The SEARCH IT Security Self- and Risk-Assessment Tool: Easy to Use, Visible Results

Download this Assessment Tool spreadsheet at **www.search.org** or see Appendix A for a hard copy version of the assessment questions and worksheets to record your responses.

The Assessment Tool was developed using Microsoft Excel. If you do not have this application, you can download a free Excel reader at **www.microsoft.com/downloads**.

To complete your self-assessment, you can use the questions we have adopted and revised from the NIST guidance under SP 800-26.[11] To make the process a little easier, SEARCH has built an **IT Security Self- and Risk-Assessment Tool**, based on the information described in this chapter, to aid you in this process.

The Assessment Tool is a Microsoft Excel spreadsheet containing worksheets that cover the three information categories and subcategories described in Step 3—**Management**, **Operational**, and **Technical**—*and* a fourth category, developed and added by SEARCH, **State and Local Law Enforcement-Specific IT Security Controls**, which assists with recording information on additional state and local government issues.

The Assessment Tool allows your policy development team to walk through the process and record their answers in one location. The Assessment Tool provides your team with a simple and concise methodology by which to assess your systems and their potential risk. It gives a graphical view of the systems assessed and their current status, based on the team's input. Because of the graphical nature of the Assessment Tool, it is immediately obvious where important issues need to be addressed. The answers can give managers a roadmap to their response to the risk and offer guidance on funding requirements for their systems.

[11] *Security Self-Assessment Guide for Information Technology Systems,* November 2001.

A Tour of the Assessment Tool

The first page of the Assessment Tool is the Table of Contents (Figure 8), an indexed listing of the spreadsheet contents. Each topical area is hyperlinked to the worksheet containing the questions to be completed. When you highlight the section and left click on it with your mouse, you will be taken immediately to that worksheet.

Figure 8: Table of Contents, SEARCH IT Security Self- and Risk-Assessment Tool

■ Introduction

The introduction page provides an overview of the Assessment Tool and its use. It also references the NIST documents that were used to build the Assessment Tool.

■ Gathering Preliminary Information

This section is a resource page containing much of the information already discussed in this chapter, describing the kinds of information that the team must have available before it starts this project.

■ System Questionnaire

This system questionnaire cover sheet is used to document or describe the system or systems that are the focus of the assessment, who is involved with the assessment, and the purpose of the assessment.

Categories

The Assessment Tool is broken down into four main categories—three of these are used as described by NIST, and we have added a fourth category for questions specific to state and local law enforcement.

As discussed on page 57, the four categories contain 18 subcategories of questions your policy development team should answer during the assessment. The four categories and their subcategories are listed in Figure 9.

Management

1. Risk Management
2. Review of Security Controls
3. Lifecycle
4. Authorize Processing (Certification and Accreditation)
5. System Security Plan

Operational

6. Personnel Security
7. Physical and Environment Protection
8. Production, Input/Output Controls
9. Contingency Planning
10. Hardware and System Software Maintenance
11. Data Integrity
12. Documentation
13. Security Awareness, Training, and Education
14. Incident Response Capability

Technical

15. Identification and Authentication
16. Logical Access Controls
17. Audit Trails

State and Local Law Enforcement-Specific IT Security

18. FBI CJIS Compliance

Figure 9: Assessment Tool Categories/Subcategories

When you click on the hyperlink to one of the subcategories, you are immediately taken to the worksheet containing the particular set of questions for that subcategory. The questions are listed down the left side of the worksheet. A group of "Effectiveness Ranking" fields runs across the top. SEARCH has tried to make answering these questions as simple as possible for policy development teams that are using the self- and risk-assessment processes laid out in this Tech Guide.

Figure 10 shows the worksheet for the "1. Risk Management" subcategory within the Management category.

Assessment Questions	References	Effectiveness Ranking				
		L1 Policy	L2 Procedures	L3 Implemented	L4 Measuring	L5 Feedback/ Reassessment
Risk Management						
1.1. Critical Element: **Is risk periodically assessed?**						
1.1.1 Is the current system configuration documented, including links to other systems?						
1.1.2 Are risk assessments performed and documented on a regular basis or whenever the system, facilities, or other conditions change, and is management made aware of any new risks?						

Figure 10: Worksheet for Risk Management Subcategory

As shown in this worksheet, the five effectiveness ranking levels are listed across the top of the Assessment Tool. (See Figure 6 on page 59 for a detailed description of these levels.) In its documentation of this process, NIST asserts that the process should be followed from left to right: build your policy first, then your procedures, implement both, build your measurements, and then create a feedback loop.[12]

This linear process is ideal, but probably not realistic for most agencies. Many agencies have existing systems in which policies and procedures have been developed in *some* areas, and a certain amount of measures have been put in place to evaluate these. **But few agencies have successfully—or adequately—covered *all* levels, and this is where the Assessment Tool will really benefit your security planning.** Answering the questions in the Assessment Tool will immediately

[12] Note: The SEARCH IT Security Self- and Risk-Assessment Tool diverges from the NIST methodology by assuming few organizations have completed a full and detailed self-assessment and risk assessment of their IT systems—an exercise central to understanding what vulnerabilities exist and, therefore, what policies are needed. By beginning with a detailed analysis of an organization's IT environment, this Assessment Tool will then identify risks, gaps, and policy needs.

highlight those areas you have not yet addressed and give you a methodology with which to adequately address all of your security issues.

Going back to our original example question from the Risk Management subcategory, here's how the self-assessment immediately indicates those areas you need to address in your policy development and implementation. Let's say your answers to the question: "Is risk periodically assessed?" for each level are:

Level 1: "Yes," a policy exists.

Level 2: "Partially," we have *some* procedures in place for periodic risk assessment.

Level 3: "No," we have not implemented the policies and procedures.

Level 4: "No," we have not developed any process for measuring the implementation of our policies and procedures.

Level 5: "No," we have not built any feedback mechanisms into the process.

So how does the Assessment Tool make this easier for your team to answer the questions? As the team reviews the questions, they can use the <arrow> keys to highlight the specific field under the Effectiveness Ranking section and record an answer for that particular question and level. Highlighting the field displays a down arrow in that field, as shown in Figure 11. Clicking on the arrow displays a drop-down menu from which you can select an answer of "NO," YES," "PARTIAL," or "N/A."

Assessment Questions	References	Effectiveness Ranking				
		L1 Policy	L2 Procedures	L3 Implemented	L4 Measuring	L5 Feedback/ Reassessment
Risk Management						
1.1. Critical Element: **Is risk periodically assessed?**			▲▼ YES NO PARTIAL N/A			
1.1.1 Is the current system configuration documented, including links to other systems?						
1.1.2 Are risk assessments performed and documented on a regular basis or whenever the system, facilities, or other conditions change, and is management made aware of any new risks?						

Figure 11: Using Drop-down Menus to Answer Questions in Worksheet

Selecting an answer for that field provides the team with a *visual* representation of the answer. Red for "NO," green for "YES," yellow for "PARTIAL," and no color for "N/A," as illustrated in Figure 12. This gives the team and any managers using the Assessment Tool an immediate understanding of the status of that question in relation to the system. It also can give a manager an overall sense of the system by visually depicting the green "YES" answers versus the red "NO" and yellow "PARTIAL" answers. (In Figure 12, the green is represented by light gray, the red by light purple, and the yellow by dark gray.)

Assessment Questions	References	Effectiveness Ranking				
		L1 Policy	L2 Procedures	L3 Implemented	L4 Measuring	L5 Feedback/ Reassessment
Risk Management						
1.1. Critical Element: **Is risk periodically assessed?**		YES	PARTIAL	NO	NO	NO
1.1.1 Is the current system configuration documented, including links to other systems?		NO	PARTIAL	NO	NO	NO
1.1.2 Are risk assessments performed and documented on a regular basis or whenever the system, facilities, or other conditions change, and is management made aware of any new risks?		PARTIAL	PARTIAL	NO	NO	NO

Figure 12: Worksheet After Effectiveness Ranking Questions are Answered

The Assessment Tool's ease of use and its ability to aid the team by quickly documenting answers to the assessment questions makes using it a much easier process by which the team can complete the self- and risk-assessment processes.

Use the Assessment Tool!

Now it's time to complete all the questions in your self-assessment in the four categories of **Management**, **Operational**, **Technical**, and **State and Local Law Enforcement-Specific IT Security Controls**. Please use the assessment questions and response worksheets included in the Assessment Tool, located in Appendix A. Or, download the Microsoft Excel spreadsheet Assessment Tool from our web site at **www.search.org**.

Once you have completed the questions in the Assessment Tool, the next phase of the IT security policy development process requires you to identify and assess all the security *risks* you will uncover from this self-assessment process. Once you have identified these risks (see Chapter 4), developed controls to mitigate these risks (see Chapter 5), and developed and implemented measures that will assess the effectiveness of the controls (see Chapter 6), then you can begin actually *formalizing* your agency's security policies (see Chapter 7).