Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

# Security Program Management and Risk

Information security should be managed as a program that requires the same degree of attention and responsibility as other resourced programs within an organization. This paper argues for building a security management program on a foundation of business risk assessment and risk management. It defines and explains risk, risk assessment, risk management and relates business risk management to security risk management. A synopsis of the steps in risk management and guidance on the key components for effectively implement...

Copyright SANS Institute
Author Retains Full Rights

AD

# Security Program Management and Risk

Archie D. Andrews Jr.

GIAC Security Essentials Certification Practical Assignment Version 1.4b

March 23, 2003

## *Abstract*

Information security should be managed as a program that requires the same degree of attention and responsibility as other resourced programs within an organization. This paper argues for building a security management program on a foundation of business risk assessment and risk management. It defines and explains risk, risk assessment, risk management and relates business risk management to security risk management. A synopsis of the steps in risk management and guidance on the key components for effectively implementing a security risk management program into an enterprise is provided. The reader should have a fuller understanding of the best practices associated with risk assessment and risk management and be able to use risk analysis to communicate with business process owners in terms of the risks to confidentiality, integrity, and availability in their areas of concern.

## *Introduction*

A recent report from the United Stated General Accounting Office [DAC02] found that all 24 Major Federal Agencies had significant weaknesses in security program management. In the testimony to congress that conveyed that finding, Robert Dacey, the Director for Information Security Issues within the GAO, explained security program management as the framework for ensuring that risks are understood and effective controls are selected and properly implemented. He asserted that security program management is fundamental to the appropriate selection and effectiveness of information security control categories e.g., access, software change, segregation of duties, system software, and service continuity. He also testified that no federal agency was doing a good job of managing their respective security programs. While the GAO report was specifically directed toward federal agencies, the principle of treating security as a program that required effective management is applicable to all organizations that rely on information technology for their competitive edge or their survival.

Security program management covers a range of activities; it is based on the foundation of understanding information security risks, selecting and implementing controls commensurate with the risk, and ensuring that controls, once implemented, continue to operate effectively. The integration of identifying and assessing risks into the management procedures and the organizational culture is essential for security program


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

management. This should not be news; assessing and managing (or accepting) risks are commonly accepted business practices throughout effective organizations. In the most basic terms, risk management includes assessing which assets are critically important to the organization, what threats may impact those critical assets, what risks to the organization evolve if those threats are realized, and how to manage, mitigate, or accept the identified risks.

Risk assessment and risk management are not single shots but rather are continuous processes repeated as a cycle of identifying risks, creating plans to address those risks, acting on those plans, and monitoring the results of the actions. This paper will examine the relationship of risk and risk management to an effective security management program.

## *Business Risk Management*

Almost all business decisions need grounding in the potential cost of inaction compared to the cost of actions to reduce the risks. Risk is simply the possibility of suffering harm of loss. More formally, risk is the net negative impact of the exercise of vulnerability, considering both the probability and the impact of the occurrence [STO01]. Risk is a function of a threat-source's exercising a particular vulnerability, and the resulting impact on the organization. Risk assessment is widely used to support decision-making processes. (Note: a risk assessment should not be confused with a vulnerability assessment. A vulnerability assessment/analysis is a critical part in any security risk assessment but it only a part. A vulnerability assessment generally focuses on discovering and diagnosing technical vulnerabilities in the systems under inspection.) The critical aspect of any risk assessment is that it ties a threat or vulnerability to a business asset or process. Employing risk assessment methodologies allows consistent and effective use of decision support data as well as removal of technical bias from what are essentially business decisions.

Risk management can be loosely defined as a systematic process for the identification, analysis, control and communication of risks, and taking steps to reduce risk to an acceptable level. Risk management methodology supports the making of informed decisions about the allocation of scarce resources appropriate to the risk exposure. A risk management program must entail identification of key assets whose loss or degradation would adversely impact the organization's capabilities, potential vulnerabilities that may be exploitable, threats to those key assets or to the organization as a whole, and decisions on how to address identified vulnerabilities, risks, and threats.

Every organization needs a set of management procedures and an organizational framework for identifying and assessing risks, deciding what policies and controls are needed, periodically evaluating the effectiveness of these policies and controls and acting to address identified weaknesses. These fundamental activities allow an organization to manage risks throughout the business rather than reacting to individual problems in an ad-hoc manner only after a problem has been detected or an audit finding reported.


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

All business decisions, in IT or otherwise, are an exercise in the evaluation of the risk of inaction versus the cost of action to reduce risks (real or perceived). A risk-management process helps to prioritize issues to allow effective use of finite resources. Most businesses need to take some risks to gain a competitive edge. Risk-management enables sound judgment when taking risks because it provides a process for thinking through possible consequences and deciding on appropriate strategies to deal with the risks. Risk management pulls together data from other areas, such as vulnerability analysis and operations monitoring, to provide an overall view of business risk. It also usually affords a level of contingency planning should a risk become a reality.

An often overlooked key advantage of risk management is the provision of a common language for the IT leader and the business decision maker to communicate needs, wants, and resource requirements. If properly used, risk management can address the rationale for investment in information security in terms that are familiar and supportable to the business process owner who must deal with competing resource requirements.

The primary goal of any security program should be to protect the organization and its ability to perform the organization's mission, not just organizational IT assets. Therefore the risk management process must not be treated primarily as a technical function carried out by the IT experts who operate and manage the IT system, but rather as an essential management function of the organization. Virginia Tech, in their guidance to all University Departments using information resources, acknowledged and reinforced the link between the mission concerns and the information security concerns by renaming their risk assessment procedures to the "Business Impact Analysis / Risk Assessment for Information Assets" [VIR00]. By recognizing and integrating business considerations into the risk program associated with information security, the process and the practices resulting from risk management decisions are enhanced.

## *Security Risk Management*

The objective of performing security risk management is to enable the organization to accomplish its mission(s) by securing the IT systems that store, process, or transmit organizational information; by enabling well informed risk management decisions to justify the expenditures that are part of an IT budget; and by assisting management in authorizing (or accrediting) the IT systems on the basis of the supporting documentation resulting from the performance of risk management.

Security risk management is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations' missions.

IT security spending must be reviewed as thoroughly as other management decisions. A well-structured risk management methodology, when used effectively, can help management identify appropriate controls for providing the mission-essential security capabilities.


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

As Allen points out [ALL01], systems, networks, and sensitive information can be compromised by malicious and inadvertent actions despite an administrator's best efforts. Even when administrators know what to do, they often don't have the time to do it; operational day-to-day concerns and the need to keep systems functioning take priority over security of those systems. Administrators choose how to protect assets, but when managers are unable to identify which assets are the most critical and the nature of threats against them (as part of a business strategy for managing information security risk), the protection an administrator offers are likely to be arbitrary.

Establishing a strong security management program requires that organizations take a comprehensive approach that involves both senior program mangers who understand which aspects of their missions are the most critical and sensitive and technical experts who know the agencies systems and can suggest appropriate technical security control techniques.

## *Regulatory Requirements*

The United States government, in recognition of the importance of security management processes, has mandated the establishment of formal security management in the healthcare industry under the auspices of the Healthcare Insurance Portability and Accountability Act of 1996, commonly referred to as HIPAA. In February 2003, the Department of Health and Human Services released the final security rules for protection of health information created or maintained by "covered entities," (i.e., healthcare providers who engage in electronic transactions and their associated business partners such as health plans) [HIP03]. The government recognized that one of the limiting factors toward wide acceptance of potential technological improvements has been and is the danger and concerns associated with securing private and confidential information within the healthcare industry.

The security management process as defined in [HIP03] CFR 164.308, includes requiring implementation of risk analysis, and risk management as key components. While these formal rules apply to a specific industry, they compose a well-reasoned set of security practices and as such should be considered commonly accepted best practices. In the future the courts may find this rule set to be the standard against which the actions of other industries are measured to show due diligence for protecting the privacy, confidentiality, integrity, and availability of information within that organization's care.

If the goal of an organization's security management program is a clear understanding between IT staff (and/or the information security staff) and business decision makers on systems essential to the organization's success; the security required for those systems in terms of integrity, confidentiality, and availability; the resources, policies and controls that the organization decides to put in place to provide the required level of protection; and the process for monitoring and evaluating the effectiveness of those decisions – then the best, most effective way to meet those goals is to implement security risk assessment and risk management process.


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

## *Steps of Risk Assessment and Risk Management*

Recognizing that security risk assessment and the resulting management activities are a significant part of a security program, how does one proceed?

There are several viable risk assessment processes, e.g., [ALB00], [PAU00], [STO01]. These various approaches can be distilled into interrelated steps: develop an inventory of systems to focus on based on the business processes they support; assess the potential threat and vulnerability of the systems identified for investigation; decide to act or to accept; evaluate the effectiveness of the action; communicate decisions made; and monitor the effect.

**Phase One: Systems inventory** – designating the assets involved in support of critical business processes. Although there may be a temptation to be as comprehensive in defining the systems to investigate, there is a real risk of overwhelming the effort while gaining little. The OCTAVE process as defined by the Software Engineering Institute [ALB00] recommends beginning by defining those assets most critical to the continued accomplishment of the organization's mission. To determine a system's criticality to the organization's mission it is essential to go beyond the IT staff and involve business process owners and decision makers. Involving these key stakeholders in the business aspects of the organization will answer the questions about criticality of the business processes. Virginia Tech, in their process description for risk assessments [VIR00] recommends classifying the assets under investigation into three categories: (1) Critical – the organization cannot operate with this asset even for a short period of time; (2) Essential – the organization could work around lose of the information asset for days or perhaps a week, but eventually the information asset would have to be returned for use; (3) Normal – the organization can operate without this information asset for an extended (though finite) period of time during which units or individuals may be inconvenienced and/or need to identify alternatives.

Understanding the organization's critical mission leads back to the essential system components that support those business processes and so define the focus of the systems to be examined. Additionally, engaging the appropriate business-process owner in the risk assessment will transfer the focus of the risk assessment from IT to business continuity and build buy-in for the resulting recommendations. By forcing the decision as to which systems are most critical to the organization, the analysis and resultant recommendations are justifiably focused on high impact assets. The analysis and recommendations will by definition address the most critical contributors to the organization's mission; they will also address those risks that are shared throughout the organization.

**Phase Two: Threat Analysis** – identifying the potential threats to the critical systems. For this phase to have legitimacy, it must also involve business process owners and business process users. They are the ones who can recognize and appreciate the threats that have a strong likelihood of adversely affecting their ability to accomplish their critical functions. By using a cross section of the organization, from


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

senior management and business process owners to business process users, insights into possible threats are shared across normal organizational barriers.

**Phase Three: Infrastructure Vulnerability Assessment** – identifying technology vulnerabilities that can be exploited. Once the target systems for investigation have been identified, the process should turn to internal or external system experts to examine the IT systems for weaknesses that could be exploited and to determine the likelihood of someone attacking those weaknesses. This investigation should lead to a list of actions to correct. Many will be correctable on the spot but they should still be documented as a measure of the health of the systems and the need for documented security practices. Some of the vulnerabilities may not be immediately correctable but the process will document and recognize these vulnerabilities for subsequent risk management decisions.

**Phase Four: Develop security control recommendations** - link the results of the assessment to risk-management strategy recommendations. The first three phases gives you a measure of risk, threats, and vulnerabilities and an understanding of how these impact the business of the organization. The risk-analysis process should lead the organization to not only controlling risk, but also defining residual risk. Controls are aimed at mitigating recognized risks to levels acceptable to the business. Implementation is a risk/value proposition because all controls have associated cost. Costs associated with operations and maintenance, and those related to usability, scalability, and performance. Evaluating controls based on business risk lets you establish a coherent plan for risk mitigation as opposed to point solutions aimed at technical challenges.

**Phase Five: Decision** – acting on risk-management recommendations. Risk assessment provides information to support business decisions. The assessment should produce recommendations for strategic and tactical action plans. It is critical that business process owners are responsible for the decision phase; with the advice of IT and security personnel, informed decisions can be made with a focus on ensuring continuation of business critical assets and processes. Possible decisions are to accept the risk (do nothing), mitigate the risk (implement controls), or transfer the risk (buy insurance). The decision to implement controls should be based on the business value it adds. Risk management is not a goal in itself; information should be protected only in support of a business need or requirement. Such requirements should be spelled out in information security policies. Risk assessment builds a linkage between business needs and the security program. Onerous decisions that result in a negative impact on the business practices, real or perceived, are best made in an informed manner and then documented and communicated.

**Phase Six: Communication and monitoring**. User and management buy-in are critical to successful implementation of control. The theme of engaging the business in the analysis of technical risk is carried through to the final stages of the process by making sure that risk-assessment results are communicated to business-process


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

owners as well as end users and the results, both positive and negative, are monitored and assessed for net effect.

## *Risk Management Cycle*

Reacting to the steps of risk management defined above, the reader will realize that the risk assessment process is a continuous cycle. In fact in May 1998, the U.S. Government Accounting Office issued a report summarizing their study of the practices of organizations with superior security programs [GAO98]. That study found that those organizations managed their information security risks through a cycle of risk management activities that include:

- Assessing risks and determining protection needs,
- Selecting and implementing cost-effective policies and controls to meet these needs,
- Promoting awareness of policies and controls of the risks that prompted their adoption among those responsible for complying with them, and
- Implementing a program of routine tests and examinations for evaluating the effectiveness of policies and related controls and reporting the resulting conclusions to those who can take appropriate corrective action.

One can see that this cycle is not new. It is based on the “plan-do-check-act” cycle of almost any well-defined business process. In the case of security risk management the cycle becomes assess, plan, implement, monitor, control [ALB01].

Implementing a continuous cycle of well organized risk management activities performed by a competent risk assessment team is the key to ensuring that information security risks are adequately considered and addressed on an ongoing, organization wide basis. The Government Accounting Office in [GAO02] recommends that organizations:

- Conduct risk assessments for all their systems;
- Establish information security policies and procedures that are commensurate with risk and that comprehensively address significant threats;
- Provide adequate computer security training to their employees;
- Test and evaluate controls as part of their management assessments;
- Implement documented incident handling procedures; and
- Identify and prioritize their critical operations and assets and determine the priority for restoring these assets should a disruption in critical operations occur.

## *Conclusions*

Poor security management leads to organizations who:

- Are not fully aware of the information security risks to their operations,


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Accept an unknown level of risk by default rather than consciously deciding what level of risk was tolerable,
- Have a false sense of security because they were relying on ineffective controls,
- Deal with security on an ad-hoc reactive basis, or
- Cannot make informed judgments as to whether they were spending too little or too much of their resources on security.

This paper argues for a well reasoned, planned and somewhat orchestrated approach to information security risk management. That approach should be founded on an information security risk assessment methodology that engages senior management and the IT staff and provides them with a common language to discuss and reason about the tough decisions about allocating resources to information security.

A successful risk management program will rely on management procedures and an organizational framework for identifying and assessing risks, deciding on needed policies and controls, evaluating the effectiveness of policies and controls, and acting to respond to identified weaknesses. The organization with well-defined processes that involve both senior managers for their understanding of the critical missions and technical experts for their ability to recommend security controls should be able to forge a competent risk assessment team. That team must have the expertise and experience to apply the risk assessment methodology to specific sites and systems, identify mission risks, and provide cost effective safeguards that meet the needs of the organization. To implement an effective security management program will also require the awareness and cooperation of the organization's user community, who must follow procedures and comply with the implemented controls to safeguard the mission of their organization. The final ingredient of the risk assessment cycle is an ongoing evaluation and assessment of the IT-related mission risks.

The immediate advantages to an organization from application of information security risk analysis and assessment methods include identification of the organization's important assets, potential threats against these assets, security requirements for these assets, and weaknesses or vulnerabilities in current practice that increase the likelihood of these assets being compromised. Armed with this understanding the management and IT staff can make reasonable decisions focusing attention on priority assets.

## References:

[ALB01] Alberts, Christopher J., and Audrey J. Dorofee; OCTAVE Criteria, Version 2.0 CMU/SEI-2001-TR-016, December 2001; http://www.sei.cmu.edu/publications/documents/01.reports/01tr016.html

[ALL01] Allen, Julia; The CERT Guide to System and Network Security Practices. Reading, MA: Addison-Wesley, 2001

[DAC02] Dacey, Robert F.; "Progress Made, But Critical Federal Operations and Assets Remain at Risk," GAO Testimony before the House Subcommittee on Government


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Efficiency, Financial Management and Intragovernmental Relations; November 19, 2002; http://www.gao.gov/new.items/d03303t.pdf

[HIP03] Department of Health and Human Services, Office of the Secretary; 45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards, Final Rule; http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2003/pdf/03-3877.pdf

Litzau, David; "Risk Management: A Foundation for Information Security," June 7, 2001; http://rr.sans.org/audit/risk_manage.php

Koss, Shannah; "Getting Ready for HIPAA Security Requirements" Chapter 3, *The 2000 Guide to Health Data Security*, IBM Inc.,

Nichols, Arthur; "A Perspective on Threats in the Risk Analysis Process," August 31, 2001; http://rr.sans.org/audit/risk_analysis.php

[PAU00] Paul, Brooke; "Risk Assessment Strategies," Oct 30, 2000; http://www.networkcomputing.com/1121/1121f3.html

Piepers, Eric; "Cost-effective Information Security (Information Security from a Business Perspective)," June 6, 2001; http://rr.sans.org/audit/cost-effective.php

Rajasingham, Prabhacker; "Threat and Risk Assessments: SOME Issues," April 10, 2001; http://rr.sans.org/audit/risk.php

[STO01] Stonebrunner, Gary, Alice Goguen, and Alexis Feringa; NIST Special Publication 800-30, "Risk Management Guide for Information Technology Systems", October 2001, http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.prf

[GAO98] United States General Administration Office; "Information Security Management: Learning from Leading Organizations," GAO/AIMD-98-68; http://www.gao.gov/archive/1998/ai98068.pdf

[VIR00] Virginia Tech; "Business Impact Analysis / Risk Assessment for Information Assets, General Information and Process Description"; Revised: December 2000; http://security.vt.edu/playitsafe/riskanalysis/RA-Dept01-MST-Blk.doc


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: June 19th, 2013

# Upcoming SANS Training

**Click Here for a full list of all Upcoming SANS Events by Location**

| | | | |
|---|---|---|---|
| **Digital Forensics & Incident Response Summit 2013** | **Austin, TXUS** | **Jul 09, 2013 - Jul 16, 2013** | **Live Event** |
| **SANS London Summer 2013** | **London, GB** | **Jul 09, 2013 - Jul 16, 2013** | **Live Event** |
| **SANS Rocky Mountain 2013** | **Denver, COUS** | **Jul 14, 2013 - Jul 20, 2013** | **Live Event** |
| **SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification** | **Washington, DCUS** | **Jul 22, 2013 - Jul 26, 2013** | **Live Event** |
| **SANS Mumbai 2013** | **Mumbai, IN** | **Jul 22, 2013 - Jul 27, 2013** | **Live Event** |
| **SANS San Francisco 2013** | **San Francisco, CAUS** | **Jul 29, 2013 - Aug 03, 2013** | **Live Event** |
| **SANS Boston 2013** | **Boston, MAUS** | **Aug 05, 2013 - Aug 10, 2013** | **Live Event** |
| **SANS SEC 560: Network Penetration Testing @ Bangalore 2013** | **Bangalore, IN** | **Aug 05, 2013 - Aug 10, 2013** | **Live Event** |
| **Critical Security Controls Summit** | **Washington, DCUS** | **Aug 12, 2013 - Aug 18, 2013** | **Live Event** |
| **Industrial Control Systems Security Training - DC** | **Washington, DCUS** | **Aug 12, 2013 - Aug 16, 2013** | **Live Event** |
| **SANS Virginia Beach 2013** | **Virginia Beach, VAUS** | **Aug 19, 2013 - Aug 30, 2013** | **Live Event** |
| **SANS Thailand 2013** | **Bangkok, TH** | **Aug 19, 2013 - Aug 31, 2013** | **Live Event** |
| **SANS Melbourne 2013** | **Melbourne, AU** | **Sep 02, 2013 - Sep 07, 2013** | **Live Event** |
| **SANS Capital City 2013** | **Washington, DCUS** | **Sep 03, 2013 - Sep 08, 2013** | **Live Event** |
| **Network Security 2013** | **Las Vegas, NVUS** | **Sep 14, 2013 - Sep 23, 2013** | **Live Event** |
| **SANS Canberra 2013** | **OnlineAU** | **Jul 01, 2013 - Jul 13, 2013** | **Live Event** |
| **SANS OnDemand** | **Books & MP3s OnlyUS** | **Anytime** | **Self Paced** |