Drug Diversion: How Robust is Your Prevention and Detection Program?

Fixed Asset Controls and Reporting
Who’s paying attention to one of your largest assets?

Development and Use of Risk, Control and Monitoring Matrices
How to direct your audit resources

Meaningful Use: Auditing Challenges and Opportunities
Your pathway to providing value
Managing Risk: Development and Use of Risk, Control and Monitoring Matrices

How to direct audit resources where they are most needed

By C. Brantley Synco, MSHI, MBA, CPA, CIA, CAMS, CHPC, CHC

Doing more with less is an imperative for internal auditors, thus making efficient use of our human resources essential. Value-added ROI expectations call for laser-like focus on those processes and functions with high impact and a high likelihood of occurring. Do you know those places in your organization? Baptist Health shares their simple yet effective means to direct and maximize audit resources.

The main purpose of an internal audit function is to provide an organization’s leadership and/or board with reasonable assurance that management is sufficiently mitigating risk. Internal auditors conduct audits and reviews of business units and processes within organization to meet this goal.

To effectively conduct an audit or review, you should understand the risks within an area and the controls management has installed to mitigate those risks. A risk, control and monitoring matrix (RCM) is a flexible and adaptive method that you can use to document the risk and controls within a business unit or process.

The RCM consists of two main components: the control narrative and the risk matrix. The narrative and matrix address:

- Definition and significance of identified risks
- Documentation of the control(s) established to mitigate these risks
- Monitoring processes to assure the controls are operating

Control narrative
The control narrative should capture all relevant elements of a process. In essence, the control narrative is a written version of a process walk-through. To create the narrative, you should review all available documentation about the process (e.g., policies and procedures, previous audit reports, job descriptions of key employees, etc.).

After the documentation review, you should engage the process owner and frontline employees in performing a walk-through. The process owner should describe the design...
of the process and the frontline employees should provide their perspectives on the actual process. If the process is transactionally based, you should select one or more items depending on transaction variety and complexity, and follow it through the full process.

Inherent risk is a function of the impact of an event and the likelihood the event will occur.

During the walk-through, you should ensure that the actual documented process supports what has been described and perhaps is supported by policy and procedures. Then look for actions that create risk and controls that are in place to mitigate these risks. The excerpt below is from an RCM of an accounts payable (AP) process:

Several times throughout the day, an AP employee checks the AP in-box for payment requests and invoices received. All items received are then date stamped and forwarded to the appropriate employee’s tray.

The first sentence defines an action that creates the risk: “An AP employee checks the AP in-box for payment requests and invoices received.” The second sentence describes the control in place: “All items received are then date stamped and forwarded to the appropriate employee’s tray.”

In this case, the control addresses the risk that payment requests and invoices are not processed in a timely manner. By time-stamping payment requests and invoices, management can monitor the length of time for payments to be processed. However, the control does not address the risk of all payment requests and invoices not being received. To address this risk, look for a log or register of all payment requests and invoices received.

The narrative should continue to document the complete process. As an auditor, you should ask questions to clarify unusual or unexpected steps in the process. After a completing the narrative, you can then begin to construct the risk matrix.

Risk matrix
The basic components of the risk matrix are:

1. Risk
2. Impact
3. Likelihood
4. Inherent risk
5. Control
6. Monitoring
7. Control Effectiveness
8. Residual risk

When placed into the matrix, the basic components become the headers for each column. Exhibit 1 is an example of a line from an AP RCM.

Risk
When defining a risk, it is important to listen to and engage with the process owner. The process owner is often keenly aware of what can go wrong. Remember, they are the experts on their process. You (as an auditor) are the expert on controls.
**RCM** is a flexible and adaptive method to document the risk and controls within a business unit or process.

**Impact**
If something did go wrong, how much damage, both financial and reputational, could occur? Process owners tend to downplay the impact of risk. One way to address this is to ask a simple question: "If this risk happened, how much would it hurt?" Generally, this should be an "ice breaker" to get the process owner to think more realistically about risk.

In an RCM, impact is measured in qualitative terms such as low, medium and high. In practice, the actual qualitative term used is irrelevant because the term is converted to a quantitative value in the calculation of inherent risk. Management and/or auditors may want to assign criteria to encourage consistency. However, criteria are not significant to the use of an RCM matrix.

**Likelihood**
Simply put, likelihood is an estimate of the possibility of the risk occurring. For example, the likelihood of an employee falsifying mileage on an expense report may be high. However, the likelihood of an employee falsifying a supervisor’s signature is relatively low.

Similar to impact, likelihood is measured in qualitative terms often correlating to frequency. Common terms used to describe frequency are remote, possible and probable. Again, the qualitative terms describing impact are converted to a quantitative value for the use of an RCM.

**Inherent risk**
Inherent risk is a function of the impact of an event and the likelihood the event will occur. As mentioned, to calculate inherent risk, the qualitative terms used for impact and likelihood are converted to quantitative values. Exhibit 2 depicts the values assigned to the Impact and Likelihood.

**Exhibit 2 – Risk values**

<table>
<thead>
<tr>
<th>Impact</th>
<th>Likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low= 1</td>
<td>Remote= 1</td>
</tr>
<tr>
<td>Med= 2</td>
<td>Possible= 2</td>
</tr>
<tr>
<td>High= 3</td>
<td>Probable= 3</td>
</tr>
</tbody>
</table>

To determine the inherent risk, use the following equation:

\[ \text{Inherent risk} = \text{Impact} + \text{Likelihood} \]

By placing Impact along the x-axis and Likelihood along the y-axis, a scoring grid is created for all possible combinations of Impact and Likelihood.

**Exhibit 3 – Likelihood**

<table>
<thead>
<tr>
<th>Impact</th>
<th>1 (Remote)</th>
<th>2 (Possible)</th>
<th>3 (Probable)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (Low)</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>2 (Med)</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>3 (High)</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
</tbody>
</table>
Residual risk is risk that remains after considering all mitigation efforts.

Then the combinations are categorized into the calculated inherent risk.

**Exhibit 4 – Inherent risk**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Low</td>
</tr>
<tr>
<td>3</td>
<td>Low</td>
</tr>
<tr>
<td>4</td>
<td>Medium</td>
</tr>
<tr>
<td>5</td>
<td>High</td>
</tr>
<tr>
<td>6</td>
<td>High</td>
</tr>
</tbody>
</table>

**Control**

A control is any action management has established to decrease the possibility of an identified risk occurring. Stated more broadly, a control is anything that increases the probability of a “good thing” occurring and/or decreases the probability of a “bad thing” occurring. Another often-used definition is a control helps management ensure their objectives are being met.

As you know, controls take many forms, such as segregation of duties, record balancing, reconciliations, edit checks, system access, etc. Generally, controls can be grouped into two generic categories, although there are other specific categorizations:

- **Detective Control**: A detective control records and reports an undesired action after it occurs. For example, record access logs.
- **Preventative Control**: A preventative control stops or blocks an undesired action. For example, passwords required for logins to applications.

**Monitoring**

Monitoring is any action management undertakes to assure that the control is functioning as intended. Monitoring is equally as important as the control itself. Consider the following example:

- **Risk**: A risk of inappropriate physical access to an area has been identified.
- **Control**: A lock with a badge swipe is placed on the entrance to the area. Only authorized personnel are allowed badges.
- **Monitoring**: None

In this scenario, how can management be confident that only authorized personnel have badges? Do unauthorized persons such as cleaning staff or terminated employees have active badges? As you can see, lack of monitoring negatively affects the control’s effectiveness.

**Control effectiveness**

Control effectiveness is, in the judgment of the auditor, how well the control mitigates the identified risk. To determine effectiveness, you should consider many factors, including:

- Design of the control
- Implementation of the control
- Compensating controls
- Monitoring of the control by management

The effectiveness of a control is often described as high, medium, or low. Similar to Impact and Likelihood, Control Effectiveness is measured in qualitative terms that are converted to quantitative values.

Residual risk

Residual risk is risk that remains after considering all mitigation efforts (i.e., after understanding and evaluating the effectiveness of all controls implemented). Residual risk is calculated using this equation:

\[
Residual\ Risk = Inherent\ Risk - Control\ Effectiveness
\]

By placing Inherent Risk along the x-axis and Control Effectiveness along the y-axis, you can create a scoring grid for all possible combinations of Inherent Risk and Control Effectiveness.
Creation of RCM matrices can be very time and resource intensive. However, after the initial development work is completed, the matrix only needs to be updated on a periodic basis or when significant changes have occurred. For example, at Baptist Health System, we have developed RCMs for all financial processes. We update the RCMs each year in preparation for our external audit. The process gives management and the external auditors a clear picture of our financial control environment. Additionally, we review and update the RCM when planning a related audit. Reviewing the RCM allows us to develop our testing plan around higher risk processes.

**Conclusion**

In a perfect world, audit departments would have sufficient time and resources to thoroughly test all risks associated with an organization. In the real world, this is not possible. Developing a robust RCM program enables the Chief Audit Executive to focus resources on departments or processes with a high residual risk. The effect is maximization of the organization’s internal audit resources. NP

---

### Use of risk, control and monitoring matrix

Creation of RCM matrices can be very time and resource intensive. However, after the initial development work is completed, the matrix only needs to be updated on a periodic basis or when significant changes have occurred.

For example, at Baptist Health System, we have developed RCMs for all financial processes. We update the RCMs each year in preparation for our external audit. The process gives management and the external auditors a clear picture of our financial control environment. Additionally, we review and update the RCM when planning a related audit. Reviewing the RCM allows us to develop our testing plan around higher risk processes.

**Likelihood is an estimate of the possibility of the risk occurring.**

---

### Exhibit 5 – Control effectiveness

<table>
<thead>
<tr>
<th>Inherent Risk (From Exhibit 4)</th>
<th>1 (Low)</th>
<th>2 (Med)</th>
<th>3 (High)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Med</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>High</td>
<td>4</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Low</td>
<td>5</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>Med</td>
<td>6</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>High</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>