Security Program "Good Practice" Profile

Ray Bernard PSP, CHS-III

Version 1.0 – the latest version of this document is available at: www.go-rbcs.com/good-practice-profile-template

Characterizing Your Good Practices

It can be very helpful to create a **good practice profile** of your security program. To do this you:

- *label the **security measures*** in each program element (as explained below)
- *label the **program element*** by (a) using all labels applied to any of the program element's security measures to show the scope of the program element, or (b) using the two or three labels used the most to reflect the predominant label values

Here are labels to use that characterize your security measures in a meaningful way.

Regulatory Requirement. The fact that it's a regulatory requirement is all the proof you need to include it in your security program. The only question might be, "To what extent do you need to implement the requirement?" That's where security design and planning come into play, as well as assessment.

Standards-Based. Standards are usually based upon best practice and/or good practice. Sometimes a standard gathers and unifies a collection of good practices under an overarching framework, to make it easier to implement and manage them. The question relating implementing a standard revolves around what parts of the standard are relevant to organization's specific security risks. Assessment usually has a role here.

Common Good Practice. Most common good security practices are easily recognizable because you see them practically everywhere. It's likely that the majority of your security program elements are common practices. Examples include central station security alarm monitoring, security officer patrols, card access control and video surveillance—which are utilized in most facilities. However, there are other good practices that are less common—such as routine security system testing, periodic re-assessment of security officer patrol routes (for completeness and value).

Sector-Specific Good Practice. Many business sectors have security practices that are specific to their type of business. For example, hospital security can include wheelchair tracking using any of several technologies; this is really asset management combined with asset protection. It is a good example of aligning a security measure with the operational needs of the organization. (In a hospital, if wheelchairs are not available, patients may not make their labs appointment and so lab time can be wasted, and patient treatment may need to be postponed as a result of a missed test.)

Company-Specific Good Practice. In large companies, it is common to find that good security practices become fine-tuned based upon company needs and company culture. In such a case the security practices can be designated for implementation on a company-wide basis and become a company standard. There can, of course, be variations based upon geographic and cultural factors.

Proven Program Element. A proven security program element is one that has shown itself to be very effective as you have implemented it, regardless of whether or not it is in practice outside your organization.

Validation Steps

Step 1. *List Your Security Program Elements and Their Key Measures.* Several earlier steps involved making or using a list of your security program elements. In this exercise you expand the list to include the key security measures of each program element.

Step 2. *Use the Good Practice Profile Chart Template*. **Use one the charts on pages 4 and 5** to profile your security program good practices, or download a Excel template to use. **Add rows to the chart as needed to hold your security program elements and their security measures that you will be rating. See page 6 for a chart formatting example.**

- The first two columns in the chart on the following page are for the names of your security program elements and their security measures. The second two columns (Age, Last Reviewed) are optional, as explained in the paragraphs that follow this columns listing.
- The next columns are for a check mark, an X, or a Yes/No dropdown selection. (The last two "company" columns are optional.)
- The final column is for any notes you may want to make for yourself:

Step 3. *Fill Out the Profile Chart*. This may require multiple sittings, with a little bit of research in between to finalize the chart. The majority of the work can be delegated if you have an available staff person; that is usually a good staff educational step.

Using the Good Practice Profile Chart

The **Age** and Last **Reviewed** columns can help you prioritize a plan for reviewing your security measures. There are a number of valuable perspectives that you can use to review security measures, and those are covered in a later article in this series.

The **Company Innovation** column is useful if your company values innovation, and you have implemented security measures that are innovative for your company. For example, providing the ability for Real Estate or Facilities personnel to securely access security video on their mobile devices could be considered a helpful innovation within your company, as it can provide a number of operational benefits to personnel with certain roles and responsibilities.

Utilize the **Company Strategic Objective** column to identify any your security program elements directly support one or more company strategic objectives, utilize that column as well. That may require a close review of your organization's strategic planning, something that you probably should be doing anyway if you are not already.

For the **Notes** column, you can eliminate space constraints by entering "See Note 1", "See Note 2", and so on and then writing the notes on pages that follow the chart pages.

During this work you may come across information a good practice that you don't have in your security program yet, but which you think would be beneficial. Be sure to make a note for the related Security Program element to capture the key information about the potential new good practice.

As always happens when you look at your security program from a new perspective, great ideas can come to light. You should gain some new security talking points and possibly something worth reporting on or maybe even some good points to brief management about.

Ray Bernard, is the principal consultant for Ray Bernard Consulting Services (RBCS), a firm that provides security consulting services for public and private facilities (www.go-rbcs.com). Mr. Bernard has also provided pivotal strategic and technical advice in the security and building automation industries for more than 28 years. For more information about Ray Bernard and RBCS go to www.go-rbcs.com or call 949-831-6788. Mr. Bernard is a member of the Subject Matter Expert Faculty of the *Security Executive Council* (www.SecurityExecutiveCouncil.com). He is also an active member of the ASIS International member councils for Physical Security and IT Security.

"Good Practice" Profile (Basic Chart)

Delete the explanatory entries in the chart. Copy and paste the square characters to mark which columns apply.

Security Program Element or Measure	**Regulation**	**Standard**	**Common Practice**	**Sector-Specific Good Practice**	**Company-Specific Good Practice**	**Proven Program Element**	**Notes** Write your notes after the chart, and number them. Put the Note number in this column like See Note 1.
1.0 Your first security program element	■	■	■	■			
1.1 This could be a sub-element containing several security measures, or a single security measure		■	■				
1.1.1 Security measure				■			
1.1.2 Security measure	■			■			

"Good Practice" Profile (Comprehensive Chart)

Add any company-specific columns that are important, such as the Insurance Requirement column included below.
Delete the explanatory entries in the chart. Copy and paste the square characters to mark which columns apply.

Security Program Element or Measure	Age	Reviewed (How long ago?)	Regulation	Standard	Common Practice	Insurance Requirement	Sector-Specific Good Practice	Company-Specific Good Practice	Proven Program Element	Company Strategic	Company Innovation	Notes Write your notes after the chart, and number them. Put the Note number in this column like See Note 1.
1.0 Your first security program element	5.5 Years	1 year	■	■	■	■	■					
1.1 This could be a sub-element containing several security measures, or a single security measure	4.0 years	2 years		■	■							
1.1.1 Security measure	4.0 years	Unknown			■	■						
1.1.2 Security measure	2.0 years	2 years	■				■					

"Good Practice" Profile – Formatting Example

Security Program Element or Measure	Regulation	Standard	Common Good Practice	Sector-Specific Good Practice	Company-Specific Good Practice	Proven Program Element	**Notes** Write your notes after the chart, and number them. Put the Note number in this column like See Note 1.
1.0 Management and Leadership	■	■	■	■	■	■	
1.1 Program Management / Security Management System		■			■		See Note 1
1.2 Policy / Standard Operating Procedures (SOPs) / Post Orders			■				
1.3 Security Sponsors and Stakeholders						■	See Note 2
2.0 Loss Prevention / Risk Management							
2.1 Risk Assessment	■	■	■				See Note 3
2.2 Risk Mitigation			■	■	■	■	See Note 4
2.3 Planning and Follow-Up			■				See Note 5
2.4 Security Education, Awareness and Training			■				
3.0 Personnel Protection							
3.1 Workplace Violence Protection Program		■	■	■			
3.1.1 Workplace Violence Training			■				
3.1.2 Security Phone Hotline			■				
3.1.3 Anonymous Employee Reporting Phone Hotline			■				
3.2 Executive Protection							
3.3 Travel Security Program							
3.4 Event Security			■				
			■				
			■				

Note 1. We are phasing over from our legacy approach to security program management, to a standards-based security management system.

Note 2. We are applying the common good practice of *360 Degree Leadership*.

Note 3. We apply the following standards:

- *NFPA 730 – Guide for Premises Security – 2006 Edition* by the National Fire Protection Association (NFPA)
- *ANSI/ASIS/RIMS RA.1-2015 – Risk Assessment* – based on ISO 31000 by American National Standards Institute, ASIS International, and the Risk and Insurance Management Society.