CSI NetSec 2005

Security Review Program Alternatives

Jennifer Bayuk

Security Review Program Alternatives

EXC-1, June 13, 2005

BEAR STEARNS

CSI COMPUTER SECURITY INSTITUTE Conferences

Has Security Reviewed This?

BEAR STEARNS

- This presentation is about work performed in the context of an organizational need to understand something about the level of information protection in a given systems environment.
- This presentation is not about attestation services based on independently defined professional practices for those who will attest, following standards for identifying, evaluating, testing, and assessing controls in the context of an accountable management structure. That is Information Systems Audit.

Audit versus Review

BEAR STEARNS

- Audit
  - Management control testing where passing implies underlying security
    - Internal and External Audit in the COSO Model
      - Sarbanes-Oxley Compliance
      - SAS70
    - Regulator Review of Compliance
  - Process audits, where passing does not imply underlying security (e.g. ISO7799)
- Review - passing cannot be assumed to prove underlying security
  - 90-second security review
  - Control self-assessments
  - Design/Architecture reviews
  - Due diligence reviews
  - Spot checks
  - Penetration studies

Measures of Independence

BEAR STEARNS

	Auditor	Reviewer
Reviewer reporting structure	Independent to board level	No requirements
Reviewer dependence on business relationship	Not rely on auditee for compensation	No requirements
Reviewer participation in design or operations	Not have participated	No requirements
Reviewer professional standards	Be distinct in attitude and appearance	No requirements

Common Elements

BEAR STEARNS

- Objective
- Scope
- Constraint
- Approach
- Result

Objective

BEAR STEARNS

- Objective
- Scope
- Constraint
- Approach
- Result

A statement of the thing to be proved or disproved in the course of a review. It is often stated in terms of assurance, for example:

The objective of this review is:

To provide assurance that:

Application Internet access cannot be exploited to gain access to internal systems

Scope

- Objective
- Scope
- Constraint
- Approach
- Result

Scope is a technical term that refers to the map of the purpose of the review to the thing to be reviewed.

Review objective dictates scope. For example, the previous review objective example dictates that the scope includes the Internet access points of the application and all underlying technology that enables that access. If the scope is hard to describe, the review objective should be clarified.

Constraint

- Objective
- Scope
- Constraint
- Approach
- Result

Constraints are situations 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.

Approach

BEAR STEARNS

- Objective
- Scope
- Constraint
- Approach
- Result

Approaches are alternative sets of activities that covers the scope in a way that meets the objective of the review, given the constraints.

*It is easy to confuse scope with approach in that people like to define the scope as something that they **can** review rather than acknowledging that there are constraints in deciding a review approach that may threaten the review objective.*

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."

Result

- Objective
- Scope
- Constraint
- 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 exists.

Variable Spectrum

BEAR STEARNS

- Objective

- Scope

- Constraint

- Approach

- Result

The 90-second Security Review

BEAR STEARNS

Objective

To answer the question, "Has security reviewed this?" with "yes."

Scope

A verbal description of "this."

Constraint

Short timeframe, reliance on assumptions concerning technical detail behind the verbal description

Approach

off-the-cuff assessment

Result

"yes" or "no"

The Control Self-Assessment

BEAR STEARNS

Objective

To establish that the controls implemented maintain security are sufficient to do so.

Scope

The systems environment housing the data that an organization is charged to secure.

Constraint

Unknowns or lack of expertise in security mechanisms in third party products. Time. Participants are also responsible for system maintenance so may be biased.

Approach

Identify risks, exposures, potential perps, evaluate ability of controls to protect, detect, or recover from exploits.

Result

Control weaknesses

The Design/Architecture Review

BEAR STEARNS

Objective

To establish that a system is capable of securing data, and identify configuration parameters in the systems environment required to effect security.

Scope

Network and operating system placement diagrams, as well as detailed technical design documents on system security mechanisms.

Constraint

Unknowns or lack of expertise in security mechanisms in third party products. Time.

Approach

Compare settable parameters of all systems components to known secure configurations and/or security policy.

Result

List of issues to address, iterative process.

The Due Diligence Review

BEAR STEARNS

Objective

To establish that a third party has adequate safeguards in place to secure data on an ongoing basis.

Scope

Service description, data exchange mechanisms, draft contract, security controls at third party site.

Constraint

Unknowns or lack of expertise in security mechanisms, as well as system configuration at third party site.

Approach

Obtain documentation on security controls at third party, evaluate effectiveness, test described controls.

Result

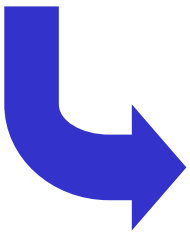
Opinion plus caveats, may be iterative.

The Spot Check

BEAR STEARNS

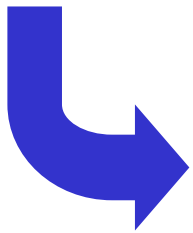
Objective

To render and opinion on whether a given security processing working.



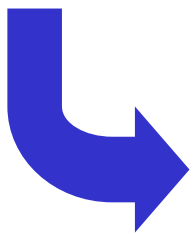
Scope

Process description, system security parameters of system directly supporting the process.



Constraint

Reliance on assumptions with respect to systems interfaces and supporting systems (e.g. data feeds, network, OS).



Approach

Review all system security procedures and settings, identify expected user community, evaluate whether expected controls are in place.

Result

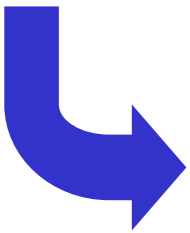
"yes" or "no"

The Penetration Test

BEAR STEARNS

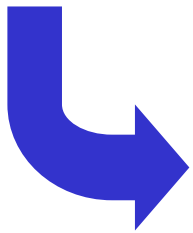
Objective

To see if a system can be broken into from a publicly accessible portal.



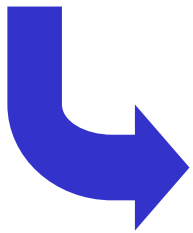
Scope

System's publicly accessible portals and supporting layers of technology.



Constraint

No direct access to supporting layers of technology (in black box testing, no knowledge of those layers). Time.



Approach

Perform standard set of scanning techniques, substitute time and materials for unknown activities in the project plan.

Result

List of vulnerabilities.

More detail on approach

BEAR STEARNS

	Substantive Data Test	Assess Implementation/ Configuration	Design Architecture/ Requirements Reconciliation	Management control testing	Audit Control Flow, Use Case, or Process
90-second security review	N	N	N	N	Y
Control self-assessments	Y	Y	Y	Y	Y
Design/Architecture reviews	N	Y	Y	N	N
Due diligence reviews	N	Y	Y	N	Y
Spot checks	Y	Y	N	Y	Y
Penetration studies	N	N	N	N	Y

To Outsource or not to Outsource

BEAR STEARNS

- Pros
  - Independence
  - Expertise in technology
- Cons
  - Those with no insider knowledge of existing security mechanism cannot rely on previous experience with controls, so even a spot-check invites an architecture review
  - Outsourcers are 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
  - Expertise in internal technology gained by in-depth systems analysis required by security review leaves the firm at the end of the engagement
  - Rarely capable of pulling off the 90-second security review

Recommendations

BEAR STEARNS

	When	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-assessments	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 reviews	Prior to production deployment of new system or major architecture change.	New systems tend to have new security mechanism 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 reviews	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 studies	Management requires assurance that a system is resistant 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.

Discussion