A Practical Approach
to
Managing Information System Risk

Tom Olzak
February 2008

Introduction

The mantra spinning around in the heads of most security managers affirms that managing security is about managing risk. Although they know this is the right approach, and they understand the importance of balance in designing and implementing security controls, many of them—including me—came up through the ranks of network engineering, programming, or some other technical discipline. While this prepared us for the technology side of our jobs, the skills necessary to assess and understand business risk arising from the use of information systems were not sufficiently developed.

The purpose of this paper is to provide security managers with a working understanding of risk management as it applies to information systems. The processes and tools included assume that organization- and enterprise-level controls are already functioning, and implementation of the target system is taking place within this existing security context.

I begin by exploring the challenges facing security managers every day when trying to balance security with the needs of business managers to maintain and improve operational effectiveness. I then define risk management and provide an overview of how to strategically approach the application of reasonable and appropriate safeguards. Finally, I provide a model and related tools for conducting a risk assessment, selecting the right controls, obtaining approval for implementation, and managing risk throughout the target system's lifetime.

The approach to managing information risk detailed in this paper is based on documents available at the National Institute of Standards and Technology (http://nist.gov/). Although the basic principles and many of the controls discussed in the following sections are straight from these documents, I frequently depart from the NIST approach based on my experience as a security manager as well as on information received via training and other sources.

Challenges

Security managers are expected to protect sensitive data from unauthorized access or modification and to ensure they are available when and where business operations require. This simple statement causes a lot of confusion about actual business risk and the amount of resources management should pull from other projects to strengthen network defenses. Eliminating this confusion is the primary role of risk management.

In my opinion, the first principle of risk management is that not all data are created equal. Some are fine for public release. Others are confidential in nature, but their release will not cause significant harm to the business, its customers, its employees, its investors, or the public. While other data are so sensitive that unauthorized release or modification would tend to drive the business into bankruptcy or result in serious financial or physical harm to individuals. So the first challenge facing risk managers is the proper classification of information. A proper classification of data is necessary before baseline and supplemental security controls can be designed, approved, and implemented.

Another challenge is the constant tension caused by the pull between business operations and the internal/external audit functions. Figure 1 depicts the balance that security managers are expected to achieve.

Figure 1: Achieving a balance
(Olzak, 2007)

Even though business management makes the final decisions about the right level of security constraints to impose on operations, security managers are expected to provide the information necessary to understand what is reasonable and appropriate. Risk management provides the processes and tools needed to produce meaningful, objective recommendations to management.

And finally, fitting necessary controls into a limited security budget is one of a security manager's biggest challenges—making sure the right budget is defined and dollars spent on people, process, and technology that provide the greatest mitigation of business risk. This includes understanding that building security into a solution—addressing security early in the solution's lifecycle—reduces initial costs as well as long term costs associated with managing applied controls.

The rest of this paper provides insight into successfully meeting these challenges by describing the process that leads to acceptable business risk as well as the tools security managers can use to work through the steps contained in that process.

What is Information System Risk Management?

The first step in managing business impact caused by information system compromise or failure is to understand what risk management is. My grandiose definition is as follows:

> Information risk management is the proper application of business risk mitigation tools and methods resulting in the implementation of security controls, that when operating properly—either alone or as part of a layered set of safeguards—mitigate business risk associated with an information system to a level acceptable to management. This must be done in a way that maintains the highest possible operational effectiveness of the personnel and processes using the systems protected by these controls.

This is a long way of saying that managing risk involves balancing system trustworthiness with the ability of the business to function. Increasing one will almost certainly diminish the other. Contained in this short version is the term "trustworthiness." According to the NIST guidelines, the goal of information system security is a trustworthy system. Trustworthy systems are defined as:

> "…systems that are worthy of being trusted to operate within defined levels of risk to organizational assets, individuals, [and] other organizations…, despite the environmental disruptions, human errors, and purposeful attacks that are expected to occur in the specified environments of operation" (Ross et al, 2007, NIST SP 800-39, p. 12).

This is another ostentatious definition that simply means that a system is trustworthy if, when placed into its target operating environment, it's protected and performs according to management's expectations.

Management's expectations are solidified by following a simple strategy to arrive at control recommendations, including (Ross et al, 2007, NIST SP 800-39, p. 11),

1. Determine the appropriate balance between the risks from and the benefits of using information. This should include asking whether the information currently collected and stored is even needed. You don't have to protect what you don't have.
2. Carefully select, tailor, and supplement the safeguards and countermeasures for information systems to achieve this balance.
3. Take responsibility for the IS solutions implemented within the information systems supporting the organizations.
4. Fully acknowledge and explicitly accept, transfer, or mitigate risks to operations, assets, individuals, or other organizations. Note that an organization's responsibility to manage risk extends beyond its own network. There is also a responsibility to ensure that business-to-business interfaces and other supporting infrastructure are reasonably protected so as not to become the source for attack against other organizations.
5. Be accountable for the results.
6. Keep it simple. Complexity is usually a counterbalance to security. As complexity grows, so does an organization's vulnerability to data leakage and other security issues. This can be complexity in network design, controls implementation, processes, etc.
7. Design security solutions with diversity in mind. The principle of diversity in design deals with the degree of variety in implemented controls. By variety is meant not only the types of controls but also the number of vendors and approaches to various controls (Olzak, 2006, p. 52).
8. Information systems should be protected by multiple layers of controls—defense in depth. Each layer should be designed to support other controls. It's the *combination* of the right policies, processes, and other controls at the appropriate layers that provides a secure processing environment (Olzak, 2006, p. 54).

The following section introduces a process and tools that can help organizations meet these objectives.

The Process

The NIST documentation on which much of this paper is based proposes a risk management process that is focused on how the U.S. government operates. In an effort to make it a little more generic—useful for private as well as public organizations—I modified the process. The result is depicted in Figure 2.

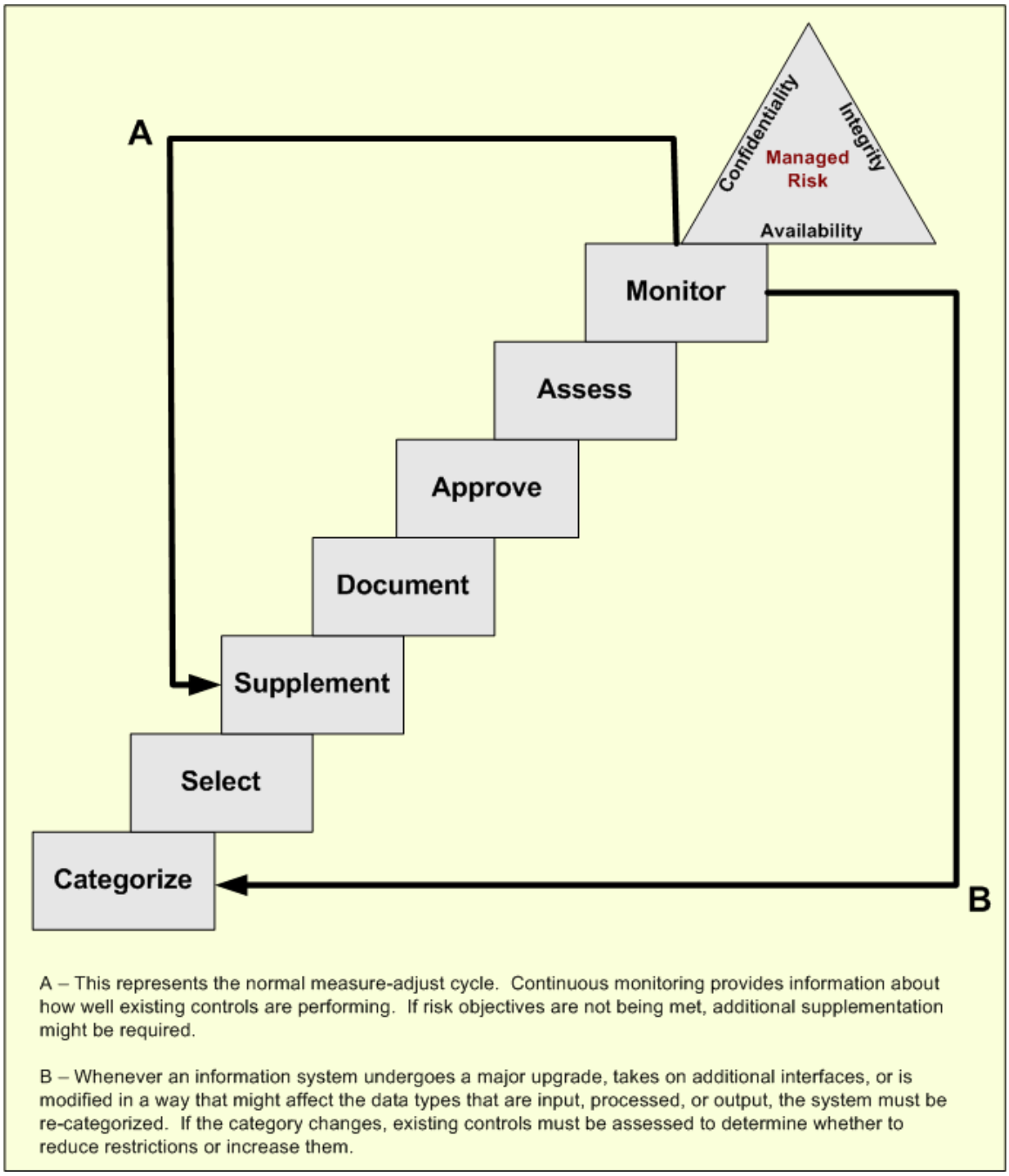

Figure 2: Risk Management Process

As I wrote in the introduction to this paper, this process targets risk in a specific information system. The assumption is made that organization- and enterprise-level controls are already in place. A complete list of potentially applicable security controls was compiled by Ross, et al, is found in NIST SP 800-53, Revision 1 (2007). In general, reasonable and appropriate controls should be applied to the following areas, and the overall organization/enterprise risks known, before performing the information system risk management process defined in this section:

- Support from all layers of management, including an organization security policy.
- Network assurance controls, including
  - Perimeter defense (e.g. firewalls)
  - Segmentation
  - Monitoring
  - Logical access controls
- Restrictions on physical access, including
  - Access control
  - Monitoring of access
- Administrative standards and guidelines, including
  - An acceptable use policy
  - User awareness training
  - Consistently applied sanctions for policy non-compliance
  - Enforcement of segregation of duties
- A documented and tested incident response process
- Regular auditing of policy compliance
- Third party security and risk assessments

Without the right higher-level controls in place, it's almost impossible to achieve any reasonable level of risk for individual systems. Which controls are necessary to achieve adequate network trustworthiness is one of the outputs of an organization- or enterprise-level risk assessment. Risk assessments at those levels are outside the scope of this paper but are covered in the NIST documentation.

I'll now step through each of the steps in the process shown in Figure 2.

Categorize the System

According to the NIST, categorization of the target system should take place as early as possible in the software or system development lifecycle (SDLC) (Stine, Kissel, Fahlsing, and Gulick, 2007, p. 5). Categorization of the system drives security requirements, which in turn determine design. The final result is a system into which security is built rather than hooked on—often as an afterthought.

System categorization is not a one time effort. The results of the initial assessment should be compared to system design as it emerges from technical and function reviews and modifications. Interfaces, processes, or stored data might change from the time the initial categorization was performed and the time comes to release the system into production.

The categorization process.

The NIST guidelines recommend breaking data down into data types and categorizing each data type. I disagree with this approach for a typical business. It introduces too much complexity into the assessment and categorization process. Instead, I step up a level looking at the most sensitive data moving through an interface or stored/processed by a server or endpoint device. This results in the application of the highest level of security controls necessary to each system component.

There are four components reviewed during system categorization: data input, data output, data processed, and data stored. It's clear from looking at these assessment targets that the system's level of risk is determined by the data passing through or stored.

The tool used to assess each of these components is a simple formula, depicted in Figure 3.

SC = Confidentiality Impact (CI), Integrity Impact (II), Availability Impact (AI)

Where CI, II, and AI are HIGH, MEDIUM, or LOW

Figure 3: Categorization Formula

SC is System Categorization—High, Medium, or Low. Confidentiality ensures that unauthorized personnel do not access the data. Data integrity is defined as the degree to which the business can rely on the accuracy of the information. Finally, the delivery of information to the users who need it, when they need it, falls within the area of availability. Impact is defined as the aggregate negative effect the compromise of confidentiality, integrity or availability would have on the business.

All data input, processed, output, or stored—payroll, protected health information, financials, employee, etc.—must be categorized. Let's step through an example.

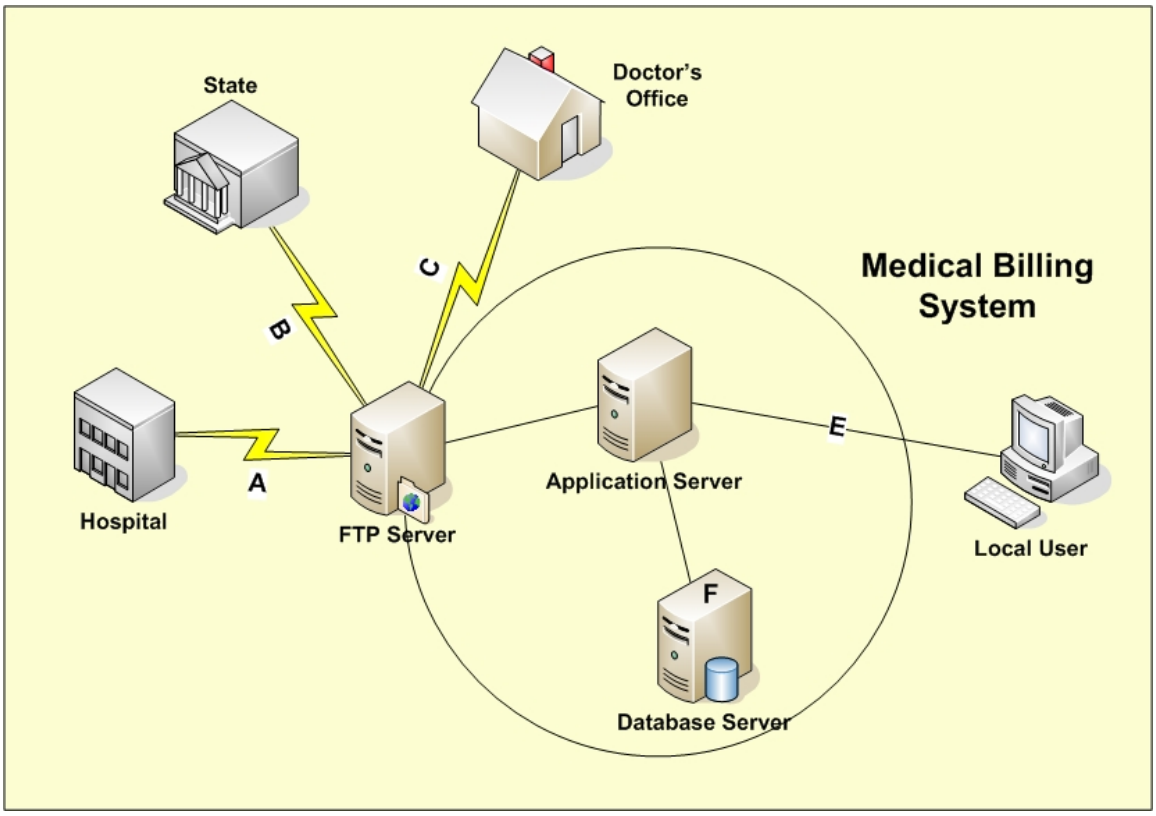

Figure 4: Sample System

Figure 4 is very simple representation of a Medical Billing System (MBS) for a long term care company. Note that "system" means all servers, endpoint devices, and other infrastructure that processes, stores, or in any way handles MBS information. This MBS consists of three external interfaces, three internal interfaces, three servers, and one endpoint device.

Using the system categorization formula shown in Figure 3, I'll step through two of the system's components. Before I do, remember that the categorization steps result in a business risk categorization that does not take into account any security controls. It's simply a measure of the business or personal impact that might result in the confidentiality, integrity, or availability of the data is compromised. The overall SC is an aggregate of the SCs of all system components.

We'll start with Interface A, the link to the hospital. This consists of results coming from the hospital's lab. For security purposes, the lab results are identified by a medical record number (MRN) only. No information that could be used to identify a patient outside the MBS is included (e.g. social security number, address, name, etc.).

Based on input from the data owner, we might arrive at the following interface categorization:

SC = (CI=Low), (II=High), (AI=High)

The overall SC of any system component is equal to the highest single impact rating. In this example, both II and AI have impact ratings of High. This makes the SC of this interface High.

Next, we'll look at Interface C. The same information is sent over this interface as is received from the Hospital over Interface A. However, there is one difference. Getting the lab results quickly into the hands of the facility caregivers is critical. The information provided to the doctor is largely informational. So, the data owner might decide to rate the three system impacts as follows:

SC = (CI=Low), (II=High), (AI=Low)

Note that the AI impact is Low for this interface. However, the overall AI for this system so far is still High. Why? Remember that the impact rating is equal to the highest single rating. This not only applies horizontally to the SC. It also applies vertically to each impact area. To clarify, refer to Table 1.

Table 1 is an example of a Microsoft Excel spreadsheet I use to calculate system categories.

System/ Interface	CI	II	AI	SC	Overall SC
MBS - App Server	H	H	M	H	
MBS - DB Server	H	H	M	H	
A	L	H	H	H	
B	H	H	M	H	
C	L	H	L	H	
E	H	H	M	H	
	H	H	H	H	High

Table 1: System Categorization Matrix

I filled in the cells corresponding to the server and interface names as well as the impact rating for each of the three impact areas. Let's look horizontally first, assessing the SC of each system component. In every row, CI, II, or AI is categorized as High. This results in an SC of High for every system component, as depicted in the SC column.

Working vertically, we can rank the overall confidentiality, integrity, and availability of the MBS. At least one component is ranked as High in the CI column. This results in a total system CI categorization of High. The same is true for II and AI.

The aggregate system categorizations for confidentiality, integrity, and availability are represented in the bottom, gray-shaded row. Since at least one of the areas (CI, II, or AI) is High, the overall system SC is HIGH. The same is true if you use the SC column that depicts the individual component rankings. So whether you use the component (horizontal) or categorization area (vertical), you'll still arrive as a system SC of High.

Because data can change and interfaces can be added or removed, IS should work with data owners to review the categories at pre-defined points in the SDLC process. For example, category reviews might be appropriate after requirements, after design, post system build, and post implementation.

Now that the system is properly categorized, it's time to select reasonable and appropriate security controls.

Select Controls

Security controls are the management, operational, and technical safeguards implemented to protect a network, individual systems, and the sensitive data that are processed, stored, or passed through them. For the purpose of this paper, I divided controls into two levels: organization and system.

Organization level controls apply to all systems and network components regardless of categorization. Examples of these types of controls—and a good place to start when applying baseline safeguards—are provided in Appendix A. The application of variations of these baseline controls across the organization creates the general security context into which engineers and developers implement individual business systems. Organization level controls should exist before system-specific controls are identified, supplemented, and implemented.

Control selection example.

System level controls are used to supplement those at the organization level. In this step in the information system risk management process, only baseline supplemental controls are selected. The NIST recommends that security designers and engineers use the process defined in NIST Special Publication 800-53A (Ross et al, 2007, p. 11). I'll use the Flaw Remediation control, as depicted in Figure 5.

ASSESSMENT PROCEDURE	
SI-2	**FLAW REMEDIATION** Control: The organization identifies, reports, and corrects information system flaws. Supplemental Guidance: The organization identifies information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws). The organization (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) promptly installs newly released security relevant patches, service packs, and hot fixes, and tests patches, service packs, and hot fixes for effectiveness and potential side effects on the organization's information systems before installation. Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling are also addressed expeditiously. Flaw remediation is incorporated into configuration management as an emergency change. NIST Special Publication 800-40, provides guidance on security patch installation and patch management. Related security controls: CA-2, CA-4, CA-7, CM-3, IR-4, SI-11.
SI-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies, reports, and corrects information system flaws;* *(ii) the organization installs newly released security patches, service packs, and hot fixes on the information system in a reasonable timeframe in accordance with organizational policy and procedures;* *(iii) the organization addresses flaws discovered during security assessments, continuous monitoring, or incident response activities in an expeditious manner in accordance with organizational policy and procedures;* *(iv) the organization tests information system patches, service packs, and hot fixes for effectiveness and potential side effects before installation; and* *(v) the organization captures all appropriate information pertaining to the discovered flaws in the information system, including the cause of the flaws, mitigation activities, and lessons learned.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** Examine: [SELECT FROM: System and information integrity policy; procedures addressing flaw remediation; NIST Special Publication 800-40; list of flaws and vulnerabilities potentially affecting the information system; list of recent security flaw remediation actions performed on the information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct information system flaws); test results from the installation of software to correct information system flaws; other relevant documents or records]. (L) (M) (H) Interview: [SELECT FROM: Organizational personnel with flaw remediation responsibilities]. (M) (H)

Figure 5: Baseline Flaw Remediation Control, NIST SP 800-53A (p. F-263)

The various controls are divided into families. The family to which a control belongs is indicated by the first two letters of the control code. In this example, SI represents the System and Information Integrity family. The number following the two letter family identifier represents a specific control within the family, with multiple assessment objectives identified with a dot-number qualifier. The control we're evaluating in this example is SI-2, Flaw Remediation.

All controls included in 800-53A consist of a baseline assessment procedure that includes a control statement, supplemental guidance and a set of assessment objectives to ensure compliance. The control statement is the overall outcome an organization is hoping to achieve. Supplemental guidance is provided to help put the control statement into

context, further define scope, and to list other controls that are affected by or impact this control. Assessment objectives are used to test the effectiveness of the control.

The level of compliance and the methods for evaluating control objectives are determined by the system's classification: high, medium, or low. Recommendations are provided in the Potential Assessment Methods and Objects section at the bottom of the procedure box: (L) = Low, (M) = Medium, (H) = High. In our example, examination of artifacts is considered sufficient for systems classified as Low or Medium. In addition to artifact assessments, interviews are recommended for systems classified as High.

Again, these are simply recommendations. The data owners and executive management must decide what constitutes reasonable and appropriate diligence.

Many controls, like our sample, also include enhancements. See Figure 6. Unlike the baseline control, control enhancements typically apply to Medium or High classifications only. For example, Flaw Remediation has two enhancements listed. The first, SI-2(1), is recommended only for systems classified as High. Enhancement SI-2(2) is intended for Medium or High systems.

Whether an organization applies control enhancements depends on the sensitivity of the data and the criticality of the systems. However, all baseline controls listed in Appendix A should be applied to some degree.

It can be a tedious task combing through the entire list of controls contained in 800-53A every time a system is designed or implemented. Organizations should integrate control application/selection into existing design and build procedures. To assist with these new tasks, control checklists can be helpful. See Appendix B for a sample, downloadable tool.

ASSESSMENT PROCEDURE	
SI-2(1)	**FLAW REMEDIATION** Control Enhancement: **The organization centrally manages the flaw remediation process and installs updates automatically.**
SI-2(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization centrally manages the flaw remediation process and installs updates automatically.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [SELECT FROM: System and information integrity policy; procedures addressing flaw remediation; automated mechanisms supporting centralized management of flaw remediation and automatic software updates; information system design documentation; information system configuration settings and associated documentation; list of information system flaws; list of recent security flaw remediation actions performed on the information system; other relevant documents or records]. (H) **Test**: [SELECT FROM: Automated mechanisms supporting centralized management of flaw remediation and automatic software updates]. (H)
SI-2(2)	**FLAW REMEDIATION** Control Enhancement: **The organization employs automated mechanisms to periodically and upon demand determine the state of information system components with regard to flaw remediation.**
SI-2(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to periodically and upon demand determine the state of information system components with regard to flaw remediation.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [SELECT FROM: System and information integrity policy; procedures addressing flaw remediation; automated mechanisms supporting flaw remediation; information system design documentation; information system configuration settings and associated documentation; list of information system flaws; list of recent security flaw remediation actions performed on the information system; information system audit records; other relevant documents or records]. (M) (H) **Test**: [SELECT FROM: Automated mechanisms implementing information system flaw remediation update status]. (M) (H)

Figure 6: Enhanced Flaw Remediation Control, NIST SP 800-53A (p. F-264)

Supplement Controls

The controls identified in the previous step are considered baseline controls. They are selected by comparing the system category to NIST recommendations. In this step, these minimum controls are reviewed within the context of the system's actual operating environment. Controls might be increased, decreased, removed, or modified. The existence or lack of compensating controls plays a major role in this process. Network diagrams and threat models are two tools used to identify system weaknesses that still exist after baseline controls are applied (Olzak, 2006, March).

Another approach to strengthening baseline controls is the implementation of system use restrictions. The following are a list of controls you might consider when assessing the efficacy of system access and use safeguards:

- Limiting the information a system can process, store, or process;
- Assessing the manner in which a business process is automated;
- Prohibiting external information access to critical organizational information by removing selected system components from the network; and
- Prohibiting moderate or high impact information on publicly accessible network components unless there is a compelling business need, and the data owner—having been made aware of all associated risks—provides approval.

The control supplementation process is summarized in Figure 7.

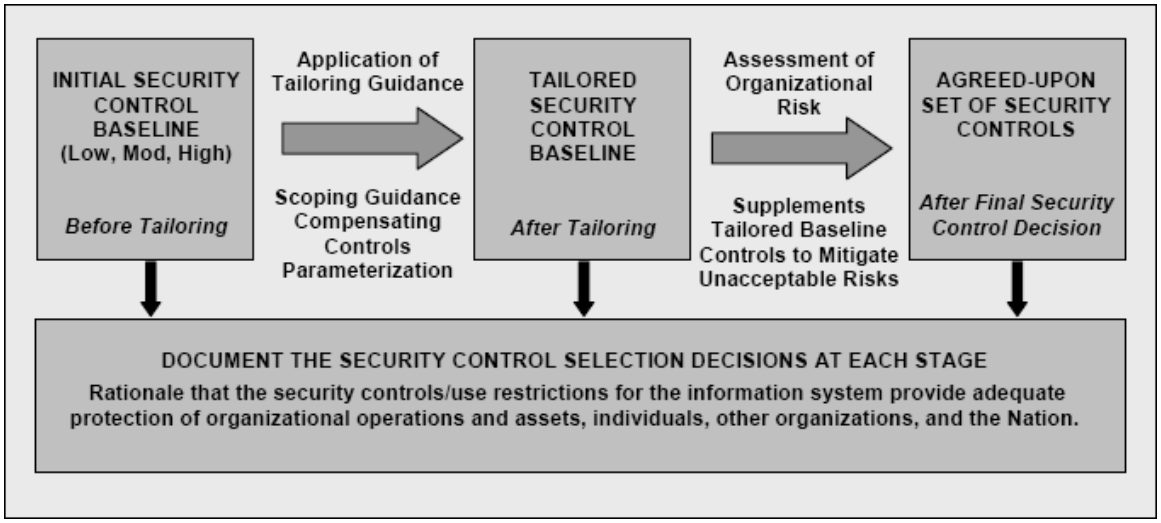

Figure 7: Security Control Selection and Supplementation
(Ross et al, NIST SP 800-39, p. 27)

Documentation

Documentation, the bane of most if not all technical people, is a critical piece of the risk management process. As depicted in Figure 7, documentation is required after each step of the control selection and supplementation process. The controls documentation builds on documents created during the categorization step.

The need for documentation is often perceived as an activity required to guide engineers through a future rebuild of the environment. However, risk management documents are much more. They should include the following (Ross et al, NIST SP 800-39, p. 28):

- Complete coverage of security controls in appropriate security plans to facilitate:
  - More comprehensive information security;
  - Increased accountability; and
  - An effective vehicle for management to better manage risk;
- Documentation of control selection and supplementation process, including:
  - The rationale behind base and supplemental control selection;
  - Cost verses effectiveness tradeoffs; and
  - Constraint verses operational effectiveness tradeoffs;
- A documented plan, including
  - Documentation from previous steps (e.g. network diagrams and attack trees);
  - Control placement; and
  - How new controls or changes to existing controls will integrate with enterprise-level controls.

Properly completed, the documentation process produces security plans that are used to organize and manage the security activities for information systems organization-wide, including;

- Individual system plans;
- Network plans; and
- Control integration/effectiveness assessments based on best practices, such as defense-in-depth and diversity-in-design.

When the documentation is complete, including review and acceptance by all technical and data owner stakeholders, it's ready for presentation to management for approval.

Approve

The purpose of a risk assessment is to provide management with the information needed to decide whether to accept, mitigate, or transfer risk. So the purpose of the approval step is to present management with the story behind the proposed controls, including:

- The criticality of the system in isolation and as an integral part of the overall information processing and delivery support for daily operations;
- The threats currently expected against the industry in which the organization operates as well as general threats across all industries;
- The probability that each threat or class of threats would attempt an attack and the effort human threats would be willing to apply to reach system data;
- The controls already present in the system's proposed operating environment, and the resulting risk mitigation and risk gaps;
- A description of recommended baseline controls and how they further mitigate risk;
- A description of the recommended supplemental controls that finally reduce risk to an acceptable level; and
- A description of how the controls will be managed and the responsible parties.

An important point many security and risk managers miss is that this is a sales presentation with the explicit purpose of convincing management that they should spend their dollars on security controls instead of other business-related—and often revenue-producing—projects. A successful presentation results in final management approval of A system security plan, including acceptance of remaining risk, and a plan of action, including milestones.

Implement

The project to implement the approved security controls is no different than any other information technology project. In fact, control implementation project activities and tasks should be included in the overall system design and build project plan. Running controls implementation as a separate project could result in security being considered as an add-on rather than as an integral part of the system's build, testing, and move to production.

Assess

Once controls are implemented, their effectiveness must be assessed. Assessments can take the form of internal or external audits, third party risk assessments, post implementation reviews, or other processes that fit into an organization's security and operational model. Whatever form an assessment takes, its purpose is to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome (i.e. reducing risk to an acceptable level without serious impact on operations).

Assessments should use some standard of best practice as a baseline against which to measure. This is easy when using NIST SP 800-53A. As shown in Figures 5 and 6, the objectives that should be met are clearly documented. Further, the documentation created during the baseline and supplemental control selection steps should include expected outcomes. It is these objectives and expected outcomes that form the framework within which an assessment is performed.

The results of an assessment must include an overall audit of risk, including system-level and organization-level controls and safeguards. Assessing a system in isolation from supporting higher-level controls will not provide an accurate picture of the potential for data compromise.

Monitor

The final step in the information system risk management cycle is to monitor administrative, technical, and physical activities that directly or indirectly affect the target system's confidentiality, integrity, or availability.

Well-designed monitoring processes and technologies provide an organization with effective tools for producing ongoing updates to information systems, security plans, security assessment reports, and plans of action and milestone documents (Ross et al, 2007, NIST SP 800-39, p. 32). Examples of monitoring activities include:

- Change management. The purpose of change management is to implement changes to production without an interruption in information services delivery—without breaking stuff. This includes not inadvertently increasing risk.
- Contract management. All contracts involving the processing of sensitive information by third parties must include clear expectations for how the data is to be handled and the controls that are to be implemented and managed. Contracts should also include an agreement by the outside entity to allow periodic reviews of security outcomes.
- Ongoing assessments of selected security controls. The purpose and intended outcome of these assessments are described in *Assess* above.
- Security status reporting to appropriate management representatives in the form of:
    - Audits
    - Results of third party assessments
    - Investigations and inquiries

- Incident response reports

An important factor to consider when planning monitoring is security control volatility. This is the measure of how frequently a control is likely to change over time. The level of volatility will determine the frequency with which monitoring results are reviewed, the length of time logs must be archived, and how closely controls must be assessed during system changes.

Conclusion

Mitigated and acceptable business and personal risk are the most important outcomes of information system security activities. It means that the confidentiality, integrity, and availability of a system and the data associated with it are protected with reasonable and appropriate controls—controls that protect without placing unreasonable constraints upon operational activities.

Managing risk is an ongoing activity that consists of multiple steps. Each of these steps includes specific tasks that support the overall risk management effort. In this paper, the NIST risk management documents formed the basis for our discussion of what constitutes an effective risk management process, starting with NIST SP 800-39.

Tom Olzak, MBA, CISSP, MCSE, is President and CEO of Erudio Security, LLC.

He can be reached at tom.olzak@erudiosecurity.com
Check out Tom's book, Just Enough Security
Additional security management resources are available at http://adventuresinsecurity.com
Free security training available at http://adventuresinsecurity.com/SCourses

---

Works Cited

Olzak, T. (2006). *Just enough security*. Toledo, Ohio: Erudio Security, LLC.

Olzak, T. (2006, March). *A practical approach to threat modeling*. Retrieved January 28, 2008 from http://adventuresinsecurity.com/blog/wp-content/uploads/2006/03/A_Practical_Approach_to_Threat_Modeling.pdf

Olzak, T. (2007, November). *Managing security is a balancing act.* Retrieved December 20, 2007 from http://blogs.ittoolbox.com/security/adventures/archives/managing-security-is-a-balancing-act-20349

Ross, R., Katzke, S., Johnson, A., Swanson, M., Stoneburner, G., & Rogers, G. (2007). *Recommended security controls for federal information systems, final public draft*, NIST SP 800-53A, Retrieved January 4, 2008 from http://csrc.nist.gov/publications/drafts/800-53A/draft-SP800-53A-fpd-sz.pdf

Ross, R., Katzke, S., Johnson, A., Swanson, M., & Stoneburner, G. (2007). *Managing risk from information systems: an organizational perspective (draft)*, NIST SP 800-39, Retrieved January 2, 2008 from http://csrc.nist.gov/publications/drafts/800-39/SP-800-39-ipd.pdf

Stine, K., Kissel, R., Fahlsing, J, & Gulick, J. (2007). *Volume 1: guide for mapping types of information and information systems to security categories (draft)*, NIST SP 800-60 (V1). Retrieved January 8, 2008 from http://csrc.nist.gov/publications/drafts/800-60-rev1/draft-SP800-60_Volume1-Revision1.pdf

Appendix A

FIPS 200 Minimum Security Requirements

(http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf)

Access Control (AC): Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

Awareness and Training (AT): Organizations must: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Audit and Accountability (AU): Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

Certification, Accreditation, and Security Assessments (CA): Organizations must: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Configuration Management (CM): Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.

Contingency Planning (CP): Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

Identification and Authentication (IA): Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

Incident Response (IR): Organizations must: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.

Maintenance (MA): Organizations must: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

Media Protection (MP): Organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.

Physical and Environmental Protection (PE): Organizations must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

Planning (PL): Organizations must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

Personnel Security (PS): Organizations must: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

Risk Assessment (RA): Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

System and Services Acquisition (SA): Organizations must: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

System and Communications Protection (SC): Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

System and Information Integrity (SI): Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

Appendix B

System Controls Worksheet

(http://adventuresinsecurity.com/Tools/SystemControls.xls)

The System Controls Worksheet—a Microsoft Excel file downloadable at the link listed at the top of this page--consists of a subset of the controls listed in NIST SP 800-53. I used only the system-level controls. When using this template, the assumption must be made that organization- and enterprise-level controls are already operational. Further, the target system should already have an assigned security category.

The following is a portion of the worksheet.

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	**Security Control Requirements Worksheet**												
2	**System Name:**												
3	**System Category:**												
4	**Security Analyst:**												
5	**Date Completed:**												
6													
7	**Control #**	**NIST Control Description**					**Complies**	**Implement**	**Risk**	**Comments**			
8	AC-3	The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy											
9		The information system restricts access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel											
10	AC-4	The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policies											
11	AC-5	The information system enforces separation of duties through assigned access authorizations											
12	AC-6	The information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks											
13	AC-7	The information system enforces a limit of 5 consecutive invalid access attempts by a user. The information system automatically locks the account for a period specified by management (at least 5 minutes) when the maximum number of unsuccessful attempts is exceeded											

The template is not protected so you can make changes. However, all cells are already flagged so that protecting the worksheet results in user access to data entry fields only (highlighted in yellow and red). Sorting and filtering the controls based on information contained in the red columns can provide a prioritized list of controls to be implemented.

Although you can use whatever flags work in your environment, I use **Y/N** in *Complies* and Implement. I use **L**(ow), **M**(edium), or **H**(igh) in the *Risk* column.