Survivability via Control Objectives

Position Paper for 3rd IEEE Information Survivability Workshop (ISW-2000)
Philip L. Campbell
Sandia National Laboratories, Albuquerque, New Mexico 87175[1]

1 Abstract

Control objectives open an additional front in the survivability battle. A given set of control objectives is valuable if it represents good practices, it is complete (it covers all the necessary areas), and it is auditable. CobiT and BS 7799 are two examples of control objective sets.

2 Introduction

Survivability evokes dramatic images, such as a super hero saving the critical infrastructure. We think of hardware that can reconfigure itself on-the-fly, transforming itself into a moving target. Or we think of networks of software agents that can detect, defend, and perhaps even counterattack. These images are important because they provide us with goals.

Meanwhile, there is at least one additional front in the survivability battle, this one involving "control objectives." This is a relatively humdrum front, exciting to accountants possibly but not to super heros. However, the more fronts we can open, the more opportunities we have to push the conflict to our favor. This paper defines control objectives, explains their strengths—good practice, completeness, and auditability—and how control objectives relate to similar approaches.

The remainder of this position paper is organized as follows. Section 3 presents needed definitions and two example sets of control objectives. Section 4 discusses their strengths. Section 5 discusses related approaches. Section 6 presents conclusions.

3 Definitions & Examples

3.1 Definitions

A control objective can be defined as a "statement of the desired result or purpose to be achieved by implementing control procedures within a particular IT [Information Technology] activity." [5]

A control can be defined as "The policies, procedures, practices and organisational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected." [5] A control is a reasonable means to ends that are defined by business objectives.

DISCLAIMER

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

3.2 Examples

CobiT [5] and BS 7799 ([2], [7]) are two examples of the control objectives approach (see also [4]). Both intend to provide "reasonable assurance." CobiT is a three-level hierarchy with 4 "domains" at the top level, 34 "high-level control objectives" at the middle level, and 302 "detailed control objectives" at the bottom level. BS 7799 consists of ten "sections," each of which consist of up to four levels. There are 36 control objectives on the second level and a total of 127 on the third and fourth.

Auditing procedures are provided for CobiT (see "Audit Guidelines" [5]) that should be performed by "Certified Information Systems Auditors" (CISA). For BS 7799 there is a scheme, "c:cure," that enables organizations to certify their compliance with BS 7799. [3] The intent is to facilitate commerce by enabling businesses to evaluate the security of potential partners.

4 Strengths of the Control Objectives Approach

The strength of control objectives is threefold. First, control objectives represent "good practice," so that those that adopt them are adopting the general consensus of experts. Second, control objectives cover all of the territory, or at least they are explicitly intended to do so. They can thus be said to be complete. And third, control objectives are auditable, so management can monitor their progress.

Another way of viewing control objectives is as prudent business practice: do what the general consensus of experts advise, and then when disaster strikes (as it will), you can defend your reputation via your last audit, rightly claiming that the disaster is a chance event and does not reflect your level of security.

4.1 Good Practice

CobiT, for example, is intended to be

> a generally applicable and accepted standard for good Information Technology (IT) security and control practices... The term **"generally applicable and accepted"** is explicitly used in the same sense as the Generally Accepted Accounting Principles (GAAP). CobiT's **"good practices"** means consensus of the experts—they will help you optimise your information investment, but foremost they are what you will be judged upon when things do go wrong. [5] (emphasis in the original)

Note that this is what CobiT is intended to be, not a declaration of what CobiT is in fact. There may be other sets of control objectives that better fulfill the same intention. What is considered to be good practice will change over time, implying that any given set of control objectives will have to change over time.

4.2 Completeness

It is not difficult for those familiar with the field to generate sample control objectives, such as those dealing with passwords, physical protection of computing hardware, and the importance of written policies. With a little more effort sample control objectives on training, classification of data, and availabilty could be generated. However, it would be difficult for anyone who did not regularly work on the entire scope of the area to generate a complete set of control objectives, without adding more than is

necessary. One of the strengths of the control objectives approach is that the set is explicitly intended to be complete.

4.3 Auditability

Control objectives are intended to be auditable. This provides management with a way to gauge their progress.

An audit is an evaluation of performance against a given standard, but unfortunately it is necessarily subjective. The best of standards make it easy for different auditors to generate consistent evaluations, thereby reducing the subjectivity of the audit and increasing the value to management.

Without auditability, control objectives become platitudes and are of little use.

5 Related Approaches

Using the three criteria from above—namely good practice, completeness, and auditability—the universe can be shown in the following diagram.

Figure 1.   Different Approaches
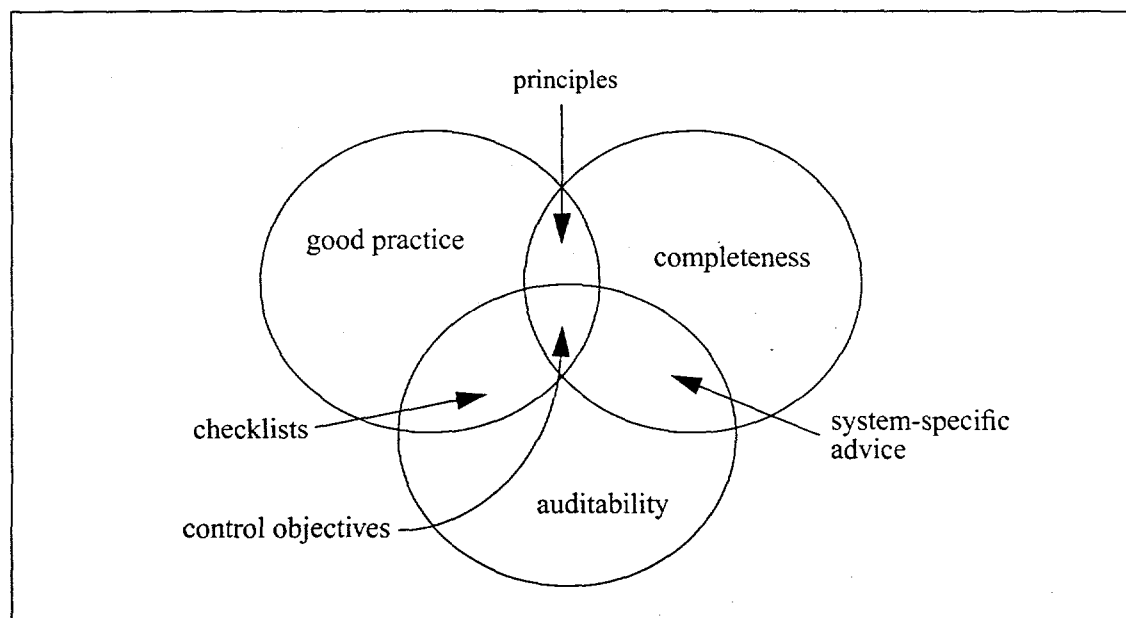
"Principles" are high-level descriptions of good design. For example, "Computer Security Supports the Mission of the Organization" [9], or "cost effectiveness" and "simplicity" [11].

"Checklists" contain yes/no questions on practices. For example, "Does the agency have an executive ADP[2] management committee?" [6], or "Are computer security related policies generally understood by

---

2. Automated Data Processing.

staff?" [10]

"System-specific advice" is targeted for specific systems (and only for that reason do we consider that they do not represent "good practice"). For example, "Routinely examine your *inetd* configuration file" [8], or "Ensure that permissions on /etc/services are set to 644." [1]

Each of these related approaches lacks an important strength enjoyed by control objectives.

6 Conclusions and Future Work

Control objectives are a distillation of good practice. They are complete and auditable. Adopting a good set of control objectives enables management to adopt the generally accepted good practice in the industry for all aspects of information security, and to be able to monitor their progress. We believe that the control objective approach provides an additional front in the battle for information survivability. In the meantime, it is not clear what the best set of control objectives would be for the particular problems facing information survivability. This suggests the need for further research.

References

[1] Australian Computer Emergency Response Team, "UNIX Computer Security Checklist" (Version 1.1) Last Update 19-Dec-1995.

[2] BS 7799-1:1999 Information security management. Code of practice for information security management. BS 7799-2:1999 Information security management. Specification for information security management systems. British Standards Institute (http://www.bsi.org.uk/).

[3] BS 7799 c:cure web site (http://www.c-cure.org).

[4] Janet L. Colbert, Paul L. Bowen, "A Comparison of Internal Controls: CobiT, SAC, COSO, and SAS 55/78." IS Audit & Control Journal, Volume IV, 1996, pp. 26-35.

[5] Control Objectives for Information and Related Technology (CobiT), available at no charge from www.isaca.cobit.htm (see also ISACA's home page: www.isaca.org).

[6] Evaluating Internal Controls in Computer-Based Systems: Audit Guide (Black Book), US GAO, June 1988.

[7] Gamma Secure Systems Limited web site (http://www.gammassl.co.uk/topics/hot1.html).

[8] Simson Garfinkel, Gene Spafford, "Practical Unix and Internet Security," Second Edition, 1996. O'Reilly & Associates, Inc. Sepastopol, CA. ISBN 1-56592-148-8.

[9] Marianne Swanson, Barbara Guttman, "Generally Accepted Principles and Practices for Securing Information Technology Systems." NIST Special Publication 800-14, September 1996. 56 pages.

[10] Charles Cresson Wood, et al., Computer Security: A Comprehensive Controls Checklist. John Wiley & Sons, 1987. ISBN 0-471-84795-X.

[11] Charles Cresson Wood, "Principles of Secure Information Systems Design." Computers & Security, 9, (1990) 13-24.