Intentional manipulation of financial statements, which can lead to:
    a. Inappropriately reported revenues.
    b. Inappropriately reported expenditures
    c. Inappropriately reflected balance sheet amounts, including reserves.
    d. Inappropriately improved and/or masked disclosures
    e. Concealing misappropriation of assets.
    f. Concealing unauthorized receipts and expenditures.

2) Misappropriation of:
    a. Assets by:
        i) Employees.
        ii) Vendors.
        iii) Former employees and others outside the organization.

3) Corruption including:
    a. Bribery and gratuities

b. Aiding and abetting fraud by other parties (e.g., vendors).
c. Conflicts of interest
d. Embezzlement

Fraudulent Financial Reporting

Each of the three general categories includes at least one scheme of how the fraud could occur. For instance, the improper recognition of expenditures can be achieved via numerous schemes, including holding bills to pay in the next biennium and improper coding to appropriation lines. Any scheme that could be relevant to the agency should be considered in the assessment.

Agencies can use the framework in Appendix A to identify specific areas of greatest risk and as a foundation for customizing the assessment process for their specific needs. For example, starting with the expenditure recognition component of fraudulent financial reporting, the assessment should consider the following questions:

- What are the agency's appropriations and appropriation lines?
- Does the agency have several appropriation lines that could be used?
- Are there numerous transactions for a variety of expenses or is most expenses routine with little variety.
- Has the agency ever overspent appropriations in the past?

The types of fraudulent financial reporting that would be most probable for a state agency would be to understate expenditures or miscode expenditures to avoid over spending of appropriations. Conversely, some agencies may overstate expenditures to use up appropriation authority. Any intentional misstatement of accounting information represents fraudulent financial reporting.

Another consideration involves fraud where the objective is not to improve the agency's financial statements, but to cover up the misappropriation or misuse of assets. In this case, the fraud also includes fraudulent financial reporting.

Misappropriation of Assets

An agency's assets can be misappropriated by employees, customers, or vendors. The agency should ensure that controls are in place to protect such assets. Considerations to be made in the fraud risk assessment process include gaining an understanding of what assets are subject to misappropriation, the locations where the assets are maintained, and which personnel have control over or access to assets. Common schemes include misappropriation by:

- Employees
  - Creation of, and payments to, fictitious vendors.
  - Charging personal expenses on procurement cards
  - Payment of inflated or fictitious invoices.

    - Invoices for goods not received or services not performed.
    - Theft of inventory
- Employees in collusion with vendors, customers, or third parties.
    - Payment of inflated or fictitious invoices.
    - Invoices for goods not received or services not performed.
- Vendors.
    - Inflated or fictitious invoices.
    - Short shipments or substitution of lower quality goods.
    - Invoices for goods not received or services not performed.

Protecting against these risks requires not only physical safeguarding controls, but also periodic detective controls such as physical counts of inventory. Remember, a smart perpetrator may be thinking about such controls and design the fraud to circumvent or be concealed from those controls. Those conducting the risk assessment should keep this in mind when deliberating misappropriation of asset schemes and their impact to the agency.

Corruption

Corruption is operationally defined as the misuse of entrusted power for private gain. There are various types of corruption, and could include such things as taking bribes to award contract, embezzlement, and aiding and abetting vendors to commit fraud.

Information Technology and Fraud Risk

Organizations rely on IT to conduct business, communicate, and process financial information. A poorly designed or inadequately controlled IT environment can expose an organization to fraud. Today's computer systems, linked by national and global networks, face an ongoing threat of cyber fraud and a variety of threats that can result in significant financial and information losses. IT is an important component of any risk assessment, especially when considering fraud risks. IT risks include threats to data integrity, threats from hackers to system security, and theft of financial and sensitive information. Whether in the form of hacking, of data, viruses, or unauthorized access to data, IT fraud risks can affect everyone. In fact, IT can be used by people intent on committing fraud in any of the three general fraud risk areas. Examples of those risks by area include:

Fraudulent financial reporting

- *Unauthorized access to accounting applications* — Personnel with inappropriate access to the general ledger, subsystems, or the financial reporting tool can post fraudulent entries.
- *Override of system controls* — General computer controls include restricted system access, restricted application access, and program change controls. IT personnel may be able to access restricted data or adjust records fraudulently.

Misappropriation of assets

- *Theft of assets* — Individuals who have access to assets (e.g., cash, inventory, and fixed assets) and to the accounting systems that track and record activity related to those assets can use IT to conceal their theft of assets. For example, an individual may establish a fictitious vendor in the vendor master file to facilitate the payment of false invoices, or someone may steal inventory and record the assets as disposed of, thus removing the asset from the balance sheet.

Corruption

- *Misuse of customer data* — Personnel within or outside the organization can obtain employee data and use such information to obtain credit or for other fraudulent purposes.

Keep in mind, cyber fraudsters do not even have to leave their homes to commit fraud, as they can route communications through local phone companies, long-distance carriers, Internet service providers, and wireless and satellite networks. What is important is that any information — not just financial — is at risk, and the stakes are very high and rising as technology continues to evolve.

To manage the ever-growing risks of operating in the information age, an agency should know its vulnerabilities and be able to mitigate risk in a cost-effective manner. Therefore, IT risk should be incorporated into an agency's overall fraud risk assessment.

Regulatory and Legal Misconduct

Regulatory and legal misconduct includes a wide range of risks, such as conflicts of interest, contract terms, and state and federal regulations. Depending on the particular agency and the nature of its business, some or all of these risks may be applicable and should be considered in the risk assessment process.

Assessment of the Likelihood and Significance Of Identified Inherent Fraud Risks

Assessing the likelihood and significance of each potential fraud risk is a subjective process. All fraud risks are not equally likely, nor will all frauds have a significant impact on every agency. Assessing the likelihood and significance of identified inherent risks allows the agency to manage its fraud risks and apply preventive and detective procedures rationally. It is important to first consider fraud risks on an inherent basis, or without consideration of known controls. By taking this approach, management will be better able to consider all relevant fraud risks and design controls to address the risks. After mapping fraud risks to relevant controls, certain residual risks will remain, including the risk of management's override of established controls. Management must evaluate the potential significance of those residual risks and decide on the nature and extent of the fraud preventive and detective controls and procedures to address such risks.

Likelihood — Management's assessment of the likelihood of a fraud risk occurring is informed by instances of that particular fraud occurring in the past at the agency, the prevalence of the fraud risk in the agency's industry, and other factors, including the number of individual transactions, the complexity of the risk, and the number of people involved in reviewing or approving the process. Agencies can have as many categories of the likelihood of potential frauds occurring as deemed reasonable, but three categories are generally adequate: remote, reasonably possible, and probable.

Significance — Management's assessment of the significance of a fraud risk should include not only financial statement and monetary significance, but also significance to criminal, civil, and regulatory liability. Agencies can also categorize the significance of potential frauds in as many buckets as deemed reasonable, but three categories are generally adequate: immaterial, more than significant and material.

People/department — As part of the risk assessment process, the agency will have evaluated the incentives and opportunities for individuals and departments and should use the information gained in that process to assess which individuals or departments are most likely to have the opportunity to commit a fraudulent act, and, if so, via what means. This information can be summarized into the fraud risk assessment grid and can help the agency design appropriate risk responses, if necessary.

Response to Residual Fraud Risks

Risk tolerance varies from agency to agency. While some agencies want only to address fraud risks that could have a material financial impact, other agencies want to have a more robust fraud response program. Many agencies will state that there is a "zero tolerance" policy with respect to fraud. However, there may be certain fraud risks that an agency considers too expensive and time-consuming to address via controls. Consequently, the agency may decide not to put controls in place to address such risks. If a fraud is discovered, zero tolerance for fraud will be applied.

An agency's risk tolerance level provides management support on how to respond to fraud risk. Fraud risks can be addressed by accepting the risk of a fraud based on the perceived level of likelihood and significance, increasing the controls over the area to mitigate the risk, or designing internal audit procedures to address specific fraud risks. Management needs to implement the right level of controls based on the risk tolerance it has established for the agency. The key is to be selective and efficient. There are probably thousands of potential controls that could be put in place. The goal is a targeted and structured approach — not an unstructured or haphazard approach — and efficient controls that deliver the most benefit for the cost of resources. The overall objective is to have the benefit of controls exceed their cost.

In addressing fraud risks, one should be careful to ensure that anti-fraud controls are operating effectively and have been designed to include appropriate steps to deal with the relevant risks. Where an internal control might be executed with limited skepticism (e.g., agreeing an expenditure to underlying support) an anti-fraud control would include an evaluation of the underlying support for consistency in application from prior periods and for potential inappropriate bias. Therefore, anti-fraud controls should be designed appropriately and executed by competent and objective individuals.

APPENDIX A - FRAUD RISK ASSESSMENT FORM

The following is a brief example of a fraud risk assessment. This example does not list all possible fraud risks that an agency might have. Each agency has to brainstorm to come up with their own risks. This example is just to help state agencies get started with their assessments.

This assessment needs to be done for all Financial areas: Accounting, Payroll, Purchasing, Contracting and for Information Technology. For agencies with more than one division that has financial functions, the assessment needs to be completed per division.

Identified Fraud risks and Schemes[1]	Likelihood[2]	Significance[3]	People and/or Department[4]	Existing Anti-fraud Controls[5]	Controls Effectiveness Assessment[6]	Residual Risks[7]	Fraud Risk Response[8]
FINANCIAL REPORTING:							
Revenue Recognition							
Recording receipts in incorrect periods	Remote	Insignificant	Accounting	Manager year end review of receipts.	Tested by Independent staff.	Risk of Management Override.	No further action, receipts are minimal and no benefit to agency of management to record in error.
Expenditure Recognition							
Holding bills	Reasonably possible	Material	Accounting	Input of bills and approval are segregated.	Tested by Independent staff.	Risk of Override.	Independent staff tests year end expenses.
Improper coding of bills	Reasonably possible	Material	Accounting	1) Input of bills and approval are segregated. 2) Review of itemized reports by Senior Management.	1) Tested by Independent staff. 2) Tested by Independent staff.	1) Risk of Override. 2) Adequately mitigated by controls.	1) Independent staff tests vouchers. 2) N/A

Identified Fraud risks and Schemes[1]	Likelihood[2]	Significance[3]	People and/or Department[4]	Existing Anti-fraud Controls[5]	Controls Effectiveness Assessment[6]	Residual Risks[7]	Fraud Risk Response[8]
Misclassification of Balances							
Reporting more receivables and less cash	Remote	Significant	Accounting	Receivable and receipt recording are segregated.	Tested by Management.	Adequately mitigated by controls.	N/A
MISAPPROPRIATION OF ASSETS:							
Cash/Checks							
At time of receipt	Probable	Insignificant	Receptionist	Independent reconciliation of receipts to deposits.	Tested by Management.	Possible that receipts aren't listed on receipt list so there would be nothing to reconcile. However, receive minimal amounts of cash/checks. Any large amounts to be coming in, either have been billed to others or management is awaiting the receipt.	N/A--Receipts are minimal.
Accounts Payable/Expenditures							
Unauthorized Pcard transactions	Probable	Material	Pcard Holders Vendors	1) Pcard Administrator is not a Pcard Holder.	1) Tested by Management.	1) Adequately mitigated by controls.	1) N/A

Identified Fraud risks and Schemes[1]	Likelihood [2]	Significance [3]	People and/or Department [4]	Existing Anti-fraud Controls[5]	Controls Effectiveness Assessment[6]	Residual Risks[7]	Fraud Risk Response[8]
				2) Pcard Administrator checks Pcard charges on-line once or twice a week.	2) Tested by Management.	2) Improper charges would be found after the fact, but policies are in place for disciplinary action for fraudulently acts.	2) There are daily and monthly spend limits so with the controls, any unauthorized amounts would be found by Pcard administrator before the amount would be significant. Also, code of conduct and Pcard policies provide for disciplinary action.
				3) Invoices required for all charges, reviewed by Senior Management, input by staff, approved by Fiscal Officer.	3) Tested by Independent staff.	3) Adequately mitigated by controls.	3) N/A
				4) Pcard Holder can check their charges on-line at any time to check for erroneous charges.	4) Tested by Management.	4) Adequately mitigated by controls-Pcard will issue credits for unauthorized charges.	4) N/A

Identified Fraud risks and Schemes[1]	Likelihood[2]	Significance[3]	People and/or Department[4]	Existing Anti-fraud Controls[5]	Controls Effectiveness Assessment[6]	Residual Risks[7]	Fraud Risk Response[8]
Fictitious Vendors	Remote	Material	Accounting	1) Only State Procurement can set up vendors. 2) Management approval of invoices and review of itemized reports.	1) Tested by Management. 2) Tested by Independent staff.	1) Accounting staff could request a vendor to be set up for a one-time only payment and Procurement would do so if payment is under $600. Staff could set up a regular vendor, but have IRS and other forms to complete to set this up. 2) Adequately mitigated by controls.	1) One-time vendor amounts are insignificant so no further controls required on that. For other regular vendor set up, any payments would be reviewed by management, who should know most vendors they are dealing with. 2) N/A
Inflated invoices submitted by vendor	Remote	Material	Vendors	Shipments counted upon receipt.	Tested by Management	Adequately mitigated by controls.	N/A
Payroll							
Unauthorized payroll adjustments	Reasonably Possible	Material	Payroll	Management approves monthly and supplemental payroll registers and one-time payment queries.	Tested by Management.	Adequately mitigated by controls.	N/A

Identified Fraud risks and Schemes[1]	Likelihood [2]	Significance [3]	People and/or Department [4]	Existing Anti-fraud Controls[5]	Controls Effectiveness Assessment[6]	Residual Risks[7]	Fraud Risk Response[8]
Capital Assets and Inventory							
Theft by employees	Reasonably Possible	Insignificant	All employees	1) Majority of capital assets are highly visible, needed for daily work, difficult to move and would be noticed if missing. 2) Accounting for assets and inventory taking are segregated.	1) Tested by Management. 2) Tested by Management	1) Slight risk of portable items, such as laptops being taken. However, have only 6 laptops and one person assigned custody of them. 2) Adequately mitigated by controls.	1) N/A--Value of portable items is insignificant and custodian would notice missing laptops. 2) N/A
Theft by others	Remote	Insignificant	Visitors	Portable items, such as laptops are kept in a room that outsiders don't have easy access to.	Tested by Management	Adequately mitigated by controls	N/A
CORRUPTION:							
Kickbacks/conflict of interest							
Contracts improperly awarded	Remote	Material	Accounting	Senior Management reviews all payments before payment and reviews monthly itemized reports	Tested by Independent staff	Risk of Override	Testing by Independent staff

1. Identified Fraud Risks and Schemes: This column should include a full list of the potential fraud risks and schemes that may face the organization. This list will be different for different organizations and should be formed by discussions with employees and management and brainstorming sessions.
2. Likelihood of Occurrence: To design an efficient fraud risk management program, it is important to assess the likelihood of the identified fraud risks so that the organization establishes proper anti-fraud controls for the risks that are deemed most likely. For purposes of the assessment, it should be adequate to evaluate the likelihood of risks as remote, reasonably possible, and probable.
3. Significance to the Organization: Quantitative and qualitative factors should be considered when assessing the significance of fraud risks to an organization. For example, certain fraud risks may only pose an immaterial direct financial risk to the organization, but could greatly impact its reputation, and therefore, would be deemed to be a more significant risk to the organization. For purposes of the assessment, it should be adequate to evaluate the significance of risks as immaterial, significant, and material.
4. People and/or Department Subject to the Risk: As fraud risks are identified and assessed, it is important to evaluate which people inside and outside the organization are subject to the risk. This knowledge will assist the organization in tailoring its fraud risk response, including establishing appropriate segregation of duties, proper review and approval chains of authority, and proactive fraud auditing procedures.
5. Existing Anti-fraud Internal Controls: Map pre-existing controls to the relevant fraud risks identified. Note that this occurs after fraud risks are identified and assessed for likelihood and significance. By progressing in this order, this framework intends for the organization to assess identified fraud risks on an inherent basis, without consideration of internal controls.
6. Assessment of Internal Controls Effectiveness: The organization should have a process in place to evaluate whether the identified controls are operating effectively and mitigating fraud risks as intended. Organizations should consider and review what monitoring procedures would be appropriate to implement to gain assurance that their internal control structure is operating as intended.
7. Residual Risks: After consideration of the internal control structure, it may be determined that certain fraud risks may not be mitigated adequately due to several factors, including (a) properly designed controls are not in place to address certain fraud risks or (b) controls identified are not operating effectively. These residual risks should be evaluated by the organization in the development of the fraud risk response.
8. Fraud Risk Response: Residual risks should be evaluated by the organization and fraud risk responses should to address such remaining risk. The fraud risk response could be implementing additional controls and/or designing proactive fraud auditing techniques.

APPENDIX B

The following illustrates the types of frauds an agency might encounter. This listing is not meant to be all-inclusive but to provide a starting point for an agency to identify which areas are vulnerable to fraud. For a few of the risks listed, a possible reason for committing fraud has been included. Once identified, the fraud risk assessment framework shown in Appendix A could be used.

1) Intentional manipulation of financial statements can lead to:
   a) Inappropriately reported revenues
      (1) Fictitious revenues
      (2) Period of recognition of revenues
          Reason: A special fund may have to turn over its fiscal year end balance over a certain amount to the General fund, and to avoid reaching that balance at the end of a fiscal year, deposits are held and recorded in the following fiscal year.
   b) Inappropriately reported expenses
      (1) Period recognition of expenses
          Reason: May hold bills to pay in next biennium and not report on closing packages otherwise will show over expenditure of appropriations.
      (2) Miscoding of expenses
          Reason: May use incorrect coding to avoid overspending a line item
          Reason: May use incorrect coding to cover up paying unallowable expenses.
   c) Inappropriately reflected balance sheet amounts, including reserves
      (1) Improper asset valuation
          (a) Capital Assets
          (b) Accounts receivable
      (2) Misclassification of assets
          Reason: May under report cash and report excess receivables to conceal the fact that payments on receivables are being stolen.
      (3) Concealed liabilities and expenses
          (a) Omission
   d) Inappropriate disclosures
      (1) Liabilities omissions
      (2) Subsequent events
      (3) Related-party transactions
   e) Concealing misappropriation of assets
   f) Concealing unauthorized receipts and expenditures

2) Misappropriation of Assets:
   Reason: All misappropriations are for personal gain/benefit.
   a) Cash theft
      (1) Collection procedures
      (2) Theft of checks received
      (3) Deposit lapping
   b) Fraudulent disbursements
      (1) False refunds
      (2) Personal purchases with state funds (including Pcard)
      (3) Fictitious vendors
      (4) False invoices

c) Payroll fraud
   (1) Falsified hours
   (2) Unauthorized salary adjustments
d) Expense reimbursement
   (1) Overstated expenses
   (2) Fictitious expenses
e) Capital Assets/ Inventory
   (1) Misuse of inventory
   (2) Theft of inventory
   (3) False shipments

3) Corruption including:
a) Bribery to
   (1) Employees
   (2) Public officials
b) Embezzlement
   (1) False accounting entries
   (2) Unauthorized withdrawals
   (3) Unauthorized disbursements
   (4) Paying personal expenses from state funds
   (5) Unrecorded cash payments
   (6) Theft of physical property
c) Receipt of bribes, kickbacks, and gratuities
   (1) Bid rigging
   (2) Kickbacks
      (a) Diverted business to vendors
         Reason: Contract may be given to an individual/company because of a kickback or because the vendor is a relative or friend. Could split payments to avoid showing payments that should have been awarded via an RFP.
      (b) Over billing
   (3) Illegal payments
      a) Gifts
      b) Travel
      c) Entertainment
      d) Credit card payments for personal items
   (4) Conflicts of interest
      a) Purchases
         Reason: Same as listed under "Kickbacks" above.
      b) Sales
      c) Ownership interest in suppliers
d) Aiding and abetting fraud by other parties such as vendors.