Risk Management Tools – Control Summary and Assessment Pro-forma

<table>
<tr>
<td>Control Name</td>
<td>
When naming a control, it needs to be specific so there can be no confusion.
Describing controls in a manner such as: Training; Policies and procedures; Induction; Physical security; and Processes is not helpful in terms of the next step, which is to determine their effectiveness.
To that end, the control name should be described as follows:

Annual fraud control training program
Separation of duties
Fraud component of induction package
Unauthorised external device audits
Penetration testing program

</td>
</tr>
<tr>
<td>Control Category</td>
<td>
The control category is derived from two things:

The consequence of the risk; and
The criticality of the control.

The consequence of the risk is self-explanatory. I use the following matrix to determine criticality of a control relative to the risk:
<table>
<tr><th>Criticality</th><th>Descriptor</th></tr>
<tr><td>5</td><td>The control is absolutely critical to the management and reduction of the risk. If this control is ineffective or partially effective, the likelihood and/or consequence of the risk will increase significantly (i.e. increases likelihood or consequnece by 3 or more levels)</td></tr>
<tr><td>4</td><td>The control is very important to the management and reduction of the risk. If this control is ineffective or partially effective, the likelihood and/or consequence of the risk will increase (i.e. increases likelihood or consequnece by 2 levels)</td></tr>
<tr><td>3</td><td>The control is important to the management and reduction of the risk. If this control is ineffective or partially effective, the likelihood and/or consequence of the risk will increase (i.e. increases likelihood or consequnece by 1 level)</td></tr>
<tr><td>2</td><td>The control has some impact on the management and reduction of the risk. Depending on the criticality of the other controls, an analysis should be undertaken to determine the necessity of this control.</td></tr>
<tr><td>1</td><td>The control has little to no impact on the management and reduction of the risk. It is unlikely this control is required.</td></tr>
</table>
Note: This criticality rating is captured in the risk register.

To determine the category of the control I use the following matrix:
</td>
</tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><th></th><th colspan="5">Criticality</th></tr>
<tr><th>Consequence</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th></tr>
<tr><td>Severe</td><td>Category 3</td><td>Category 2</td><td>Category 2</td><td>Category 1</td><td>Category 1</td></tr>
<tr><td>Major</td><td>Category 3</td><td>Category 3</td><td>Category 2</td><td>Category 2</td><td>Category 1</td></tr>
<tr><td>Moderate</td><td>Category 4</td><td>Category 3</td><td>Category 3</td><td>Category 3</td><td>Category 2</td></tr>
<tr><td>Minor</td><td>Category 4</td><td>Category 4</td><td>Category 4</td><td>Category 3</td><td>Category 3</td></tr>
<tr><td>Insignificant</td><td>Category 4</td><td>Category 4</td><td>Category 4</td><td>Category 4</td><td>Category 4</td></tr>
</table>

Note: As many controls will be controlling multiple risks, the lowest category assessed will be the one recorded in the pro forma.
As an example, the same control may be controlling 5 risks, but due to the consequence and criticality of each, there are different categories:
Risk #1: Category 3
Risk #6: Category 2
Risk #11: Category 1
Risk #17: Category 3
Risk #21: Category 4
The lowest category assessed in this case is a Category 1 – which is the category that is recorded in the pro forma.
</td></tr>
<tr><td>Requirement</td><td>This is a brief summary of what is required by the control.
As an example:
All new starters are to be subject to police background checks prior to commencing work within the Department</td></tr>
<tr><td>Control Type</td><td>Controls are categorised as either:
Preventative
Detective
Corrective
Your organisation may have different names for the different types of control.</td></tr>
<tr><td>Control Owner</td><td>This is the person within the organisation with responsibility and accountability for the effective implementation, monitoring, measuring and improvement (where necessary) of the control.
The owner of the risk will be by name or by position.</td></tr>
<tr><td>Legislative/Regulatory Requirements the Control is Linked to (Policy Only) – if applicable</td><td>Many controls (mainly policies) within an organisation will be linked to a Legislative/Regulatory requirement. Listing them in the control register will align the compliance program to the risk program.
In my opinion, there are only two reasons for an organisation to develop a policy:
To meet a compliance obligation; and/or
To reduce risk.</td></tr>
</table>

<table>
<tr><td></td><td>The alignment of the two programs is critical to ensure risks are being managed and compliance obligations are being met.</td></tr>
<tr><td>Procedures/Processes Control is linked to</td><td>This will highlight all of the procedure and process documents that are aligned to the policy (where applicable)</td></tr>
<tr><td>Risks control is linked to</td><td>As previously stated, many of the controls in an organisation will be controlling more than one risk.
As an example; the control: Background Checks on new Starters will be linked to the following enterprise risks:
Inappropriate behaviour towards a client by a member of staff
Unauthorised release of confidential information
Fraudulent/corrupt act by an employee involved in procurement
Fraudulent/corrupt act by an employee involved in accounts payable/receivable/cash transactions</td></tr>
<tr><td>Performance Measure/s</td><td>To be able to determine if a control is effective in both design and implementation, performance measures need to be identified for each control.
If we use the control previously mentioned; Background Checks on new Starters the following are the performance measures I would capture in this proforma:
% of new starters that have had their backgrounds checked (this simply measures whether it is being done – i.e. implementation)
# of issues/anomalies discovered where the issue/anomaly should have been identified during the background checking process (this measures whether it is being done in accordance with guidelines).</td></tr>
<tr><td>Effectiveness Measure</td><td>Based on the category of the control, the performance required for the control to be effective will be different. For Category 1 controls, the target should be 100% and anything less than that might be considered ineffective, as shown in the matrix below:
<table>
<tr><th>Effectiveness</th><th>Performance</th></tr>
<tr><td>Effective</td><td>100% of new starters that have had their backgrounds checked</td></tr>
<tr><td>Mostly Effective</td><td rowspan="2"></td></tr>
<tr><td>Partially Effective</td></tr>
<tr><td>Not Effective</td><td><100% of of new starters that have had their backgrounds checked</td></tr>
</table>
For a Category 3 control it may look like this:
<table>
<tr><th>Effectiveness</th><th>Performance</th></tr>
<tr><td>Effective</td><td>100% % of new starters that have had their backgrounds checked</td></tr>
<tr><td>Mostly Effective</td><td>80-99% of new starters that have had their backgrounds checked</td></tr>
<tr><td>Partially Effective</td><td>50-79% of new starters that have had their backgrounds checked</td></tr>
<tr><td>Not Effective</td><td><50% of new starters that have had their backgrounds checked</td></tr>
</table></td></tr>
</table>

<table>
<tr><td>Frequency of Control Review</td><td>Once again, the category of the control will determine the frequency of control assessment.
<table>
<tr><th>Control Category</th><th>Control Self-Assessment</th><th>Assurance by Internal Audit</th><th>External Audit of Control</th></tr>
<tr><td>Category 1</td><td>Monthly</td><td>Quarterly</td><td>Annually</td></tr>
<tr><td>Category 2</td><td>Quarterly</td><td>Every 6 months</td><td></td></tr>
<tr><td>Category 3</td><td>Annually</td><td></td><td></td></tr>
<tr><td>Category 4</td><td>Annually</td><td></td><td></td></tr>
</table></td></tr>
<tr><td>Results of Last Review</td><td>This is where the results are recorded of the assurance/audit activities of the control</td></tr>
<tr><td>Control Effectiveness</td><td>On the basis of the results above, and assessment of the control is made as either:
Effective
Mostly Effective
Partially Effective
Ineffective
Not yet assessed</td></tr>
</table>