PATHWAY TO REVENUE PROTECTION

Vilas Sateesh

1. ABOUT THIS ARTICLE

Organizations in this digital, agile, innovative (and now the "post-pandemic") era continuously steer through various challenges. However, regardless of the era or type of organization, "revenue protection" is of prime significance because revenue represents the daily flow of oxygen for an organization to sustain. Any erosion or leakage or whatever term is used affects the organizations deeply and might often turn an otherwise profitable business into a less or not profitable one at all. In an international survey conducted across 2000 business leaders, 45% of the respondents mentioned that revenue leakage is a systematic problem that they face (BCG, July 2020, Achieving rapid topline growth with revenue assurance). Effective revenue protection can contribute as much as 10% to an organization's total revenue without the need to sell additional products or services (BCG, July 2020, Achieving rapid topline growth with revenue assurance). This article explains how to approach revenue protection pragmatically.

2. INTRODUCTION

The term "revenue protection" is a loosely used term that is highly subjective. For a better understanding of this term as well as to narrow down its definition, the broader concept of "revenue management" first needs to be understood. In layman's terms, the term revenue management refers to any activity that is aimed at improving the revenues of the organization. More specifically, revenue management could be defined as the set of activities carried out by an organization to protect, optimize, or maximize its revenues. It can now be seen that there are 3 further components in revenue management. A better way to understand these 3 components is to look at the pertinent question that each of them tries to address.

- **Revenue protection** - How do I protect my existing revenues? Am I billing and collecting whatever I am supposed to bill and collect?
- **Revenue optimization** - How do I optimize my operations to increase revenue or prevent opportunity losses?
- **Revenue maximization** - Can I expand my fields of play and introduce additional revenue streams?

Out of the above 3 layers, revenue protection could be viewed as the foundation layer, i.e., without this layer, the other 2 layers cannot be sustained. After all, what is the point in maximizing or optimizing revenues when organizations cannot effectively protect them?

Narrowing down the definition, revenue protection encompasses all the activities undertaken by an organization to protect its existing revenues by ensuring the accuracy of its billings and enhancing the efficiency of its collections. Revenue protection is not a one-time activity, rather it is an ongoing journey that needs a lot of organizational support and dedication. Broadly speaking, the revenue protection journey typically comprises of three stages, i.e., detection, prevention, and sustainance. The rest of the article focuses on these three stages.

3. DETECTION STAGE

The detection stage commences upon realization by the organization, where it begins to suspect that something is wrong but cannot articulate where the issue is, how big the issue is, or what exactly is leading to the issue. Detection specifically tries to address "where are the revenue leakages" through various techniques but relies heavily on data analytics and process vulnerability analysis. The basic objective at this stage is to identify "what could go wrong" which is nothing but potential scenarios that might ultimately lead to revenue leakages. To understand this better, consider the below table that lists some of the risks that prevail at various stages of a typical revenue life cycle.

#	Revenue life cycle phase	Examples of typical revenue risks ("what could go wrong")
1	Pricing strategy	• Unknowingly providing goods or services at a lower rate or free of cost, where the cost base is complex and cost allocations are not adequately performed. • Misuse of discounts to boost sales performance
2	Customer onboarding and granting of credit facility	• Granting credit facility to a non-eligible customer or provision of credit more than the eligible amount • Failing to protect credit limit with adequate collateral security
3	Delivery of goods and services	• Provision of goods or services in excess of secured credit limits • Manipulation of the delivery mechanism by the customer to avail excess delivery or similar economic benefits (including internal manipulation by employees)
4	Billing	• Intentional suppression of billable transactions by the customers (more prevalent in revenue share agreements) • Delays in billing resulting in working capital loss
5	Collections[1]	• Delinquent customers or bad debts where there is no recourse available to collect the amount due from them. • Granting credit period in excess of the period availed by the organization from its suppliers, resulting in working capital loss

The above-mentioned risks are just illustrative and not exhaustive. Another key overarching element that will always be considered is the fraud risk. It is estimated that organizations typically lose 5% of revenue to fraud each year[2].

1. It is estimated that 1 to 5% of EBITDA (i.e., Earnings before interest, taxation, depreciation & amortization) flows unnoticed out of companies, because they do not have their contract management system and payment follow-up completely in order (EY, August 2019, Revenue Leakage – How to identify revenue leakages in your company and recoup them). Based on similar research, focusing on government revenue leakages, it was observed that 20% of government revenues worldwide go missing every year, either because of non-payment or outgoing payments gone awry (McKinsey & Company, January 2018, The trillion-dollar prize: Plugging government revenue leaks with advanced analytics).

2. Based on a study of 2110 cases across 133 countries (The Association of Certified Fraud Examiners, 2022, "Occupational fraud 2022 – A report to the nations")

3.1 Significance of data analytics in the detection of leakages

Living in an age of "big data" there is no further messaging needed to mention the significance of data analytics in detecting revenue leakages. Traditionally data analysis or rather revenue analysis was nothing more than a comparative analysis of transactions, some trend analysis, performance metrics analysis, etc. With the advancement of data analytics, organizations these days are employing advanced data analytics techniques and methods such as econometrics, machine learning, etc. These techniques when combined with forensic accounting make the detection layer even stronger where the fraud risk is higher. Research suggests that in large, developed economies, analytics capabilities have the potential to increase total government revenue by 1 to 3%, while in developing countries the opportunity is much larger as much as 10% (McKinsey & Company, January 2018, The trillion-dollar prize: Plugging government revenue leaks with advanced analytics). In parallel, stakeholder expectations are rising, wherein the revenue leakages are expected to be less than 1% due to advanced analytics providing visibility on leakage at every step (McKinsey & Company, January 2022, Finding hidden value with order-to-cash optimization)

In today's world, there are numerous platforms available for performing analytics ranging from spreadsheets to SQL queries to advanced software like R, Python, Alteryx, etc. Regardless of the platform, the objective is to come up with red flags or anomalies that if further investigated could be unearthed as leakages. The following is an illustrative list of some of the non-conventional ways of anomaly detection using data analytics, which is being used these days for revenue leakage detection typically in the retail/trading sector:

- Sales price realization analysis to analyze leakages from excessive discounts.
- Analysis of transactions carried out at unauthorized prices.
- Analysis of average transaction processing time per employee, mainly cashiers at the supermarket to identify any suspicious behaviors.
- Analysis of credit limit overshoots for each customer
- Identification of transactions with blacklisted customers who had payment issues in the past
- Important transactions which were approved just before the departure of an employee.
- For self-invoicing / invoicing based on customer declaration or data:
    - Analysis of missing transaction sequences
    - Analysis of excess usage of void transactions
    - Identification of manipulations using techniques such as Benford's Law[3]
    - Validation of declared information against information provided by an independent third party.

It should however be noted that data analytics alone will not effectively pinpoint all probable areas of leakage. Data analytics should go hand in hand with in-depth analysis of business processes and their vulnerabilities.

3 Benford's law, named after Physicist Frank Benford, states that in numbered lists providing real-life data (e.g., a journal of cash disbursements and receipts, contract payments, or credit card charges), the leading digit is one almost 33 percent (i.e., one third) of the time. On the other hand, larger numbers occur as the leading digit with less frequency as they grow in magnitude to the point that nine is the first digit less than 5 percent of the time (Regional Training Institute Kolkata, Comptroller and Auditor General of India, 29 February 2016, Research paper on "Using Benford's Law in Audit")

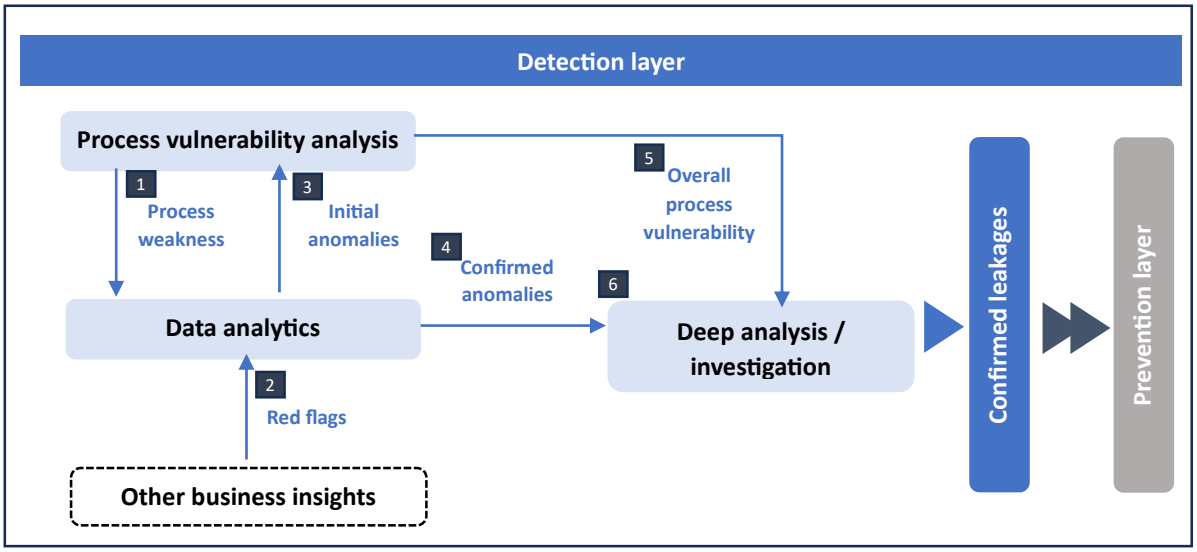
3.2 What is "process vulnerability analysis"?

"Process vulnerability analysis" examines how vulnerable are the revenue processes to revenue risks. The starting point is to identify what are the typical revenue risks considering the industry and the business model. Once the risks are identified, the next step is to assess the revenue processes in terms of available internal controls to mitigate those risks. In today's world, system controls or information technology controls play a significant role in the functioning of business controls. Hence, process vulnerability analysis should lay special emphasis on information technology/system controls assessment. In fact, the presence of internal controls is associated with lowering fraud losses and quicker fraud detection. Based on a study of 2110 cases across 133 countries, it is estimated that nearly half of the fraud cases occurred due to lack of internal controls or an override of existing controls (The Association of Certified Fraud Examiners, 2022, "Occupational fraud 2022 – A report to the nations").

3.3 Overall schema of detection

So, how do analytics, vulnerability analysis, and all fit together in the identification and confirmation of leakages? This is better explained through an interrelationship diagram as shown in figure 1.

Figure 1



Source: Author

1	**Process weaknesses**	Weaknesses in process controls (including information technology controls) that could expose revenue to leakages (more qualitative), but very important input for data analytics. The weaknesses discovered herein are often treated as scenarios for data analytics.
2	**Red flags**	Most of the organizations would have some idea regarding the loopholes or areas of weakness. These red flags if analyzed in depth through process vulnerability analysis and data analytics could be a typical low-hanging fruit for any revenue leakage analysis.
3	**Initial anomalies**	Initial insights from data analytics may or may not turn out to be real leakages, but each of these anomalies needs to be analyzed in detail, i.e., complemented with the knowledge of process weaknesses to assess whether these are confirmed anomalies or just anomalies themselves (hence to be dropped).

4	**Confirmed anomalies**	Not just anomalies in the data but are serious candidates for revenue leakage. However, needs to be investigated further before confirming as leakage.
5	**Overall process vulnerability**	Initial process weaknesses strengthened with some story from analytics, i.e., these are areas that are not just qualitative weaknesses, but there are some supporting anomalies observed in the data which might be hinting towards potential leakage.
6	**Deep analysis/investigation**	The stage at which the data anomalies coupled with an understanding of process weaknesses are analyzed further. Usually, each material anomaly is analyzed against process weakness and if it is pointing towards a leakage, then additional analysis is performed. This additional analysis involves verification of source documents for the underlying transaction or set of transactions, interviewing the relevant personnel, verifying the backend of information systems, etc. The end result is either confirmation of leakage or dismissing the anomaly.

3.4 Types of leakages

The leakages that are confirmed could be classified broadly into the following categories.

1	**Recoverable leakages**	Leakages that could be recovered from the customer either in line with the contractual clause or have the potential of being recovered through legal action. These types of leakages are viewed very seriously by the management as the issue might have persisted in the past and have the potential to persist in the future.
2	**Irrecoverable leakages**	Leakages that can no longer be recovered mostly due to time-barred issues. However, the root causes need to be examined so that this kind of leakage does not persist in the future.
3	**Notional leakage**	Indirect leakages that might not be perceived as leakage in the first place but have a material impact on the working capital that ultimately affects the bottom line. e.g., delays in billing. Most of the organizations does not view this seriously, but those with high commercial mandate treat this very seriously.
4	**Probable leakage**	Serious process vulnerabilities that indicate leakage or potential for leakage, but which have not been substantiated with data. e.g., the absence of a sound credit policy. Organizations usually take a calculated risk here and try to implement mitigation mechanisms that would limit the probability of leakage.

Regardless of the type, once leakage is confirmed, the next phase is to establish adequate mitigation actions in place.

4. PREVENTION STAGE

At the prevention stage, the organization realizes that a particular type of leakage has occurred or there is a potential for future leakage and thereby the need for corrective measures. As per studies, 81% of organizations that were victims of fraud, modified their controls following the fraud. Out of this 75% increased management review procedures while 64% increased use of proactive data monitoring analysis (The Association of Certified Fraud Examiners, 2022, “Occupational fraud 2022 – A report to the nations”).

But before putting the prevention mechanisms in place, be it corrective or pre-emptive, the critical thing is to identify what exactly caused the leakage typically known as “root-cause analysis”.

4.1 Root-cause analysis

Root-cause analysis implies analyzing the underlying environment of the leakage. This could be explained with the example of a "sales skimming fraud" which is a type of business fraud in which the cash proceeds are stolen by a fraudster employee before the transaction is entered into the financial accounting system. Imagine this kind of fraud has been detected at one of the supermarkets. Now, apart from the disciplinary measures taken against the culprit employee, the victim organization would be more interested in preventing similar cases in the future. This is where root cause analysis comes into the picture. In this specific case, root cause analysis comprises of analyzing:

1. Are there policy guidelines available for thresholds for acceptance of cash, periodic stock count, surprise cash verifications, etc., and to what extent these are followed?
2. What is the underlying process of customer ordering, cash collection, tendering of change, and delivery of goods including information technology and physical access controls?
3. What process and information technology controls are in place for the segregation of duties between cashiering and stock count and separation of access controls between point-of-sale machine and stock module?

The above is just an indicative list, but organizations need to go into similar depth if they are to implement mechanisms to prevent revenue leakages.

4.2 Implementation of mitigation actions

"Mitigation actions" are corrective measures or pre-emptive measures put in place by an organization in response to a revenue leakage. Examples include information technology fixes, the introduction of new controls, strengthening the adherence of existing controls, etc. Once required mitigation actions are determined, the organization, before implementing them will typically weigh those against several parameters such as:

- Overall risk appetite
- Cost vs. benefit – i.e., what is the cost of implementation of the measure compared against the value it protects.
- Confirmed vs. probable leakage, i.e., likelihood of occurrence.
- Availability of other mitigating controls
- One-time initiative vs. repeated monitoring (e.g., a system enhancement is more of a one-time initiative that could be preferred over a manual control that needs to be monitored periodically)

5. SUSTAINANCE STAGE

Once the organization has identified the leakages and has put in place the mitigation measures, the next natural step is to continue the momentum and lay down a solid foundation to continue protecting the revenues on an ongoing basis, i.e., "revenue monitoring". But unfortunately, this is where most of the organizations fail. In an international survey conducted across 2000 business leaders, out of the organizations that identified revenue leakage as a significant concern, three fourth of the organizations did not have an automated revenue assurance process, 64% did not have any standardized tools as part of their enterprise system and 59% do not devote any full-time staff or equivalent to revenue monitoring function (BCG, July 2020, Achieving rapid topline growth with

revenue assurance). Organizations that have been successful in sustaining the momentum of revenue protection had some critical ingredients, explained below.

5.1 Dedicated organizational function

Successful organizations create a dedicated revenue monitoring function as part of their organization structure. The housing of this dedicated function could depend upon the nature, size, and complexity of the organization and business model, e.g., could be housed within Finance, Commercial, or as a standalone function. Alongside the positioning of the function, equally important is how well the function is staffed in terms of capabilities and skills. The revenue monitoring function needs two kinds of core skill sets, data analytics and business process risk analysis. Further to these core skill sets, there are certain generic skills that any resource working in this function should have such as commercial acumen, problem-solving skills, good communication and articulation skills, etc.

5.2 Effective partnering with other functions

The basic nature of the revenue monitoring function calls for effective and deep working relationships with quite a lot of wider organizational functions. These functions include, but are not restricted to Sales, Commercial, Contracts Management, Legal, Finance, Information Technology, Business Intelligence, etc. In most cases, there will be a constant flow of information and input between revenue monitoring and these functions which in turn calls for adequate support and sponsorship from top management. To ensure effective coordination and support from other functions, it is quite a common practice to form working groups with a specific mandate depending upon the needs of the organization.

5.3 Clearly defined processes

Like any other function, the revenue monitoring function also needs sound governance. It is advisable to have clearly define governance around:

- **Leakage detection** – covering data acquisition, data validation, cleansing, running analytical procedures, validation of anomalies, confirmation, and communication of leakages.
- **Risk & controls/vulnerability analysis** – covering the process framework to be adopted for analysis of processes, maintenance of risk register, methodology for mapping of controls with leakages, etc.
- **Controls monitoring** – covering procedures for testing of relevant revenue controls, periodicity/frequency, data owners, etc.

5.4 Adequate monitoring tools

Monitoring tools, as the name suggests, are not strictly data analytics tools, but rather any platform or models that are used by the revenue monitoring function on an ongoing basis. The most common ones are “monitoring dashboards” that would give the initial inputs to the team in the following areas:

- On areas where the leakage was detected before, is it persisting or decreasing thanks to the implementation of mitigation mechanisms.
- On areas where no leakage was detected previously, does the situation still hold good, i.e., no leakages could be detected.
- Other basic analysis of revenue KPIs and measures

6. RECAP AND KEY TAKEAWAYS

- Revenue protection is more of a continuous journey than a one-time assignment and calls for patience, a methodical approach, and extensive organizational and management support.
- Revenue protection is not just about improving billing accuracy, but rather analyzing the entire revenue touchpoints.
- In today's world of big data, organizations use both conventional and non-conventional data analysis techniques to uncover leakages.
- Mere detection of leakages is not sufficient to ensure the protection of revenues. This calls for side-by-side analysis of process risks & controls with data analysis to identify leakages and to put control measures to prevent leakages from occurring in the future.
- To continue the momentum of revenue protection, organizations need to have a dedicated function that is well equipped with top management support, skillsets, processes, and tools.

7. REFERENCE

1. "Achieving rapid topline growth with revenue assurance". BCG. 2020. Retrieved 20 August 2023 from https://web-assets.bcg.com/37/de/22e7339f4cf99e36a30e75be1cd6/bcg-achieving-rapid-topline-growth-with-revenue-assurance-july-2020.pdf
2. "Revenue Leakage – How to identify revenue leakages in your company and recoup them". EY. 7 August 2019. Retrieved 20 August 2023 from https://www.ey.com/en_be/consulting/revenue-leakage--how-do-you-identify-revenue-leakages-in-your-co
3. "The trillion-dollar prize: Plugging government revenue leaks with advanced analytics". McKinsey & Company. 29 January 2018. Retrieved 20 August 2023 from https://www.mckinsey.com/industries/public-sector/our-insights/the-trillion-dollar-prize-plugging-government-revenue-leaks-with-advanced-analytics
4. "Occupational fraud 2022 – A report to the nations". Association of Certified Fraud Examiners. 2022. Retrieved 20 August 2023 from https://acfepublic.s3.us-west-2.amazonaws.com/2022+Report+to+the+Nations.pdf
5. "Finding hidden value with order-to-cash optimization". McKinsey & Company. 31 May 2022. Retrieved 20 August 2023 from https://www.mckinsey.com/capabilities/operations/our-insights/finding-hidden-value-with-order-to-cash-optimization#/
6. Research paper on "Using Benford's Law in Audit". Regional Training Institute Kolkata, Comptroller and Auditor General of India. 29 February 2016. Retrieved 20 August 2023 from https://cag.gov.in/uploads/research_paper/RES-2-Benford-05ebe241db89494-32544853.pdf