Risk Overview Template

Version 1.0

This template is a companion piece to the [online article](http://www.go-rbcs.com/articles/how-to-validate-your-security-program-part-nine), “How to Validate Your Security Program – Part Nine – Security Relevance”, by Ray Bernard PSP CHS III

**Validation Attribute: Relevant**

**Definition:**

1. pertinent to matters at hand
2. relating to a subject in an appropriate way

In this case we’re talking about the security program’s relevance to the organization. Both of the definitions above apply, and could be restated this way:

1. supporting the current goals, objectives and activities of the business
2. applied in a way that is harmonious to business operations and activities

This is both a risk-orientation factor and a business-alignment factor.

Use the table within this document to hold the Risk Overview information. There is a separate worksheet for recording the Business Alignment information.

**Risk Orientation**

The main purpose for this risk orientation exercise is to get a high level view of the risks, how they relate to your security program elements, and see how recently the individual risks or risk categories have been evaluated.

Use these steps is to determine when, and how thoroughly, each risk or risk category has been considered, and whether or not further risk evaluation may be warranted. Much of the work of collecting this information (the first 4 or 5 columns in Step 1 below) can be delegated to staff.

**Step 1.** Utilize the **Risk Overview Data Table** below to list the risks.

* **Risk ID** (a number)
* **Risk** (the name or brief description of the risk or risk category)
* **Security Program Element** (this is not the security control or measure, but the name of the security program element that addresses the risk, such as Executive Travel Protection or IT Disaster Recovery Plan or Insurance Program)
* **Date Risk Assessed** (Date of most recent assessment, or “Unknown”)
* **Note** (any comment you wish to make)
* **Conclusion** (whether further risk examination is needed, and how that should be approached)

Fill out the first four columns, capturing any key thoughts or questions you have in the Notes column. If you already have a risk register or risk list, you can copy the risk information into this table. Many risk registers don’t identify the security program element in which the security control or measure resides, but you can identify that easily enough. If you don’t already have a risk register or list of risks that various security program elements are addressing, then take the actions you need to identify the risks each program element is addressing and enter the information into the table.

**Step 2.** Review your Notes, getting answers for your open questions.

**Step 3.** Review each Risk entry, and enter your Conclusion as to whether any action is needed to further evaluate the risk or the measures being used to address it. You may find a few risk items that require you to dig deeper to reach a sound conclusion. Outline a small plan for following up, using micro-assessments where helpful to delegate some of the work.

**Step 4.** Reviewyour conclusion, and if further action is needed, outline an action plan for following-up.

**Risk Overview Data Table**

| **Risk ID** | **Risk** | **Security Program Element** | **Date Risk Assessed** | **Note** | **Conclusion** |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |