Business Alignment Worksheet

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.

**Business Alignment**

Good business alignment takes into account the impact of security on the business. The smoother security controls work from a business planning and operations perspective, the better. This prompts an update to the traditional description of security’s role:

The role of security is to reduce security risks to acceptable levels, at an acceptable cost, *in a manner harmonious to the business*.

**Step 1.** Copy and paste a set of placeholder heading sections for each element in your security program, copy these headings to create a blank section to fill out. For each security program element, under each heading you will describe the degree of business alignment harmony from the perspective of the heading.

* Culture
* Planning
* Processes
* Communications
* Competencies
* Technology
* Relationships

**Step 2.** For each security program element, **c**heck with the personnel involved to identify any frustrations, friction points, excessive burdens or subversion that your or your security personnel experience. Then check also with the non-security personnel who interact with security personnel related to the security program element, or who have processes, procedures or tasks to execute relating to the security program element.

You may already know about some points of disharmony that exist for several of your security program elements. For those program elements where you are not closely familiar with the communications, collaborations and interactions that take place, check with the security personnel and those whom they deal with (separately is preferable), to identify any points of disharmony that they are aware of.

*You may have to begin your conversation by assuring the personnel that you are not performing a security audit or examining any personnel*, but simply looking for opportunities for improvement in how the security program is being carried out.

**Step 3.** Create an additional document section titled, “Opportunities for improvement”. Review your notes and determine where opportunities for improvement exist, and write down your ideas for making those improvements. In some cases, additional research, thought or collaboration may be required to work out exactly how improvements could be accomplished. Write down how you would approach those actions.

**Step 4.** In a separate document, create an action plan for pursuing the opportunities for improvement, establishing a schedule or at least a sequence for carrying out the improvements. Make sure that you include a “Lessons Learned” action item in which you document what you have learned along the way. Obtain whatever management approval or buy-in is required to put the plan into action, and execute the plan according to the sequence or schedule you have established.

**Important Note:** If you are responsible for the security function in a large organization, you may want to pilot these actions in a single facility or business unit, or for a small selection of security program elements. That will make it easier to determine where and how you could best apply these validation steps with an optimal amount of effort.

**Supporting Materials:** You will find some very helpful perspectives for executing these validation steps in the first four sections (Manageability, Business Alignment, Security Ladder of Involvement, and Relationships and Allies) of the five sections of the [**Rate Your Security Program**](http://www.go-rbcs.com/rate-your-security-program) page.

## Final Note

Security practitioners who have applied these validation steps have said that they have strengthened their security program in ways that they would not have otherwise considered, and they also ended up with a good set of new “security talking points” for discussing any element of their security program.

***Initial instruction:*** *Save this template under a new filename, to preserver the original copy.*

# Business Alignment Evaluation

(Count the number of security program elements you have, and copy the headings immediately below that many times, to create empty document sections to fill out.)

## **Security Program Element:** [insert name here]

## Culture

[insert a note about the harmony or lack of it (frustrations, friction points, excessive burdens or subversion that you or your personnel experience) from the perspective **Culture** perspective]

## Planning

[insert a note about the harmony or lack of it (frustrations, friction points, excessive burdens or subversion that you or your personnel experience) from the perspective **Planning** perspective]

## Processes

[insert a note about the harmony or lack of it (frustrations, friction points, excessive burdens or subversion that you or your personnel experience) from the perspective **Processes** perspective]

## Communications

[insert a note about the harmony or lack of it (frustrations, friction points, excessive burdens or subversion that you or your personnel experience) from the perspective **Communications** perspective]

## Competencies

[insert a note about the harmony or lack of it (frustrations, friction points, excessive burdens or subversion that you or your personnel experience) from the perspective **Competencies** perspective]

## Technology

[insert a note about the harmony or lack of it (frustrations, friction points, excessive burdens or subversion that you or your personnel experience) from the perspective **Technology** perspective]

## Relationships

[insert a note about the harmony or lack of it (frustrations, friction points, excessive burdens or subversion that you or your personnel experience) from the perspective **Relationships** perspective]

# Security Program Element Harmony Check

(Per Step 1, copy the harmony check headings once for each security program element, into this section.)

## Opportunities for Improvement