Security Review Alternatives

by Jennifer L. Bayuk

Information security awareness is at an all-time high. Businesses that contract with information service providers wonder whether their data is secure. Corporate lawyers are concerned with regulatory compliance. Chief information officers (CIOs) are insisting that security be addressed during the systems development lifecycle. Requests for security reviews are proliferating. Everyone is asking, "Is this secure?"

In the context of information security, the question assumes that "this" has undergone some sort of "information security review." Yet even if it has, the question may be difficult to answer. Even a seasoned information security professional with access to the results of an "information security review" of "this" may not be able to say whether it meets a given data protection requirement. The reason the answer can be difficult is two-fold:

- "This" can refer to a system, a technology, process, a set of data, or any combination thereof.
- The term "information security review" can be applied to a wide variety of activities.

In the context of the "Is this secure?" question, the term "information security review" refers to work performed in the context of an organizational need to understand something specific about the level of information protection in a given systems environment. Previous security review activity in that environment may not have been cognizant of that specific need. For example, passing a Security Architecture review does not necessarily mean that data being displayed to end users has been appropriately protected as per the Gramm-Leach-Bliley Act.

Nevertheless, if an information security officer (ISO) is familiar enough with both the environment and the context of the question, there is always a way to answer. The method chosen by the ISO will depend on several factors. These include his or her estimation of the level of precision required by the questioner as well as his or her competence as a security officer. But assuming all behavioral and political factors aside, the methods available are fairly straightforward.

Audit Versus Security Review

One way to perform a security review is to identify, evaluate, test and assess security controls in the context of an accountable management structure. This follows the model of IT audit. There are two types of audit. There is an audit of management control testing, where passing this type of audit does imply underlying system security. The reason why passing this type of audit does imply system security is that the first step in any audit of management control testing is to identify the management controls and to give a high-level assessment of whether or not the systems would be secure if these management controls were in place. It is a theoretical move as a first step. Once that step has been successfully passed, it will be determined whether in fact those controls are in place.

Activities of internal and external auditors working within the COSO[1] framework follow this model. They test to see whether management has implemented and monitors controls appropriately to ensure that systems are secure. Examples of this type of security review activity are Sarbanes-Oxley and Statement on Auditing Standards Number 70

1. COSO refers to the committee of Sponsoring Organizations of the Treadway Commission, a consortium that defined the responsibilities of management with respect to controls implementation and supervision. See www.coso.org.

(SAS 70) reviews. "Passing" an audit of this variety is generally assumed to mean that the underlying systems are secure because it validates that management's processes for securing things work.

Some regulatory compliance reviews fall into this category as well. But there are still those that simply require certain data to be secured in a certain way, and compliance does not require the theoretical step of assessing management controls. This is the reason for the advent of Sarbanes-Oxley-type legislation. People want to be assured that security is in place because management has established it and not just because the company has a heroic administrator or two that manage to overcome great odds and keep security in place.

Yet not all types of audit activities will answer the security question definitively. The term audit may also refer to process audits, where processes implemented by management are compared to some external standard (e.g. ISO7799). "Passing" an audit that follows a process model does not imply the systems in its scope are secure, it simply indicates that management has implemented a process that is designed to improve security.

Auditors that are professionally certified by organizations like the Institute of Internal Auditors and the Information Systems Audit and Control Association are bound by professional practices. There is remarkably firm consensus in the audit community as to what counts as an adequate test. However, the term "information security review" also refers to reviews that are not formally structured as audits, but are performed in the context of an organizational need to understand something specific about the level of information protection in a given systems environment. In these cases, there is no expectation that the security reviewer will be an auditor or be bound by the audit community's standards.

Table 1 shows a small sample of the difference in constraints placed on security professionals in an audit role versus those not following professional practices of the audit profession, but simply acting in the role of security reviewer. Auditors are not dependent on the management they audit for salary and they have no stake in proving out the design or operations plans for the systems they audit. As opposed to audits, many security review services and the output produced by them are wholly controlled by the organization that commissioned the review. Because of the reviewer lacks independence, a passing grade on a security review does not guarantee that a system will pass any other security audit.

TABLE 1

Constraint with respect to:	For auditors:	For security reviewers:
Reporting structure	Independent to board level	No requirements
Dependence on business relationship	Not rely on auditee for compensation	No requirements
Participation in design or operations	Not have participated	No requirements
Professional standards	Be distinct in attitude and appearance	No requirements

This is not to say that audit should always be the first choice when security review is required. It is one type of security assessment, but it is by no means the only type. Independent audits do not necessarily provide the best answer to the "Is this secure?" question. Note that the flexibility that security reviewers have over auditors is the absence of focus on management accountability. In response to a specific organizational requirement, security reviewers can have complete flexibility in the design of a security review. The process need never consider management control objectives. They can get to the bottom of an issue without the political baggage that comes with it being obvious who is accountable. Lack of reviewer objectivity may be an asset if the reviewer has a personal stake in making sure there is no data leakage. Moreover, the reviewers themselves are not constrained by the formality required of an audit situation; they can often draw on management resources to assist in the assessment processes.

Common Elements

That is not to say that security professionals not working in audit have no standards. This paper is about what is common in that process to all information security reviews and where discretion or process dictates what differentiates one review from another. All reviews, including audits, have at least one of the following:

- ❑ Objective
- ❑ Scope
- ❑ Constraint
- ❑ Approach
- ❑ Result

Objective

A review objective is a statement of the thing to be proved or disproved in the course of a review, for example:

The objective of this review is to provide assurance that application Internet access cannot be exploited to gain access to internal systems

The objective defines what the commissioning organization wants to get out of the review. It is usually to determine whether or not a given systems environment meets some security standard. In this example, the review objective is that of a typical external penetration study; that is, to make sure that users of Web services cannot exploit system vulnerabilities to gain access to the systems that host those services.

Note that the example states the review objective in terms of assurance. Most reviewers, especially auditors, prefer to "provide assurance" that something is secure rather than to simply state that something is secure. This is because of the potential liability for falsely guaranteeing something is secure, as well as the fact that something that is secure today may not be tomorrow.

Scope

A review's "scope" is a definition of precisely what elements of a security program must be examined in order to sufficiently meet the review's objective. Review objective thus dictates scope. For example, the review objective in the previous example dictates that the scope includes the Internet access points of the application and all of the underlying technology that enables that access. If the scope is hard to describe, the review objective should be clarified.

Scope creep is a term that refers to the possibility that the scope will change during the course of the review. It is often said to occur when the technology under review is not completely known at the time the objective is set and the set of underlying technology to be reviewed turns out to be larger than originally thought. However, as long as the objective remains the same, this situation is not an expansion of scope, it is a correction of the original misconception. The scope is what it is, given the objective. If it was incorrectly described in a statement of work, it should be corrected, or the objective should be modified. Thus, the process of defining any given security review is often a small project in itself.

Constraint

A constraint is a situation within which a reviewer operates, which may or may not hinder his or her ability to review the entire scope and complete the review objective. In the previous example, a constraint may be a prohibition on accessing the application during business hours. A reviewer must evaluate his or her ability to fulfill the objective of the review in the context of constraints. All reviews are in some sense constrained by the time available to the reviewer to complete the review.

Approach

An approach is a set of activities that cover the scope in a way that meets the objective of the review, given the constraints. There are usually alternative sets of activities that cover the scope and objective. The idea is to find the set hampered by the fewest constraints.

Say in the previous example, a constraint was that reviewers would not be given the credentials necessary to pose as an authorized user of the application under review. Recall that the objective requires the reviewer to provide assurance that "Application Internet access cannot be exploited to gain access to internal systems." In order to meet this objective, the review must have "application Internet access" as part of the scope. A reviewer in this situation should identify the lack of credentials for application access as a constraint. He or

she may take a chance that it will be possible to gain application user credentials in the course of the review. However, if that turns out not to be possible, and that internal system access was not gained, the reviewer could not claim that the objective was met. In this case, there is no approach that is guaranteed to cover scope and the reviewer should reject the assignment or accept it only with the caveat that it may not be possible to produce a result.

Note the flow of review definition from objective, or purpose, to scope, or target, through constraints to arrive at approach. It is easier to consider something out of scope than to acknowledge that it may not be possible to meet the objective of the review. Nevertheless, constraints do not affect scope per se, they affect only approach. Many reviewers faced with conflicting constraints and objectives write a very detailed "statement of work" that skips the definition of scope and instead defines a review approach that takes into account constraints and ignores the original objective. Clients that sign off on the "statement of work" tacitly agree that the full review objective may not be met. In this way, many people confuse approach with scope because people like to define the scope as something that they can review, rather than acknowledge the constraints in deciding a review approach that may threaten the review objective. This is especially true when time is short. Reviewer resources are not infinite. The objectives of many types of security reviews may only be met in an asymptotic kind of way – thus the phrase "level of assurance." However, it is always more appropriate and professional to rewrite the review objective than to confuse scope with approach.

Result

A result is an assessment of whether the review objective was met. It need not be communicated to exist, but a review is not complete unless it does exist. It is an answer to the question, "Is this secure?" If it is not possible to answer the question with any level of assurance, the review should be declared incomplete. This would occur in the case above if the application access required for covering scope was never gained.

Variable Spectrum

Though all security reviews have common parameters, they can vary widely in objective, scope, constraint, approach and results.

Figure 1 demonstrates just how flexible a security review can be. Reviews can have objectives driven by business or technology. They can have scope that is defined by technology or process. They can have constraints ranging from time and money to reviewer sphere of influence. (Reviewer sphere of influence cannot be underestimated as a constraint because the data gathering required for a typical security review often crosses organizational and even institutional boundaries.) Approaches can range from interviews to technology testing. Results can range from verbal "yes or no" answers to formal published reports Moreover, security review design may encompass part of the spectrum or the full spectrum of any one component.

Types of Security Reviews

There are as many types of security reviews as there are different combinations of objective, scope, constraint, approach, and result, and the variables in any review are by no means limited to the examples in Figure 1. However, there are a few major common types of security reviews, and they are:

- ❑ 90-second security reviews
- ❑ Control self-assessments
- ❑ Design/architecture reviews
- ❑ Due diligence reviews
- ❑ Spot checks
- ❑ Penetration studies

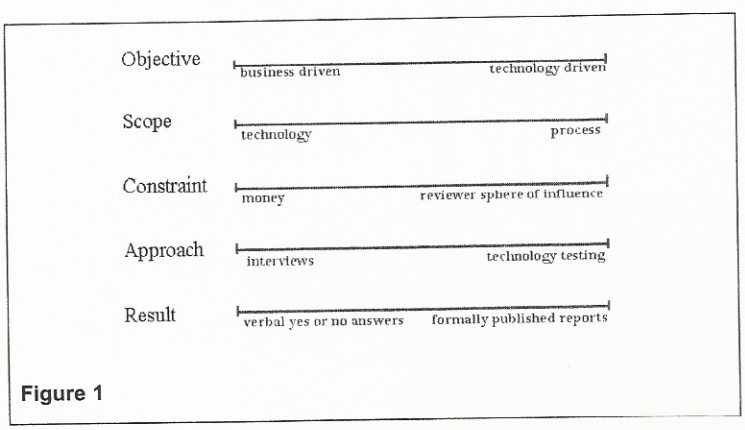
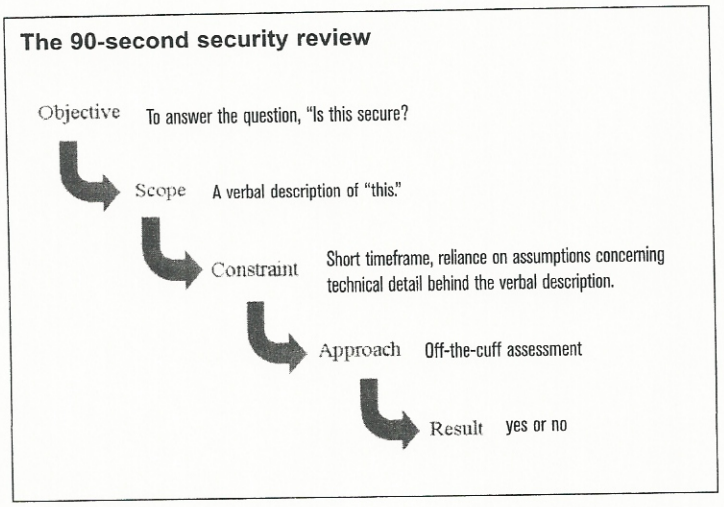
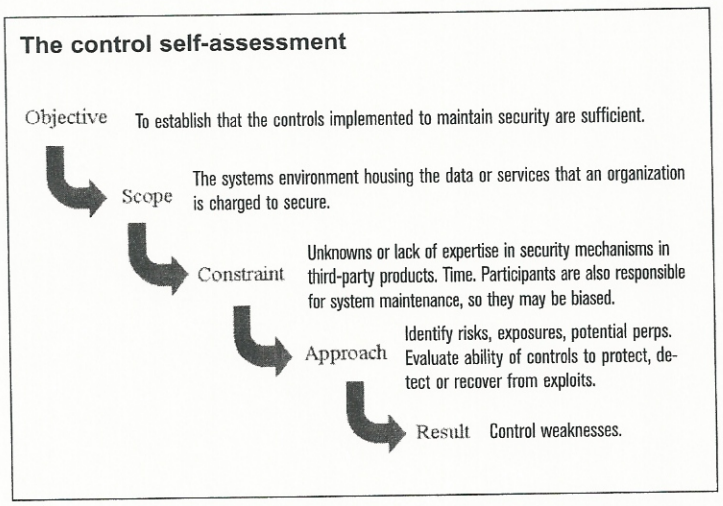


Figure 1

The 90-Second Security Review

In the 90-second security review, the objective is usually business-driven. An executive will call an information security officer (ISO) into a meeting and ask the question, "Is this secure?" The ISO will have about 90 seconds to come up with an answer. The scope could be technology, data, process, or any combination of these, as the spectrum is not necessarily a point along the scope line in Figure 1, but rather a sampling of values along it. It should be possible to clarify scope with a verbal description of the process, system, or data under review. However, the constraint of a required response in a conversationally limited time frame renders the only approach available—an off-the-cuff assessment based on previous knowledge of the system environment as described in the review objective. The result will be a yes or no answer. Spending more time to define scope, or eliminating the time constraint would effectively change the review from a 90-second security review to another type of review entirely.





For example, the ISO is called into the office of the CIO and asked, "Is the XYZ system secure?" The ISO may hesitate, may ask a question, "The XYZ system, is that the one we talked about four months ago?" With an affirmative answer, the ISO may remember that four months ago there was some kind of work done on the system that did not pass review at the time and was not followed up. Hence, the result of the 90-second review will be the verbal assessment, "No. Not likely."

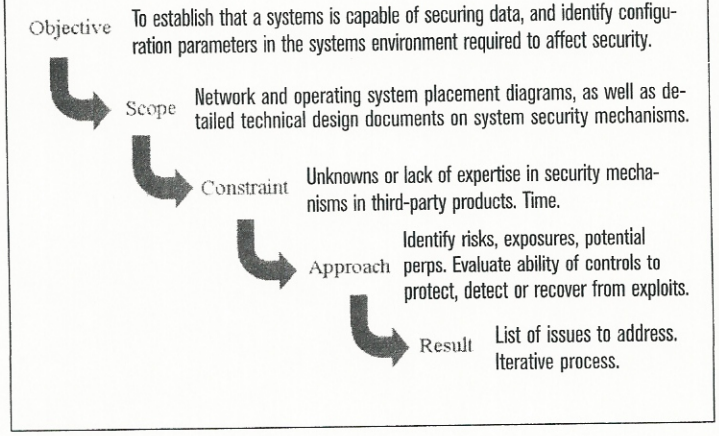
The Control Self-Assessment

In the control self-assessment, the objective is for an organization to determine whether it is properly securing data or services for which it has been a designated steward. The scope is the set of systems that provide the data or services identified in the objective. This is a fairly standard security review.

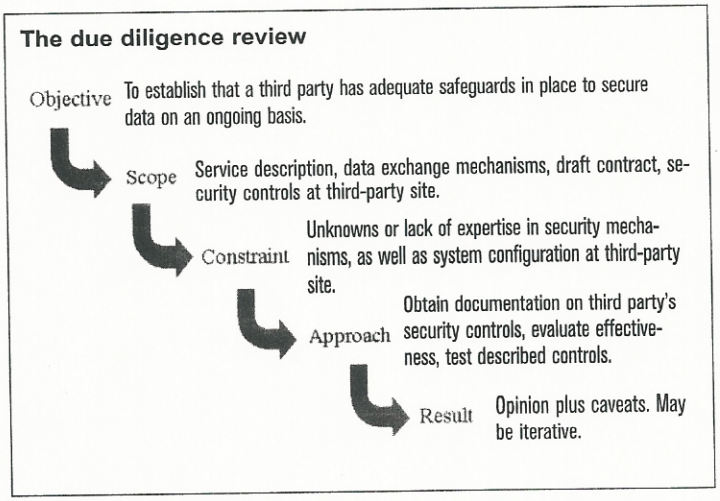
Its major constraint is that the people participating are also responsible for design, implementation and operation of the system under review, so they may be biased as to its security status. However, as the people in the room are also accountable for the security of the system, that constraint may be somewhat mitigated.

Also, it provides the advantage that the people are intimately familiar with the system. The approach usually makes use of a "facilitator" who is not part of the organization, but there is no requirement for independence in the facilitator, just for security expertise. The roles of the facilitator are to guide discussion through various stages of the security risk assessment and vulnerability analysis process, and then to assist the organization in identifying security controls that will reduce risk. Usually, it will begin with a list of information assets to be secured. This will be followed with a list of sources of harm to those assets, e.g.:

The design/architecture review



The due diligence review



hackers, insiders, system failures, etc. System vulnerabilities will then be listed, followed by analysis of the threat of harm. Once the full set of meaningful vulnerabilities is determined, controls are identified that either currently or could in the future mitigate the risk of vulnerabilities being exploited to cause harm. The result of such a review should be a list of control weaknesses for the organization to address.

The Design/Architecture Review

A design or architecture review is typically done as part of a systems development lifecycle process. In the system lifecycle context, the idea of performing a security design or architecture review is to ensure that the system security requirements are defined and, moreover, actually met by the system architecture or design.

Ideally, security should be built into the system and the review will catch design or architecture characteristics that may be detrimental to systems security enforcement efforts. However, a security design or architecture review can occur at any point in the systems' life cycles, and its objective is the same; that is, to establish that security requirements are met by the system architecture and/or design.

The scope of the review will be defined with respect to the objective. It will encompass all systems, networks, and software that comprise the systems architecture. If the system has not yet been built, it will include only the functional and technical requirements and design documents, as well as whatever architecture decisions have been made to date.

Common constraints on these reviews are that they tend to deal with new technology for which there is little expertise and new technology vendors do not always have a design for security. In addition, there may be a time constraint driven by a project schedule that requires architecture decisions to be made before all required subject matter expertise is made available. Hence the approach is often iterative.

It is helpful if the technology environment is covered under existing security policy or standards enforced within the organization. This can narrow design alternatives and reduce the amount of research into security mechanisms. While some unknowns are being researched, some lower-risk decisions may be tentatively accepted. These open issues and security-specific design and configuration decisions form preliminary results until the design is complete. The final result is the completed security configuration of the fully architected system.

The Due Diligence Review

When an organization enters into legal agreements, such as an application service contract or a

merger agreement, it is often required to exercise due diligence in protecting assets, which include information systems and data. For example, due diligence may be required to ensure that the services will indeed perform as expected, that the merged entity does have expected asset protection, and/or that regulatory requirements are met.

The level of due diligence in examining information security controls should be commensurate with the risk of uncontrolled systems operations. The level actually required from a given security reviewer will be set by review's objective. A typical objective in a due diligence review is to establish that a third party has adequate safeguards in place to secure data on an ongoing basis. The scope of the review is the systems operations required to fulfill the statement of work or other information services description.

Constraints are usually that the systems at the third party site may be inadequately documented and that third parties may be loath to invite customers in to review their security configurations. The only realistic approach is to collect as much information as possible about how data will be handled at the third-party site, then assess whether a reasonable and informed security subject matter expert relying on this data would conclude that there was adequate security at the third-party site. Information collected may include security policies and procedures, documented security reviews and audits, network diagrams and system configuration files. It may also include security test results performed in the course of the review. The result will be an opinion on whether it is reasonable to assume there is security at the third party site, and if not, what measures could they take or documentation could they provide that would make it reasonable. As concessions on the part of the third party may result from preliminary review results, these reviews are likely to be iterative as negotiations for the contract continue.

It is tempting to develop an approach to due diligence review that relies only on documentation provided by the third party. However, this works only when the objective of the review and the scope of the documentation provided are a perfect match. There is always research required in that verification step, and often there will be data flow between two parties that is unique to a contract and so will not be covered under any previously prepared material.

Another tempting approach for a due diligence review is to require the service provider to produce a SAS 70 audit. There are two types of SAS 70 audits, informally referred to as SAS 70 Type 1 and SAS 70 Type 2. A SAS 70 Type 1 is an independent assessment by a third party of whether or not controls established by management would secure data if they were implemented. A SAS 70 Type 2 tests that they are implemented.

Unfortunately, a third party under review may provide a SAS 70 audit report that does not cover the scope of the review. For example, an application service provider may outsource their operating system configuration and maintenance. The service provider that performs the operating system security may have a SAS 70 but the application service provider might not. In addition, the SAS 70 report may contain a conditional opinion. It might say that if controls were in place, they would be adequate, but that the auditors were not able to confirm that controls were in place. A final caveat to asking for a SAS 70 is that many service providers do not have them and they take several months to produce. Due diligence decisions must be made based on available information, not on information that may provide assurance in the future. In addition, many service providers do not understand the difference between an audit and a security review. They will often attempt to provide security review reports in lieu of SAS 70 that are not performed by an independent audit. The security reviewer is burdened with explaining to the service provider what additional evidence would provide the required level of assurance.

The Spot Check

The objective of a spot check is to determine whether some specific system or data is properly secured. It differs from an audit or control self-assessment in that the information required is very specific and needs to be determined fairly quickly. It is often the fallback when the 90-second security review fails to produce a result. For example, the CIO will say "Is this system secure?" and the ISO will respond, "I'm not sure, give me a few days to

look at it." The scope of a spot check will be the systems environment directly supporting the security of "this" in the question, "Is this secure?" All people, process and policy with respect to the "this," as well as the technology with which it is implemented, will be in the scope. Constraints on the spot check usually stem from its narrowly defined scope. System dependencies and interfaces may have to be assumed rather than investigated. The approach is very much like audit, where all security parameters are examined for compliance with management control objectives. The result is a "yes or no" opinion, as it is in the 90-second security review.

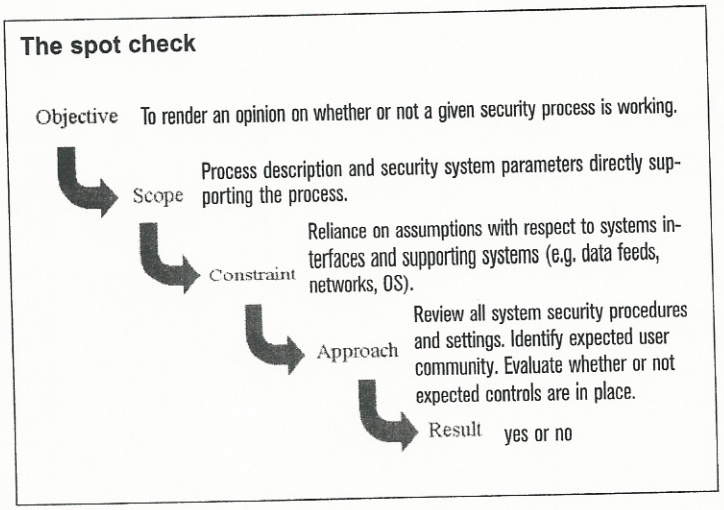
The Penetration Study

In its original sense, the term "penetration study" referred to what is now called a "black box" penetration study. It is a security review in which the objective is to see if the general public can penetrate the security controls of a system meant to be restricted to authorized individuals.

Now, there is much differentiation among consultants as to what types of security review will be done under the heading of "penetration study." "White box" penetration studies refer to a spot check in combination with a black box test. It often includes analyzing application source code. Various other reviews in which more system configuration or documentation is available to the reviewer are referred to as "gray box" testing. Another term for "black box" is "blind." This implies that the reviewer has no knowledge of how the system is engineered. This makes white and gray box tests "non-blind" penetration studies.

The general term "penetration test" still refers to a blind test—that is, the objective is to see if system security controls can be circumvented to allow unauthorized access from a publicly accessible portal. The scope is the portal and the technology that supports it. One constraint is that there is no advance knowledge of the technology comprising the portal, though it may be collected as part of the review. However, given that there is no advance knowledge of how much data will be available to collect, the major constraint is time. Thus the approach for a penetration test is usually a set of data collection techniques followed by a given amount of time spent by a subject matter expert to defeat controls.

The result of a penetration test is a list of vulnerabilities. Often the vulnerability list offered as a result of a penetration test will include items that have not been proven to be real vulnerabilities due to review constraints. If this is the case, and there is no definitive answer on whether the system can or cannot be penetrated, the penetration study will have provided some results but nevertheless failed to meet its objective.



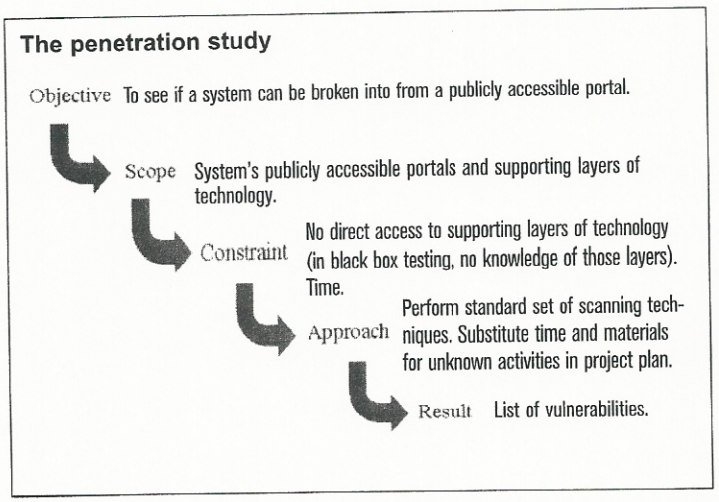


TABLE 2: COMPONENTS OF REVIEW APPROACH

Review Type	Audit Control, Flow, Use, Case or Process	Management control testing	Design/architecture requirements	Assess implementation/ configuration	Substantive data test
90-second security review	Y	N	N	N	N
Control self-assessment	Y	Y	Y	Y	Y
Design/architecture review	N	N	Y	Y	N
Due diligence review	Y	N	Y	Y	N
Spot checks	Y	Y	N	Y	Y
Penetration studies	Y	N	N	N	N

One way around this is to take time into account when setting the objective. For example: "To see if a system can be broken into from the Internet, given the attacker is an expert hacker with access to state of the art software and willing to spend six weeks on the effort." Often a penetration study team will make concessions in quoting additional time and materials in recognition of this failure. However, an organization may be inclined to accept the incomplete result, as evidence that the time and materials required to penetrate the system are cost-prohibitive.

Recommended Approaches

It should by now be apparent just how oversimplified the model in Figure 1 is in describing the possibility of continuum in identifying the objective, scope, constraints and approach in security review. For example, consider that approaches in the reviews described above span from interviews to technology testing. Interviews are usually used to understand how systems are used and how processes support information systems controls. Interviews, combined with documentation that describes current controls, add a level of management control testing. Management requirements for security can at a high level be compared to security design and architecture. The architecture can be confirmed to be working only if implemented and configured as designed. Substantive data tests are required to see if access to information is properly administered. Each of these review techniques, which form the columns of table 2, can to some extent be brought to bear on a number of different types of security reviews.

Table 2 is not meant to represent a flow from activities that are better than others on a spectrum. Different types of reviews will validly make use of different activities in their approaches. In a 90-second review, the only possible approach is to draw upon memory of existing security process strength with respect to the scope. In the control self assessment, any and all possible approaches are possible, though the implementation checks and data test are in fact rarely included. In a design or architecture review, the focus is more on the technology than the use cases, but can be very specific when it comes to implementation and configuration. For a due diligence review, one rarely has access to detailed test results, but may be able to make use of various types of interviews, architecture and configuration documentation. Spot checks look deeply at everything except the big picture provided by an architecture perspective. Typical penetration studies tend to focus on how a system is used.

Third party assessment is a good example of a security review for which there are many existing review approaches. In a third-party assessment, the review objective is to determine whether information is handled by a third party in such a way that maintains the confidentiality, integrity and availability of the data. Scope then becomes the systems at the third-party site that hold the data and all potential access points into these systems. Purpose and scope are the same for both types of reviews. Often, the approach taken will be a due diligence review or a penetration study because both types of reviews share the common constraint of the fact that reviewers do not have direct access to the

TABLE 3: RECOMMENDATIONS FOR REVIEWS

Review Type	Situation	Why
90-second security review	The reviewer is intimately familiar with the system under review and the need for a response is urgent.	Anyone not familiar with the system will not be able to provide a credible opinion in so short a time.
Control self-assessment	Whenever there is a management concern that controls may not be adequate, and always before an audit.	The only way to really know whether a system is operated securely is to know exactly how it is operated. Also provides accountability for poor audit results.
Design/architecture review	Prior to production deployment of new system or major architecture change.	New systems tend to have new security mechanisms or use existing ones in unfamiliar ways. Even if security is sound, operational controls may need to adjust and this usually gives time for that to happen prior to production.
Due diligence review	Whenever sensitive data must be shared with third parties.	Third parties often sign contracts without knowing that they can fulfill the security requirements in them.
Spot checks	Whenever there is a report of a security problem or potential security problem.	An appropriate response is to make sure expected controls are in place.
Penetration study	Management requires assurnace that a system is resistent to the average hacker.	New hacker technologies are usually not immediately picked up by auditors and internal security reviewers, due to their concentration on other deliverables.

configuration of systems in scope. However, due diligence reviewers are not constrained by requests for documentation concerning those systems. By contrast, in a penetration study reviewers are often constrained by requests for documentation. They may be further constrained by not knowing whether or not access will be gained and when, making it extremely difficult—if not impossible—to estimate the amount of testing required to fully achieve the review objective. By contrast, a due diligence review can gather enough information to completely list out the unknowns with respect to data handling and request contract clauses to provide some legal if not technical mitigation of risk. Thus, in a third party assessment situation, a due diligence review should be considered a superior alternative to a penetration study.

Of course, within each of these approaches there is enormous leeway for an individual reviewer to determine how much scrutiny is enough to meet the objective. Yet the general categories of reviews do reveal that some levels of assurance may be met by reliance on a specific review type, performed well. Constraints on any type of activity may increase the reliance on the others. Table 3 makes some recommendations on the type of review that should be considered in a given situation, as well as why that review is considered the most appropriate.

Note that some review approaches are themselves constrained by the availability of a knowledgeable insider. Where there is no familiarity at a organization-wide level with system security controls, it will be impossible to find anyone with the knowledge requisite to conduct a 90-second security review. Similarly, a control self-assessment, by definition, must be performed by those intimate with the system from both a process and technology perspective. By contrast, spot checks and penetration studies may be more objectively performed by those with no insider knowledge of the system under review, and may safely be outsourced to a reputable firm.

That said, those with no insider knowledge of existing security mechanisms cannot rely on previous experience with controls, so even a spot check invites an architecture review—thus these may be more economically done by insiders. When considering the question of whether or not to outsource security reviews, it is usually only economical when the necessary technological expertise cannot be found internally. When a review is outsourced, an internal staff member should be assigned to work with the reviewer so that expertise in internal technology that a reviewer will gain by the in-depth systems analysis the review requires does not leave the organization at the end of the outsourced engagement.

Another consideration on the "outsource versus insource" decision is that any review that requires some level of objectivity or independence should rely on outsourced resources. However, outsourcers will be loyal to the executive that they perceive will sign off on their invoice or provide future business, so that person may get first look at the results. Where a high level of objectivity is required, an organization should fall back on its auditors.

However, there are a growing number of information security review requirements where the objective is not independent assessment. Instead, the objective is internal assurance. The level of comfort a manager can take in internal assurance need not be considered less than that of an independent assessment. When accepting an opinion from an internal security reviewer, an executive gains accountability. Audits may be good or bad, and they do not provide accountability unless accountability for security is established well prior to the audit.

Summary

In summary, there is no even continuum of security reviews where one is more rigorous than the next, culminating in a "full systems audit." Six type of security reviews have been identified and differentiated in these pages. Yet there are as many others as there are consulting firms wishing to differentiate themselves. It is important to understand that the approach determines the format and quality of the result. The important take-away here is that different types of security reviews are useful in different contexts. Context is the combination of review objective, scope, constraint, and approach. Choosing the right type of security review is fundamental to achieving the best possible assessment as a result.

So if in response to the question, "Is this secure?" the answer is, "yes," the next question should be, "What did the review consist of?"

JENNIFER BAYUK, CISA, CISM is the Chief Information Security Officer at Bear Stearns & Co., Inc. Her responsibilities include security policy, architecture, design, management, monitoring and investigation. She has been a manager of information systems audit, a Big 4 security consultant and auditor and a security software engineer at AT&T Bell Laboratories. She has been published on information security topics ranging from security process management to client/server application controls, including two editions of an ISACA education foundation textbook called, "Stepping Through the IT Audit." She has lectured for ISACA, NIST and CSI.