

Building a Robust Fraud Risk Assessment Framework: Best Practices and Tips

In the previous article of *#ForensicForesight*, we explored the significance of conducting a fraud risk assessment and how it can help organisations identify and prevent fraudulent activities.

Want a recap? Check it out [here!](#)

In this article, we will build upon that foundation and learn how to create a comprehensive fraud risk assessment using real-world examples. We begin with understanding about assessing the vulnerability of an organisation, as it is crucial in identifying potential risks.



Vulnerability Assessment

Before any organisation can effectively prevent fraud, it must first **identify the areas where it is most vulnerable**. *For example, inadequate internal controls over financial reporting, insufficient monitoring of third-party vendors, lack of whistle-blower hotlines and reporting mechanisms, etc.* Once these have been identified, the next step is to assess the **likelihood** and potential **impact** of each fraud risk event. This involves **assigning a risk score** to each risk using **historical data, industry standards, and expert judgement**.

The likelihood and impact of a fraud risk event are determined based on a subjective assessment of the probability of the event occurring and the potential impact on the organisation. Here are some steps to follow when determining likelihood and impact:

- **Likelihood:** Consider the probability of the fraud risk event occurring. This can be based on historical data, industry standards, and expert judgment.
- **Impact:** Consider the potential impact of the fraud risk event on the organisation. This can include financial losses, reputational damage, and regulatory sanctions.

- **Assign ratings:** Use a rating scale, such as high, medium, or low, to rate the likelihood and impact of the fraud risk event.
- **Calculate the risk score:** Multiply the likelihood rating by the impact rating to calculate the risk score. This will give you an overall assessment of the risk associated with the fraud risk event.
- **Prioritise risks:** Use the risk scores to prioritise the fraud risks and determine which risks require the most attention and resources.

It's important to note that the likelihood and impact ratings are subjective and can vary depending on the individual conducting the assessment. *It's essential to use a consistent approach and involve multiple stakeholders to ensure that the ratings are as objective as possible.*

Fraud Risk Assessment Template

In this article, we have used a **basic template** to provide a fundamental understanding of fraud risk assessment and then an **advanced template with responses**. It is important to note that this template can be customised and adapted to suit the specific needs of different organisations. While learners can improvise and use their own matrix and templates, there are also several templates and guidelines provided by various organisations, such as the Association of Certified Fraud Examiners (ACFE), that can be used to **ensure a comprehensive and effective fraud risk assessment**. By utilising these resources, organisations can **proactively identify their vulnerabilities and take appropriate measures** to prevent fraud.

Following is a basic fraud risk assessment template applied to four different industries:

Industry	Fraud Risk Category	Fraud Risk Factor	Likelihood	Impact	Risk Rating
Retail	Sales transactions	Point of Sale (POS) skimming	Low	High	High
Retail	Financial Reporting	Improper revenue recognition	Medium	High	High
Healthcare	Billing and coding	Upcoding	High	Medium	High
Healthcare	Inventory management	Theft of drugs	Low	High	High
Banking	Loans and mortgages	Loan fraud	Medium	High	High
Banking	Internal controls	Insider fraud	Low	High	High
Manufacturing	Procurement	Kickbacks and bid-rigging	High	Medium	High
Manufacturing	Asset misappropriation	Theft of raw materials	Low	High	High

In this example, we have applied the template to four different industries: **retail, healthcare, banking, and manufacturing**. For each industry, we have **identified two different fraud risk**

categories and **assigned a fraud risk factor**, likelihood, impact, and risk rating to each category.

For the retail industry, we have identified **point of sale (POS) skimming** and **improper revenue recognition** as two high-risk fraud categories. In the healthcare industry, we have identified **upcoding** and **theft of drugs** as high-risk fraud categories. In the banking industry, we have identified **loan fraud** and **insider fraud** as high-risk fraud categories. Finally, in the manufacturing industry, we have identified **kickbacks** and **bid-rigging** and **theft of raw materials** as high-risk fraud categories.

This table serves as a starting point for conducting a fraud risk assessment in each industry, allowing fraud examiners and forensic accountants to identify areas of high risk and develop strategies for mitigating those risks.

A Walkthrough to Create a Fraud Risk Assessment

Based on the above template, here is a simple walkthrough to understand the various components of creating a fraud risk assessment framework for an organisation.

Task Description	
Identify and prioritise fraud risks	Interviews, surveys, and reviewing past fraud incidents.
Assess the likelihood and impact of fraud risks	Evaluating the likelihood of the risk occurring and the potential impact it could have on the organisation.
Evaluate existing controls	Reviewing policies, procedures, and other internal controls to determine their effectiveness.
Develop a fraud risk management plan	Strategies to mitigate and manage fraud risks, such as implementing additional controls or procedures.
Monitor and update the plan	Regularly reviewing and updating the plan to ensure it remains effective and relevant to the organisation's changing fraud risks.

Advanced Template with Response

As we have understood from the industry perspective, the following is an **advanced template** for the framework that illustrates how the elements of fraud risk identification, assessment, along with responses are applied in a rational, structured approach to specific circumstances.

Identified Fraud Risk	Likelihood	Significance	People/Dept.	Existing Anti-Fraud Control	Effectiveness	Residual Risks	Fraud Risk Exposure
Inappropriate journal entries	Reasonably possible	Material	Finance	Standard monthly and quarterly journal entries maintained. The review process in place for standard entries and on-standard entries subject to two levels of review.	Tested by IA Tested by management.	Risk of override	Unusual Dr./Cr. combinations.
Domineering Board members. Conflicts of interest	Moderate	Significant	General Mgt.	Annual conflict of interest disclosure Stringent board recruitment and selection policy and processes	Tested by external auditors.	Undeclared conflict of interest. Inadequate understanding of the roles of some AC members Lack of background checks.	Lack of Established protocol for disclosure of potential conflicts of interest. Poor tone at the top.
Intruders gaining access to the systems using default or weak passwords or stolen and reused credentials.	Reasonably possible	Material	ICT/All	Cobit 5 regular Mgt. review of all password-protected accounts and related privileges and ensure that all users on IT systems (business application, IT infrastructure, system operations, development and maintenance) are uniquely identifiable. Define and implement procedures to grant, limit and revoke access to systems, premises, buildings and restricted areas.	Tested by IA.	Weak logical access control in place.	Unauthorised access to key info.

Both these templates can be modified using the above idea, or by using a standardised template like the one provided by the ACFE, organisations can ensure that they conduct a thorough and comprehensive fraud risk assessment.

Navigating the Challenges

As we have gained a practical understanding of implementing a fraud risk assessment framework, it will be evident that it comes with its own set of challenges that can impede its effectiveness, such as:

1. *Failure to use subject matter experts to analyse the fraud risk.*
2. *Viewing fraud risk assessment as a one-off episodic event with no value addition.*
3. *Difficulty in interpreting and using information and data.*
4. *Failure to act upon the results of fraud risk assessment.*
5. *Leaving the responsibility to manage fraud risk to the Risk Management and Compliance Unit.*
6. *Over-controlling fraud risk.*
7. *Too many different risk assessments are being performed across the organisation.*

However, professionals can follow a few tips to ensure that their fraud risk assessments are successful and valuable to their organisations, such as formulating **simple and understandable terms** in communicating data, **reviewing for reasonableness** of

implementing recommended actions for addressing residual fraud exposure, **holding staff/process owner accountable** with action plans/deadline for implementation, **solicit heightened interest** from all stakeholders, and importantly, **adopting a consistent approach** to avoid too many assessments being performed.

Here's a Condensed 7-Step Guide to Help You Establish a Robust Fraud Risk Assessment for An Organisation:



It is now apparent that implementing a fraud risk assessment framework is a critical component of any effective fraud prevention program. *A fraud risk assessment helps organisations identify their vulnerabilities and proactively take measures to prevent fraud. This preventive measure can be a beneficial practice for individuals starting their careers in forensic accounting and fraud examination.* By conducting regular fraud risk assessments, individuals can gain valuable experience and skills while helping organisations safeguard against fraud. **A strong understanding of the fraud risk assessment process can help individuals identify red flags and risks and take appropriate actions to mitigate them.** By following the steps outlined in this article, forensic professionals can develop and implement a robust fraud risk assessment framework that can help protect organisations and individuals against fraud.

Remember, fraud prevention is not a one-time effort but a continuous process. Regular fraud risk assessments are essential to identify new threats and protect against potential losses.



DR. DURGESH PANDEY