SAND2002-0131
Unclassified Unlimited Release
Printed September 2003

An Introduction to Information Control Models

Philip L. Campbell
Networked Systems Survivability & Assurance Department
Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-0785

Abstract

This report presents information control models, focusing on a subset known as control frameworks. Those (and several other) models include BS 7799, CobiT, CoCo, COSO, FISCAM, GAPP, GASSP, ITCG, SSAG, SSE-CMM, and SysTrust. To provide contrast, other types of information control models are also presented. The purpose of this report is to help readers increase their information security via the rigor of an information control model, in particular a control framework.

Keywords

American Institute of Certified Public Accountants (AICPA), AICPA / CICA SysTrust™ Principles and Criteria for System Reliability, attack taxonomies, audits, BS 7799, c:cure, CIA security model, CICA, Certified Information Systems Auditor (CISA™), Common Criteria, control frameworks, control objectives, Control Objectives for Information and Related Technology (CobiT ®), Control / Risk Self-Assessment (CRSA), Control Self-Assessment (CSA), computer security, computer security checklists, computer security principles, Control Objectives for Network Centric Technology (CONCT), confidentiality, controls, control objectives, Enterprise Security Architecture (ESA), EPS-IT, eSAC, Financial Information System Controls Audit Manual (FISCAM), GAO "Black Book," Generally Accepted System Security Principles (GASSP), Generally Accepted Principles and Practices (GAPP), Guidance on Control (CoCo), INFOSEC Assessment — Capability Maturity Model (IA-CMM), information assurance, Information Security Framework (ISF), Information Technology Control Guidelines, Integrated Control — Integrated Framework (COSO), integrity, International Standards Organization (ISO), ISO 17799, Information Systems Audit and Control Association (ISACA ®), Information Systems Audit and Control Foundation (ISACF), ISO / IEC 17799, IT governance, IT Governance Institute™, National Institute of Standards and Technology (NIST), OCTAVE^{SM} (Operationally Critical Threat, Asset, and Vulnerability Evaluation^{SM}), Organization for Economic Cooperation and Development (OECD), risk assessments, Security Self-Assessment Guide for Information Technology Systems, Systems Auditability and Control (SAC), Systems Security Engineering — Capability Maturity Model (SSE-CMM), taxonomies.

Table of Contents

Appendices

1 Executive Summary

This report presents information control models. Each model can be thought of as a definition of information assurance, as a taxonomy, and as an answer to the following questions:

> What do I need to do to make my system sufficiently reliable and secure, based on my organizations assessment of the costs of security measures versus the value of operating reliable systems for my customers?
>
> How much is enough? What method can I use to determine the minimum level of due care based on best practice benchmarks needed to reduce my enterprise risk to an acceptable level?
>
> Whom can I trust to tell me what I need to do and to help me protect my systems and networks? [18] (bold in the original)

This report focuses on a subset of information control models known as control frameworks. Those models (and a few others) include BS 7799, CobiT, CoCo, COSO, FISCAM, GAPP, GASSP, ITCG, SSAG, SSE-CMM, and SysTrust. To provide contrast, other types of information control models are also presented in this report.

The purpose of this report is to help readers increase their information security via the rigor of an information control model, in particular a control framework.

2 Introduction

> The growth and success of nearly all enterprises rely on harnessing information technology (IT) for secure, profitable use. All enterprises benefit from an integrated and comprehensive approach to risk management, security and control... Too often information security has been dealt with as a technology issue only, with little consideration given to enterprise priorities and requirements. Responsibility for governing and managing the improvement of security has consequently been limited to operational and technical managers... Effective security is not just a technology problem, it is a business issue. [72]

This report presents information control models. Each model can be thought of as a definition of information assurance, as a taxonomy, and as an answer to the following questions:

> What do I need to do to make my system sufficiently reliable and secure, based on my organizations assessment of the costs of security measures versus the value of operating reliable systems for my customers?
>
> How much is enough? What method can I use to determine the minimum level of due care based on best practice benchmarks needed to reduce my enterprise risk to an acceptable level?
>
> Whom can I trust to tell me what I need to do and to help me protect my systems and networks? [18] (bold in the original)

This report focuses on a subset of information control models known as control frameworks. Those models and ones from the two other "communities" of models, as we will explain below, include BS 7799, CobiT, CoCo, COSO, FISCAM, GAPP, GASSP, ITCG, SSAG, SSE-CMM, and SysTrust. To provide contrast, other types of information control models are also presented in this report. There is not a crisp division between these two groups but generally the "other" models are not as comprehensive or they do not focus as much on "controls," as we will define it below.

The purpose of this report is to help readers increase their information security via the rigor of an information control model, in particular a control framework.

We need several definitions before we proceed:

> *Taxonomy:* A recursive partitioning of a complete set.[1]
>
> *Control*: 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. ([28], page 12)

[1] Our definition is more constrained and mathematical than the one usually found in dictionaries. For example, Webster defines taxonomy as a "classification, *specif.*: orderly classification of plants and animals according to their presumed natural relationships," and classification is defined as a "systematic arrangement in groups or categories according to established criteria."

> *Control Objective*: A statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT[2] activity. ([28], page 12)
>
> *Control Framework:* A taxonomy of control objectives.

Control frameworks[3] present a superstructure above the hundreds of controls required for information assurance.

We can make the following observations about all of the models we present, couched in control framework terms:

1. Every organization that uses IT uses a set of controls, perhaps unconsciously, even if the "controls" are to let everyone have full access.
2. An ideal set of controls for a given organization should depend on the business objectives, budget, personality, and context of that organization.
3. The set of control objectives—as opposed to the set of controls—can and should be constant across organizations.
4. Therefore, each organization could use the same control framework to manage their particular controls to meet those constant control objectives.

The value of the models presented in this report is their balance of conciseness and completeness. The best ones include every necessary item and no superfluous ones. The only way to evaluate that balance appears to be by experience over time.

[2] Information Technology.

[3] The only definition I have seen of "framework" in the current context is "a collective term that refers to policies, standards, and procedures." [82]

Most of the models we present are shown in Figure 1, plotted against time.

Figure 1 Time Diagram

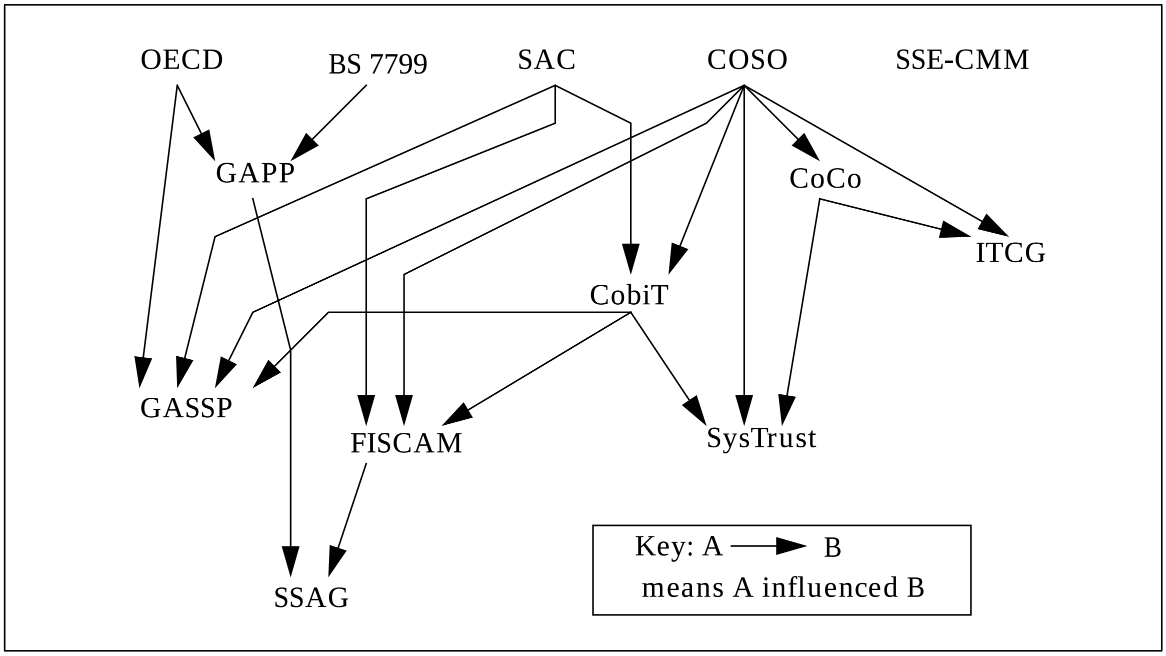
1980	Kraus					
1982						
1984	Perry & Wallich					
1986						
	Wood's Checklist					
1988	GAO Audit Guide					
	Neumann & Parker	Vallabhaneni				
1990	Wood's Principles					
1992	Meadows					
1994	OECD	SAC	COSO			
	Levine	CoCo				
1996	GAPP	Garfinkel & Spafford				
1998	ITCG	Howard & Longstaff	LfLO	PoLO		
	FISCAM	GASSP	CONCT	BS 7799	SSE-CMM	Common Criteria
2000	CobiT	SysTrust	CIAO			
	OCTAVE	SSAG				
2002	IA-CMM					

The explicit influences between the control frameworks and their root models is shown in Figure 2.[4]

Figure 2 identifies three communities—control objectives, principles, and Capability Maturity—

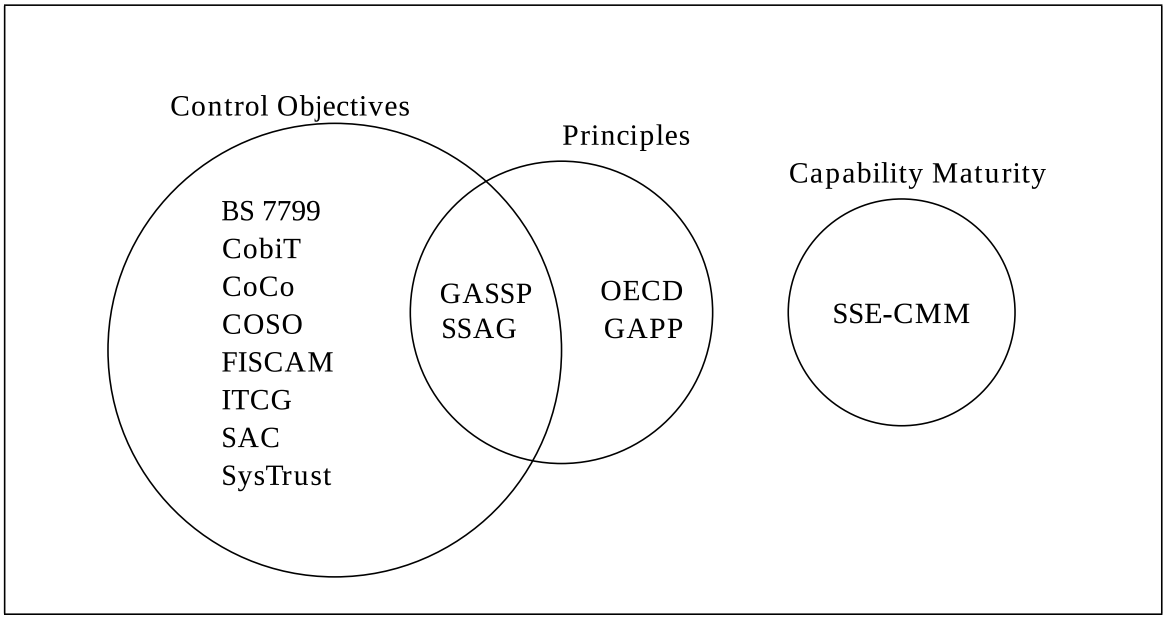
[4] Included in this Figure is GAPP and SSE-CMM. Neither is a control framework per se. However, each represents a "community," as shown in Figure 3.

Figure 2 Influence Diagram



based on underlying models, as shown in Figure 3.

Figure 3 Model Communities



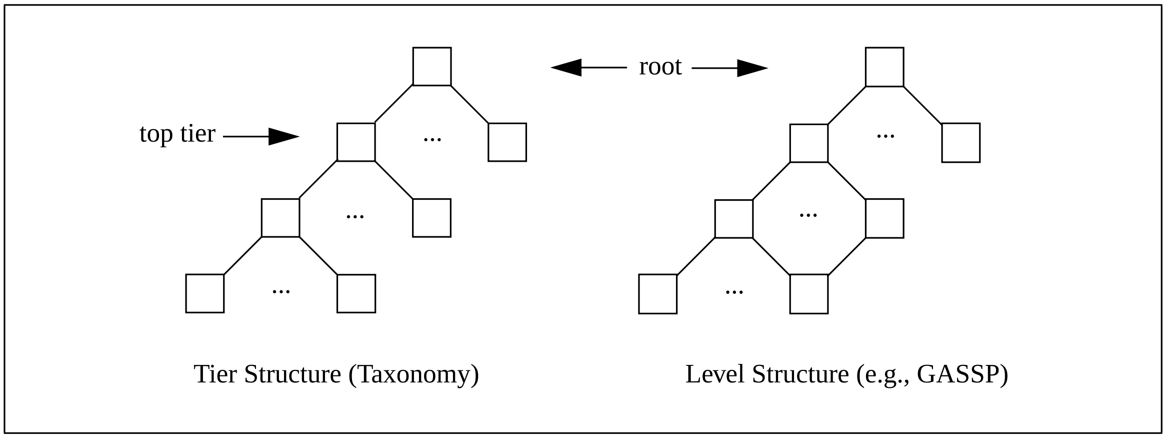
The first, the largest of these three communities, is the one based on control objectives. This community—consisting currently of BS 7799, CobiT, CoCo, COSO, FISCAM, ITCG, SAC, SysTrust, and partially GASSP and SSAG—traces its roots to COSO and, secondarily, to SAC. (BS 7799 is part of this community even though there are no explicit influences.)

The second community is based on the principles model, each instance of which consists of a list of principles or "qualities," such as Accountability, Awareness, and Ethics—the first three in OECD's list. This community—consisting currently of GAPP, GASSP, OECD, and SSAG—traces its roots to OECD. GASSP and SSAG span both the control objectives and the principles communities, tracing their roots to BS 7799, COSO, and SAC in the former community and to OCED in the latter.

The third community is based on the Capability Maturity model. There is only one member of this community shown in Figure 1, namely SSE-CMM. The model that is the basis for this community is described when we present SSE-CMM (see Section 3.3.1).

Taxonomies are by (our) definition hierarchically structured. Usually they can be depicted as a tree, which is a graph with the additional constraint that there is only one path from any given node to the root, as shown in the left side of Figure 4. The nodes with the same pathlength to the root are said to be on the same "tier," as we will use the term.

Figure 4 Structures



One of the models presented, namely GASSP, uses a more general (and more confusing) structure that allows more than one path from at least one node to the root. For purposes of distinction we refer to the tiers in GASSP as "levels."[5] This level structure is shown on the right side of Figure 4.

This report presents taxonomies of various sizes. The small ones are so small that they consist of a single tier. These taxonomies can consist of little more structure than a list. These smaller taxonomies can be presented in their entirety, when there is no copyright issue. However, for the larger taxonomies, space constraints prevent presenting more than the top two tiers, shown `in this font`, sometimes with integers in parentheses indicating the number of elements in the subtree below so that the reader can get a sense of the size. For most of these larger taxonomies a table is included that shows the number of nodes in each tier. For example, the tier organization table for SysTrust, Table 9, is shown below as Table 1.

[5] SSAG, SSE-CMM, and CobiT all use "levels" but it is in the context of "maturity levels," which is a different matter (see Appendix C).

Table 1 Sample Tier Organization Table (compare Table 9)

Tier	Name	Elements
Top	Principles	4
Middle	Criteria	12
Bottom		58

Most of the taxonomies have three tiers, a few have four. In order to avoid confusion the tiers are labelled “top,” “middle,” and “bottom”—as exemplified in Table 1—if there are only three tiers, and “top,” “second,” “third,” and “bottom” if there are four. The first or “top” tier is the one below the root, as indicated in Figure 4.

The size of each tier (i.e., the number of elements) of each of the control frameworks (and closely related models) is shown in Table 2.

Table 2 Tier Size (Taxonomies listed alphabetically)

Taxonomy	Top	Second	Third	Bottom
BS 7799	10	36	~50	~80
CobiT	4	34	318	▨
CoCo	4	20	98	▨
COSO	5	16	~80	~250
FISCAM	6	22	57	7
GAPP	14	34	100	▨
GASSP	9	14	0[a]	▨
ITCG	7	31	~160	~400
SSAG	3	17	36	174
SSE-CMM[b]	5	12	29	▨
	2	22	128	▨
SysTrust	4	12	58	▨

[a] This bottom level has not yet been populated.

[b] SSE-CMM consists of two tiers (see Section 3.3.1).

The rest of this report is organized as follows. Section 3 presents the control frameworks (and representatives of the principles and Capability Maturity communities (see Figure 3)). Section 4 presents other models. Appendix A presents “Exhibits” (i.e., photocopies) of the models presented in Section 3. Appendix B presents Exhibits of a few of the models presented in Section 4. (And Appendix C presents a comparison between the level names for the three models that use “maturity levels.”)

A guide to the abbreviations and colloquial names used in this report is available on page 71.

3 Control Frameworks

> The survey results over the years offer compelling evidence that neither technologies nor policies alone really offer an effective defense for your organization. Intrusions take place despite the presence of firewalls. Theft of trade secrets takes place despite the presence of encryption. Net abuse flourishes despite corporate edicts against it. Organizations that want to survive in the coming years need to develop a comprehensive approach to information security, embracing both the human and technical dimensions. They also need to properly fund, train, staff and empower those tasked with information security. [96]

In this Section we present most of the models shown in Figure 2, organized by community (and alphabetically within communities), as shown in Figure 3:

- the control objectives community,
- the principles community, and
- the Maturity Model community.

Because of our opinion of the importance of control frameworks, we present here all of those models but only representatives of the other communities.

For each of the models presented, a set of "Exhibits" is included and is shown in Appendix A. Each exhibit is a photocopy of a page or pages from the model definition. This information is photocopied instead of transcribed so that the reader can get a glimpse of the model definition itself. In order to provide some uniformity across the exhibits, the initial part of the material has in each case been chosen for the exhibit.

3.1 Control Objectives Community

The models in this community are based on the concept of "control objective," as defined in Section 2 and reproduced here:

> *Control*: 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. ([28], page 12)
>
> *Control Objective*: A statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity. ([28], page 12)

This community has the following members: BS 7799, CobiT, CoCo, COSO, FISCAM, ITCG, and SysTrust.

3.1.1 BS 7799

"BS 7799-1:1999 Information security management—Part 1: Code of practice for information security management" and "BS 7799-2:1999 Specification for information security management systems"[6] constitute what is known as BS 7799 from the British Standards Institute ([12], see also [14], [50], [78]). The "Security Code of Conduct" from the British Government's Department of Trade and Industry [43] was a precursor from which grew BS 7799, which has, in turn, subsequently grown into ISO 17799 [70]. The Australian / New Zealand standard, AS / NZS 4444 [8], is a very close adaptation of BS 7799. We are familiar with BS 7799 but not with the others. However, our review of BS 7799 would appear to apply to the others as well.

BS 7799 is explicitly a "starting point," intended to describe "best practice" in the form of good examples from which one's own controls can be developed [12]. BS 7799 focuses on information security—the CIA model—that is a proper subset of information assurance, as defined in Section 4.1 above. BS 7799 notes, for example, that the establishment of security requirements is dependent on risk assessment, although no specific risk assessment method, such as CSA ([95], [59]) or AS / NZS 4360:1999 [7], is mentioned.

A scheme, known as "c:cure" ([13], [88]), has been developed that enables organizations to certify their compliance with BS 7799. The intent is to facilitate commerce by enabling businesses to evaluate the security of prospective partners.

BS 7799 has enjoyed support by increasingly global organizations: first the Department of Trade and Industry (DTI) [43], where it was known as the "Security of Code of Conduct," then the British Standards Institute (BSI), where it was known as BS 7799, and finally the International Standards Organization [67], where it is known as ISO 17799. Considering the length of BS 7799's roots and the stature of its currently sponsoring organization, support for it should continue.

Organization

BS 7799 is organized into four tiers, as shown in Table 3.

Table 3 BS 7799 Organization

Tier	Name	Elements
Top	Sections	10
Second	Control Objectives	36
Third		~ 50
Bottom		~ 80

Here are the entire top and second tiers[7] of BS 7799:[8]

[6] BS 7799-2 has been recently updated to BS 7799-2:2002 and presents a "Plan-Do-Check-Act" cycle that is similar to CoCo's cycle (see Section 3.1.3).

[7] Peltier's book, for example, shows all three upper tiers, including the objectives for all of the items on the second tier ([91], pp. 77-81).

[8] Exhibits from BS ISO / IEC 17799: 2000 reproduced with the permission of BSI under licence number 2002SK / 0164. British Standards can be obtained from BSI Customer Services, 389 Chiswick High Road, London W4 4AL. (Tel + 44 (0) 20 8996 9001). BS ISO / IEC 17799: 2000 & associated standards may be obtained electronically from http: / / www.bspsl.com / 17799 / .

3.[9] Security policy
  3.1 Information security policy
4. Security organization
  4.1 Information security infrastructure
  4.2 Security of third party access
  4.3 Outsourcing
5. Asset classification and control
  5.1 Accountability for assets
  5.2 Information classification
6. Personnel security
  6.1 Security in job definition and resourcing
  6.2 User training
  6.3 Responding to security incidents and malfunctions
7. Physical and environmental security
  7.1 Secure areas
  7.2 Equipment security
  7.3 General controls
8. Communications and operations management
  8.1 Operational procedures responsibilities
  8.2 System planning and acceptance
  8.3 Protection against malicious software
  8.4 Housekeeping
  8.5 Network management
  8.6 Media handling and security
  8.7 Exchanges of information and software
9. Access control
  9.1 Business requirement for access control
  9.2 User access management
  9.3 User responsibilities
  9.4 Network access control
  9.5 Operating system access control
  9.6 Application access control
  9.7 Monitoring system access and use
  9.8 Mobile computing and teleworking
10. System development and maintenance
  10.1 Security requirements of systems
  10.2 Security in application systems
  10.3 Cryptographic controls
  10.4 Security of system files
  10.5 Security in development and support processes
11. Business continuity management
  11.1 Aspects of business continuity management
12. Compliance
  12.1 Compliance with legal requirements
  12.2 Reviews of security policy and technical compliance

[9] We use the BS 7799 numbering, starting with 3.

```
12.3 System audit considerations
```

Exhibits

Appendix A.1 presents a photocopy of material from BS 7799.

3.1.2 CobiT

The “Control Objectives for Information and Related Technology” (CobiT) [32] has been developed and is being maintained by a non-profit organization, the IT Governance Institute [72], which we abbreviate in this report as ITGI. The ITGI is part of the Information Systems Audit and Control Association (ISACA) [65]. The latter was formed in 1969 from the EDP[10] Auditor’s Association.[11] CobiT is in its third edition, published in July 2000. The second edition was published in 1998, the first in 1996. The ITGI intends on “updating” CobiT at least every three years ([29], page 70). CobiT was originally based on a document produced by ISACA’s entitled “Control Objectives.” ([29], page 19)

This is how the ITGI describes CobiT’s purpose:

> On the one hand, we have witnessed the development and publication of overall business control models like COSO (Committee of Sponsoring Organisations of the Treadway Commission-Internal Control-Integrated Framework, 1992) [40] in the US, Cadbury in the UK, CoCo [33] in Canada and King in South Africa. On the other hand, an important number of more focused control models are in existence at the level of IT. Good examples of the latter category are the Security Code of Conduct from DTI (Department of Trade and Industry, UK), Information Technology Control Guidelines [71] from CICA (Canadian Institute of Chartered Accountants, Canada) [21], and the Security Handbook from NIST (National Institute of Standards and Technology, US) [69]. However, these focused control models do not provide a comprehensive and usable control model over IT in support of business processes. The purpose of CobiT is to bridge this gap by providing a foundation that is closely linked to business objectives while focusing on IT.
>
> A focus on the business requirements for controls in IT and the application of emerging control models and related international standards evolved the original Information Systems Audit and Control Foundation’s Control Objectives from an auditor’s tool to CobiT, a management tool. Further, the development of IT Management Guidelines has taken CobiT to the next level-providing management with Key Goal Indicators (KGIs), Key Performance Indicators (KPIs), Critical Success Factors (CSFs) and Maturity Models so that it can assess its IT environment and make choices for

[10] Electronic Data Processing.

[11] I do not know when the EDP Auditor’s Foundation began.

> control implementation and control improvements over the organisation's information and related technology.
>
> Hence, the main objective of the CobiT project is the development of clear policies and good practices for security and control in IT for worldwide endorsement by commercial, governmental and professional organisations. It is the goal of the project to develop these control objectives primarily from the business objectives and needs perspective. (This is compliant with the COSO perspective, which is first and foremost a management framework for internal controls.) Subsequently, control objectives have been developed from the audit objectives (certification of financial information, certification of internal control measures, efficiency and effectiveness, etc.) perspective. ([29], page 12) (references not in the original)

Note that the ITGI considers CobiT to be a "bridge" between "business control models," such as COSO and CoCo, and "more focused control models," such as ITCG and the Security Handbook from NIST. And note the ITGI's statement of CobiT's "main objective."

CobiT is intended to be a common framework [55], cumulative instead of exclusive. It explicitly does not exclude any other accepted standard ([29], page 19). It is based on 41 primary reference materials ([29], Appendix III, pages 84-5).

CobiT is based on the notion of "control," adapted from COSO [40] (see also Section 3.1.4), and "control objective," adapted from SAC [100] (see also Section 4.5), which CobiT defines as follows ([28], page 12):

> *Control*: 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.
>
> *IT Control Objective*: A statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity.

New with the 3rd Edition is CobiT's "IT Governance Maturity Model" that provides a methodical path for gauging and thus improving the quality of an organization's processes [30].[12] Like SSAG's levels (see Section 3.2.3), CobiT's maturity model describes six grades or levels that provide a "scorecard" for an organization's processes (see Appendix C). The model is intended to help answer the "perpetual question: 'What is the right level of control for my IT such that it supports my enterprise objectives?'" ([30], page 9) or, put another way, "How far should we go, and is the cost justified by the benefit?" ([30], page 9)

CobiT also provides guidelines on how to evaluate an organization's controls. The "Audit Guidelines" document provides instruction on how to audit each process. This includes whom to interview, what documents to obtain, how to evaluate the controls, how to assess compliance, and how to substantiate the risk of the control objectives not being met. (A sample from the Audit Guidelines is included in the Exhibits below.)

[12] Appendix C compares the names of the maturity levels used by various models presented in this report.

The ITGI provides explicit auditor certification, which, according to the ITGI, is the “only global designation,” known as “Certified Information Systems Auditor” (CISA) [22].

The ITGI considers SysTrust to be the “most closely related” to Cobit of all of the frameworks discussed ([29], page 12). (Control Objectives for Net-Centric Technology (CONCT) is produced and maintained by ISACA and is an “application” of CobiT [32].)

Organization

CobiT is organized into three tiers, as shown in Table 4.

Table 4 CobiT Organization

Tier	Name	Elements
Top	Domains	4
Middle	Processes or High-Level Control Objectives	34
Bottom	Detailed Control Objectives	318

Here are the entire top and middle tiers of CobiT:[13]

```
Planning & Organisation Domain

    PO1  Define a Strategic Information Technology plan
    PO2  Define the Information Architecture
    PO3  Determine Technological Direction
    PO4  Define the Information Technology Organisation and
         Relationships
    PO5  Manage the Information Technology Investment
    PO6  Communicate Management Aims and Direction
    PO7  Manage Human Resources
    PO8  Ensure Compliance with External Requirements
    PO9  Assess Risks
    PO10 Manage Projects
    PO11 Manage Quality

Acquisition & Implementation Domain

    AI1 Identify Automated Solutions
    AI2 Acquire and Maintain Application Software
    AI3 Acquire and Maintain Technology Infrastructure
    AI4 Develop and Maintain Procedures
    AI5 Install and Accredit Systems
    AI6 Manage Changes
```

[13] Reprinted with permission. COBIT: Control Objectives for Information and related Technology. Copyright 1996, 1998, 2000, The IT Governance Institute™ (ITGI™), Rolling Meadows, IL, USA 60008.

Delivery & Support Domain

DS1	Define and Manage Service Levels
DS2	Manage Third-Party Services
DS3	Manage Performance and Capacity
DS4	Ensure Continuous Service
DS5	Ensure Systems Security
DS6	Identify and Allocate Costs
DS7	Educate and Train Users
DS8	Assist and Advise Customers
DS9	Manage the Configuration
DS10	Manage Problems and Incidents
DS11	Manage Data
DS12	Manage Facilities
DS13	Manage Operations

Monitoring Domain

M1	Monitor the Processes
M2	Assess Internal Control Adequacy
M3	Obtain Independent Assurance
M4	Provide for Independent Audit

The organization of the processes and domains is described in the “CobiT Framework” document [28], and all three tiers are described in the “CobiT Control Objectives” document [26].

Exhibits

Appendix A.2 presents photocopies of material from CobiT.

3.1.3 CoCo

The “Guidance on Control” report [33], known colloquially as CoCo, was produced in 1999 by the Criteria of Control Board of The Canadian Institute of Chartered Accountants, the same organization that maintains ITCG [71] (see Section 3.1.6).

CoCo does not cover any aspect of information assurance per se. It is concerned with control in general. CoCo is “guidance,” meaning that it is not intended as “prescriptive minimum requirements” but rather as “useful in making judgements” about “designing, assessing and reporting on the control systems of organizations.” ([34], page 1) As such, CoCo can be seen as a model of controls for information assurance, rather than a set of controls. CoCo’s generality is one of its strengths: if information assurance is just another organizational activity, then the criteria that apply to controls in other areas should apply to this one as well.

CoCo “builds on the concepts in the COSO document.” ([33], page 27). CoCo can be said to be a concise superset of COSO. It uses the same three categories of objectives:

- effectiveness and efficiency of operations
- reliability of financial reporting
- compliance with applicable laws and regulations

CoCo states that the “essence of control is purpose, capability, commitment, and monitoring and learning,” ([33], page 2). These form a cycle that continues endlessly if an organization is to continue to improve. Four important concepts about “control” are as follows ([33], page 3):

1. Control is affected by people throughout the organization, including the board of directors (or its equivalent), management and all other staff.
2. People who are accountable, as individuals or teams, for achieving objectives should also be accountable for the effectiveness of control that supports achievement of those objectives.
3. Organizations are constantly interacting and adapting.
4. Control can be expected to provide only reasonable assurance, not absolute assurance.

Amelia Financial systems considers CoCo’s significance to be that it “further developed control thinking [beyond COSO] by explicitly including the failure to identify and exploit opportunities as a risk for which controls should be specifically assessed” [2].

Organization

CoCo is organized into three tiers, as shown in Table 5.

Table 5 CoCo Organization

Tier	Name	Elements
Top	Criteria	4
Middle		20
Bottom	Issues to Consider	98

The criteria can be assessed, CoCo tells us, by changing each criterion into a question ([33], page 25). For example, the first, middle-tier criterion

```
A1 Objectives should be established and communicated
```

could be assessed by asking the question

```
Do we clearly understand the mission and vision of the
  organization?
```

The Exhibits show the entire top two tiers of CoCo.

Exhibits

Appendix A.3 presents photocopies of material from CoCo.

3.1.4 COSO

The “Internal Control — Integrated Framework” report [40], known colloquially as COSO, was generated by the Committee of Sponsoring Organizations of the Treadway Commission. The latest version of COSO is dated 1994. This report represents an important step in the development of the concept of “control.” The following is a typical description of COSO and its importance:

> In 1985 the National Commission on Fraudulent Financial Reporting, known as the Treadway Commission, was created through the joint sponsorship of the AICPA, American Accounting Association, FEI, IIA and Institute of Management Accountants. Its report, issued in 1987, contained a number of recommendations including a call for sponsoring organizations to work together to integrate the various internal control concepts and definitions. Based on this recommendation, a task force under the auspices of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) conducted a review of internal control literature. The eventual outcome was the 1992 document Internal Control - Integrated Framework.
>
> COSO was important because it emphasised the responsibilities of management for control. It also set definitions for what was included within internal control and the key components of control... [2]

COSO presents the following “fundamental concepts:”

> Internal control is a process. It is a means to an end, not an end in itself.
>
> Internal control is affected by people. It’s not merely policy manuals and forms, but people at every level of an organisation.
>
> Internal control can be expected to provide only reasonable assurance, not absolute assurance, to an entity’s management and board.
>
> Internal control is geared to the achievement of objectives in one or more separate but overlapping areas. ([2], page 13)

COSO defines three categories of control objectives, which CoCo subsequently adopted:

- effectiveness and efficiency of operations
- reliability of financial reporting
- compliance with applicable laws and regulations

Controls can be partitioned into five “components:”

- control environment
- risk assessment
- control activities
- information and communication
- monitoring

Each of the components has an “Evaluation” section that includes what look like control objectives, though they are not given that label. The “Evaluation Tools” in Volume 2 provides a sufficient template for auditing.

Volume 2 also includes a “Reference Manual” using a diagrammatic “Generic Business Model,” based on Porter’s model [94]. Even though CobiT uses the same “business process” model ([29], page 69)), COSO’s use is unique: it partitions 130 activities into three groups: operations, financial reporting, and compliance. For each activity the risks are identified, as well as the associated “Points of Focus.” This approach is unique in the set of models considered in this report.

Organization

COSO is organized into four tiers, as shown in Table 6.

Table 6 COSO Organization

Tier	Name	Elements
Top	Components	5
Second	Points of Focus	16
Third	(unnamed)	~80
Bottom		~250

The entire top and second tiers of COSO are shown below:[14]

```
Control Environment
    Integrity and Ethical Values
    Commitment to Competence
    Board of Directors or Audit Committee
    Management’s Philosophy and Operating Style
    Organizational Structure
    Assignment of Authority and Responsibility
    Human Resource Policies and Practices
Risk Assessment
    Entity-Wide Objectives
    Activity-Level Objectives
    Risks
    Managing Change
Control Activities
    Top Level Reviews
    Direct Functional or Activity Management
    Information Processing
    Physical Controls
    Performance Indicators
Information and Communication
```

[14] Copyright © 1992 by the American Institute of Certified Public Accountants, Inc. Reprinted with permission.

```
        Information
        Communication
    Monitoring
        Ongoing Monitoring
        Separate Evaluations
        Reporting Deficiencies
```

Exhibits

Appendix A.4 presents photocopies of material from COSO.

3.1.5 FISCAM

The “Federal Information Systems Controls Audit Manual” (FISCAM) [46] was produced by the Accounting and Information Management Division of the U. S. General Accounting Office in 1999. The purpose of the manual is described as follows:

> The methodology outlined in this manual provides guidance to auditors in evaluating internal controls over the integrity, confidentiality, and availability of data maintained in [computer-based information] systems. The manual is primarily designed for evaluations for general and application controls over financial information systems that support agency business operations. However, it could also be used when evaluating the general and application controls over computer-processed data from agency program information systems, as called for in Government Auditing Standards.” ([46], page 5)

FISCAM is based on an extended CIA model (see Section 4.1), as should be clear from the preceding passage. For example, the first “Critical Element” in FISCAM is Entitywide Security Program Planning and Management, which is outside the CIA model.

Volume I of FISCAM is entitled “Financial Statement Audits.” Volume II is planned to contain “audit practice aids for addressing specific software products, such as access control software and selected computer operating systems” ([46], page 5).

FISCAM describes a general methodology, followed by guidance on planning an audit, and then, guidance on evaluation of general controls (constituting the bulk of the manual), to be performed by considering a hierarchy of “Critical Elements,” each of which is named as a directive, as in “Periodically assess risks” but is described via goal-oriented language (i.e., what should happen). For each such Critical Element a list of “Control Activities” is listed, along with “Control Techniques” and “Audit Procedures.” These are collected in a 50-page Appendix. A photocopied page from this Appendix is shown in the Exhibits below.

The organization that has generated FISCAM, namely the U. S. Federal Government, will persist, and so will the General Accounting Office. There will continue to be a need for auditing standards for IT systems in the Federal Government. What is not clear is whether or not GAO will adopt commercial standards, such as CobiT. There are obvious benefits in using Commercial Off The Shelf (COTS) products. However, we presume, on somewhat slender evidence, that FISCAM will continue to be supported.

Organization

FISCAM is organized into three tiers, with a small fourth tier, as shown in Table 7.

Table 7 FISCAM Organization

Tier	Name	Elements
Top	Control Activities	6
Second		22
Third		57
Bottom[a]		7

a. This bottom tier would not be needed if one second-tier control activity, namely

AC-3 "Establish physical and logical controls to prevent and detect unauthorized access,"

were divided into two:

"Establish physical controls to prevent and detect unauthorized access,"

and a new

"Establish logical controls to prevent and detect unauthorized access."

The entire top and second tiers of FISCAM are shown below:

Entitywide Security Program Planning and Management (SP)

SP-1 Periodically assess risks.
SP-2 Document an entitywide security program plan.
SP-3 Establish a security management structure and clearly assign security responsibilities.
SP-4 Implement effective security-related personnel policies.
SP-5 Monitor the security program's effectiveness and make changes as needed.

Access Control (AC)

AC-1 Classify information resources according to their criticality and sensitivity.
AC-2 Maintain a current list of authorized users and their access authorized.
AC-3 Establish physical and logical controls to prevent or detect unauthorized access.
AC-4 Monitor access, investigate apparent security violations, and take appropriate remedial action.

Application Software Development and Change Control (CC)

CC-1 Processing features and program modifications are properly authorized.

CC-2 Test and approve all new and revised software.
CC-3 Control software libraries.

System Software (SS)

SS-1 Limit access to system software.
SS-2 Monitor access to and use of system software.
SS-3 Control system software changes.

Segregation of Duties (SD)

SD-1 Segregate incompatible duties and establish related policies.
SD-2 Establish access control to enforce segregation of duties.
SD-3 Control personnel activities through formal operating procedures and supervision and review.

Service Continuity (SC)

SC-1 Assess the criticality and sensitivity of computerized operations and identify supporting resources.
SD-2 Take steps to prevent and minimize potential damage and interruption.
SC-3 Develop and document a comprehensive contingency plan.
SC-4 Periodically test the contingency plan and adjust it as appropriate.

Exhibits

Appendix A.5 presents photocopies of material from FISCAM.

3.1.6 ITCG

The “Information Technology Control Guidelines” [71], abbreviated as ITCG in this report, was developed and is maintained by the Canadian Institute of Chartered Accountants (CICA) [21]. ITCG is currently in its 3rd edition, published in 1998. The second edition was published in 1986. The first edition was published in 1970 as “Computer Control Guidelines.”

ITCG uses the CoCo report [33] (see Section 3.1.3) but is more narrowly focused on the risks involved with the use of IT, as the name implies. Enterprise-wide issues such as “shared ethical values and integrity, human resources policies, and trust” ([71], page 11) are in the purview of CoCo but not ITCG.

ITCG is explicitly role-based. It speaks of controls to be performed by people who hold various roles in an organization, such as Senior Management, Chief Information Officer, Owners, Custodians, and so on.

There does not appear to be a certification scheme associated with ITCG. The current edition of ITCG was written by a team of “Computer Assurance service specialists for the accounting firm of Deloitte & Touche” ([71], page V), many of whom are CISAs [22], indicating a familiarity with CobiT. Deloitte & Touche is described as the “Principal Author” of the ITCG. We presume that those authors were presuming that ITCG would be used by people like themselves, already accredited and most likely CAs, so there may have been no perceived need for a certification scheme.

ITCG can trace its roots back to at least 1970. It has the financial support of Deloitte & Touche and the organizational support of the Canadian Institute of Chartered Accountants. It appears in both of their interests to continue support. We anticipate continued support for ITCG.

Organization

ITCG is organized into four tiers, as shown in Table 8.

Table 8 ITCG Organization

Tier	Name	Elements
Top	Chapters	7
Second	Control Objectives	31
Third	Minimum Control Standards	~ 160
Bottom	Control Techniques	~ 400

The names of the tiers require the following definitions ([71], page 37):

> *Objectives*: “strategic, tactical, divisional, departmental and individual plans of the enterprise. Objectives are the starting point for effective risk management.”
>
> *Control*: “those elements of an enterprise (i.e., its resources, systems, processes, culture, structure and tasks) that, taken together, support people in the achievement of the enterprise’s objectives. The extent of control that should be implemented is the essence of the risk management process. The desire to minimize risk is balanced against the cost of implementing and maintaining control and the net result is a residual risk or exposure.”
>
> *Minimum control standards*: “represent criteria that should be met if the relevant control objective is to be achieved.”
>
> *Control techniques*: (not formally defined).

Here are the entire top and second tiers of ITCG: [15]

    [2][16] Responsibility for Risk Management and Control

[15] Reproduced from the “Information Technology Control Guidelines” [71] with the permission of the Canadian Institute of Chartered Accountants.

A To ensure than an enterprise-wide culture exists to support the identification, assessment and management of information technology risk.

B To ensure that information technology risk is effectively managed at all levels within the enterprise.

[3] Information Technology Planning

C To ensure that an effective and efficient information technology planning process is established.

D To ensure that information technology strategic and tactical plans are adhered to, and support the enterprise objectives and business strategy, and appropriately consider risks.

E To ensure the development and communication of information technology strategic and tactical plans.

F To ensure information technology plans are effectively implemented, and results are effectively monitored and used.

G To ensure overall information technology performance is effectively measured.

[4] Information Systems Acquisition, Development and Maintenance

H To ensure an effective and efficient process for systems development and acquisition.

I To ensure efficient and effective project management of systems development and acquisition.

J To ensure that systems developed and acquired meet relevant requirements and that identified risks are managed.

K To ensure the efficient and effective development and acquisition of information systems.

L To ensure the efficient and effective implementation of developed and acquired systems.

M To ensure systems continue to meet business and technical requirements.

[5] Computer Operations and Information Systems Support

Computer Operations

N To ensure that operations services are appropriately controlled and meet defined user requirements efficiently and effectively.

O To ensure the integrity and availability of computer

[16] The controls for ITCG begin in Chapter 2.

operations services.

Information Systems Support

P To ensure that systems software procedures and activities contribute to the reliability, effectiveness and control of computer operations services.
Q To ensure that appropriate controls are established over information transmitted to and from outside organizations.
R To ensure that appropriate controls are established over data management activities.
S To ensure that end-user computing activities are appropriately supported and controlled.

[6] Information Technology Security

T To ensure the integrity, confidentiality and availability of information technology processing throughout the enterprise.
U To ensure that access to the enterprise’s systems and information is reliably controlled.
V To ensure that information technology resources are housed and operated in appropriate environmental conditions.
W To ensure that appropriate consideration is given to security issues and technical skills when management and staff are hired into information technology positions.
X To ensure that information technology security is operated in an efficient and effective manner.

[7] Business Continuity Planning and Information Technology Recovery

Y To ensure that critical business processes can continue, or be resumed promptly, in the event of significant disruption to normal business operations (business continuity planning).
Z To ensure that critical information systems processing functions can continue or be resumed promptly in the event of significant disruption to normal computer operations (Information technology recovery planning).

[8] Application Based Controls

AA To ensure that application controls are designed with due regard to business requirements and business risk analysis.
BB To ensure that application controls are only relied upon

```
   with due regard to the overall condition of information
   technology operation and support.
CC To ensure that information stored by and delivered to
   applications is complete, accurate and authorized.
DD To ensure that information processed and provided by
   applications is complete, accurate, and authorized.
EE To ensure that sufficient evidence is created and
   maintained to provide a complete management trail.
```

Exhibits

Appendix A.8 presents photocopies of material from ITCG.

3.1.7 SysTrust

"AICPA / CICA SysTrust Principles and Criteria for System Reliability" [111], known colloquially and in this report as SysTrust, has been developed and is maintained by the American Institute of Chartered Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA). The document is intended for auditors. It is built on the CIA model (see Section 4.1) with "maintainability" added in. The current version is 2.0, dated January 2001; version 1.0 was dated November 1999. SysTrust is intended to provide "assurance on the reliability of systems" ([111], page 1) in the following way:

> In general, the objective of a SysTrust engagement [e.g. audit] is for the practitioner to issue a report on whether management maintained effective controls over its system based on the fifty-eight criteria presented...in this document. The practitioner determines whether controls over the system exist and performs tests to determine whether those controls were operating effectively during the period covered by the attestation / assurance report. ([111], page 11)

There does not appear to be an explicit certification scheme associated with SysTrust, such as c:cure with BS 7799 [13]. However, SysTrust is intended as part of a "professional service:"

> The SysTrust service is an assurance service developed by the Assurance Services Executive Committee (ASEC) of the AICPA and the Assurance Services Development Board (ASDB) of the CICA to be provided by a certified public accountant or a chartered accountant (hereinafter, referred to as practitioner). ([111], page 1)

SysTrust defines "system security" to be protection against unauthorized physical and logical access, including some aspects of privacy ([111], page 4).

SysTrust also includes what it calls "Illustrative Controls," which are examples of controls. These illustrative examples were developed with explicit use ([111], page 10) of CobiT [32], the control guidelines from CICA [71], and material from COSO [40], and CoCo [33].

Organization

SysTrust is organized into three tiers, as shown in Table 9.

Table 9 SysTrust Organization

Tier	Name	Elements
Top	Principles	4
Middle	Criteria	12
Bottom		58

Here are the entire top and middle tiers of SysTrust:[17]

Availability

A1 The entity has defined and communicated performance objectives, policies, and standards for systems availability.

A2 The entity uses procedures, people, software, data, and infrastructure to achieve system availability objectives in accordance with established policies and standards.

A3 The entity monitors the system and takes action to achieve compliance with system availability objectives, policies, and standards.

Security ←This is known as “Confidentiality” in the CIA model.

S1 The entity has defined and communicated performance objectives, policies, and standards for systems security.

S2 The entity uses procedures, people, software, data, and infrastructure to achieve system security objectives in accordance with established policies and standards.

S3 The entity monitors the system and takes action to achieve compliance with system security objectives, policies, and standards.

Integrity

I1 The entity has defined and communicated performance objectives, policies, and standards for systems integrity.

I2 The entity uses procedures, people, software, data, and infrastructure to achieve system integrity objectives in accordance with established policies and standards.

I3 The entity monitors the system and takes action to achieve

[17] Copyright © 2000 by American Institute of Certified Public Accountants, Inc., and Canadian Institute of Chartered Accountants. Used with permission.

compliance with system integrity objectives, policies, and standards.

Maintenance

M1 The entity has defined and communicated performance objectives, policies, and standards for systems maintainability.

M2 The entity uses procedures, people, software, data, and infrastructure to achieve system maintainability objectives in accordance with established policies and standards.

M3 The entity monitors the system and takes action to achieve compliance with system maintainability objectives, policies, and standards.

Exhibits

Appendix A.11 presents a photocopy of material from SysTrust.

3.2 Principles Community

The models in this community are based on the notion of principles, such as accountability, awareness, and ethics, the first three for GAPP. This community has the following members: GAPP, GASSP, and SSAG. (There are a number of books that expand sets of principles and practices. For example, Garfinkel & Spafford’s book [52] (see Section 4.3.2), Allen’s [1], Pipkin’s [93], and Wood (see Section 4.4.4) (and [117]).)

3.2.1 GAPP

Swanson & Guttman of the U.S. National Institute of Standards and Technology (NIST) provide a set of “generally accepted principles and practices” (GAPP) [51], published in 1998. They present eight “Generally Accepted System Security Principles,” and a set of “Common IT Security Practices.” The former are intended as a “guide when creating program policy or reviewing existing policy,” and the latter are intended as a “reference document and an auditing tool” ([51], page 3). GAPP traces it roots to BS 7799 [12] and to OECD [87].

GAPP’s strength is its simplicity. In only 55 pages, GAPP presents a convincing definition of information assurance.

There are three related NIST documents. The “Introduction to Computer Security” [69] is a high-level discussion of the area. The “Guide for Developing Security Plans for Information Technology Systems” [51] has a narrower focus than GAPP. And the “Guide to Auditing for Controls and Security” [99] is for system development.

Organization

GAPP is organized into three tiers, as shown in Table 10.

Table 10 GAPP Organization (Practices)

Tier	Name	Elements
Top	(unnamed)[a]	14
Middle		34
Bottom		~100

[a] The top and middle tiers are numbered but the bottom tier is identified only with a symbol that looks like ❑.

The top and middle tiers of GAPP are shown in the Exhibits.

Exhibits

Appendix A.6 presents photocopies of material from GAPP.

3.2.2 GASSP

“GASSP (Generally Accepted System Security Principles)” [53] is the product of the International Information Security Foundation (I^{2}SF). The document is the result of an international effort in response to the first recommendation in the seminal study “Computers at Risk” [83], namely that comprehensive, generally accepted system security principles be promulgated. The GASSP Committee officially began at the 1992 National Security Conference in Baltimore, Maryland. It included people from a variety of backgrounds, including Charles LeGrand, the Director of Research at The IIA and the driving force behind SAC (see Section 4.5), and Harold Tipton, co-editor of the three-volume Information Security Management Handbook [112], one of the key references for the Common Body of Knowledge required for the CISSP title [23]. GASSP is built on the “Information Security Principles” developed by OECD [87] (see Section 4.4.1). GASSP uses the same principles as OECD, presented in the same order and with the same names, with one exception: what OECD calls “Democracy,” GASSP calls “Equity.”[18] GASSP has developed two additional levels of principles, one of which is populated.

The GASSP Committee published the current version of GASSP in June 1997. They appear to be active and involved with the continued development and maintenance of the principles.

Organization

GASSP is organized into three levels, not tiers, the difference being that there is not exactly one path from an element on a lower level to the root (see Figure 4, “Structures,” on page 7). The

[18] FISCAM [46] (see Section 3.1.5) uses the same principles, with two exceptions. First, it does not include Ethics. And second, what OECD calls “Democracy” and GASSP calls “Equity,” FISCAM calls “Societal Factors” ([46], page 273) (see also Section 3.1.5).

organization is shown in Table 11.

Table 11 GASSP Organization

Level	Name	Elements
Top	Pervasive Principles[a]	9
Middle	Broad Functional Principles	14
Bottom	Detailed Security Principles	0[b]

[a] These are the same as those presented by OECD with the exception of one name change, as noted in the text above.

[b] This bottom level has not yet been populated.

The nine Pervasive Principles expand on the CIA model (see Section 4.1) and are as follows, with explanatory notes:

PP-1 Accountability
    --assign it
PP-2 Awareness
PP-3 Ethics
PP-4 Multidisciplinary
    --represent everyone’s interests
PP-5 Proportionality
    --balance costs for controls and risks
PP-6 Integration
    --make security pervasive
PP-7 Timeliness
PP-8 Assessment
    --do it periodically
PP-9 Equity
    --respect human rights and dignity

The fourteen Broad Functional Principles are as follows:

BFP-1 Information Security Policy
BFP-2 Education and Awareness
BFP-3 Accountability
BFP-4 Information Management
BFP-5 Environmental Management
BFP-6 Personnel Qualifications
BFP-7 System Integrity
BFP-8 Information Systems Life Cycle
BFP-9 Access Control
BFP-10 Operational Continuity and Contingency Planning
BFP-11 Information Risk Management
BFP-12 Network and Infrastructure Security
BFP-13 Legal, Regulatory, and Contractural Requirements of Information Security
BFP-14 Ethical Practices

Each PP and BFP is presented with a Rationale and Example.

The relationship between PPs and BFPs is many-to-many and is presented explicitly in Figure 2.2-1 on page 21 of the GASSP document [53] (see Appendix A.7). For example, BFP-1 applies to all of the Pervasive Principles, but BFP-2 applies only to PP-1 through PP-4 and to PP-9.

Exhibits

Appendix A.7 presents photocopies of material from GASSP.

3.2.3 SSAG

The "System Self-Assessment Guide for Information Technology Systems" [107], abbreviated as SSAG in this report, was, like GAPP (see Section 3.2.1), developed by NIST [85]. We presume that NIST intends on maintaining it. SSAG was published in November 2001, making it very recent. It is, as its title implies, a self-assessment method. It is concise and well-structured. It is explicitly not a risk assessment, nor is it intended to be comprehensive. The goal of the document is to "provide a standardized approach to assessing a system" ([107], page 2). Audit techniques are explicitly beyond the scope of the document.

SSAG consists primarily of a questionnaire. It is focused on the CIA model (see Section 4.1). Each item in the questionnaire is to be ranked based on the following five levels:

Level 1 — Control objective documented in a security policy
Level 2 — Security controls documented as procedures
Level 3 — Procedures have been implemented
Level 4 — Procedures and security controls are tested and reviewed
Level 5 — Procedures and security controls are fully integrated into a comprehensive program ([107], page 10)[19]

These levels are based on those in the "Federal Information Technology Security Assessment Framework" [45], upon which SSAG is based (see Appendix C). SSAG also uses FISCAM, GAPP, and various other NIST documents. SSAG appears to be more of a complement to these other documents than a replacement for them.

Though the term "control objective" is used to describe the lowest tier in SSAG, the items on that lowest tier are closer to a checklist. They are light on "desired result" and heavy on eliciting Yes / No responses. For example, the first, fourth-tier item is as follows: "1.1.1 Is the current system configuration documented, including links to other systems?"

[19] Appendix C compares the names of the maturity levels used by various items presented in this report.

Organization

SSAG is organized into four tiers, as shown in Table 12.

Table 12 SSAG Organization

Tier	Name	Elements
Top	Control Area	3
Second	Topic Area	17
Third	Critical Element	36
Bottom[a]	Specific Control Objectives and Techniques	174

[a] For some of the Critical Elements, SSAG provides groupings of the specific control objectives and techniques. We do not consider these groupings to constitute an additional tier.

All of the top, second, and third tiers of SSAG are shown below:

```
Management Controls

    1. Risk Management
         1.1 Is risk periodically assessed?
         1.2 Do program officials understand the risk to systems
             under their control and determine the acceptable
             level of risk?
    2. Review of Security Controls
         2.1 Have the security controls of the system and
             interconnected systems been reviewed?
         2.2 Does management ensure that corrective actions are
             effectively implemented?
    3. Life Cycle
         3.1 Has a system development life cycle methodology been
             developed?
         3.2 Are changes controlled as programs progress through
             testing to final approval?
    4. Authorize Processing (Certification & Accreditations)
         4.1 Has the system been certified/recertified and
             authorized to process (accredited)?
         4.2 Is the system operating on an interim authority to
             process in accordance with specified agency
             procedures?
    5. System Security Plan
         5.1 Is a system security plan documented for the system
             and all interconnected systems if the boundary
             controls are ineffective?
         5.2 Is the plan kept current?
```

Operational Controls

6. Personnel Security
    - 6.1 Are duties separated to ensure least privilege and individual accountability?
    - 6.2 Is appropriate background screening for assigned positions completed prior to granting access?
7. Physical and Environmental Protection
    - 7.1 Have adequate physical security controls been implemented that are commensurate with the risks of physical damage or access?
    - 7.2 Is data protected from interception?
    - 7.3 Are mobile and portable systems protected?
8. Production, Input/Output Controls
    - 8.1 Is there user support
    - 8.2 Are there media controls?
9. Contingency Planning
    - 9.1 Have the most critical and sensitive operations and their supporting computer resources been identified?
    - 9.2 Has a comprehensive contingency plan been developed and documented?
    - 9.3 Are tested contingency/disaster recovery plans in place?
10. Hardware and System Software Maintenance
    - 10.1 Is access limited to system software and hardware?
    - 10.2 Are all new and revised hardware and software authorized, tested and approved before implementation?
    - 10.3 Are systems managed to reduce vulnerabilities?
11. Data Integrity
    - 11.1 Is virus detection and elimination software installed and activated?
    - 11.2 Are data integrity and validation controls used to provide assurance that the information has not been altered and the system functions as intended?
12. Documentation
    - 12.1 Is there sufficient documentation that explains how software/hardware is to be used?
    - 12.2 Are there formal security and operational procedures documented?
13. Security Awareness, Training, and Education
    - 13.1 Have employees received adequate training to fulfill their security responsibilities?
14. Incident Response Capability
    - 14.1 Is there a capability to provide help to users when a security incident occurs in the system?
    - 14.2 Is incident related information shared with

appropriate organizations?

Technical Controls

15. Identification and Authentication
    - 15.1 Are users individually authenticated via passwords, tokens, or other devices?
    - 15.2 Are access controls enforcing segregation of duties?
16. Logical Access Controls
    - 16.1 Do the logical access controls restrict users to authorized transactions and functions?
    - 16.2 Are there logical controls over network access?
    - 16.3 If the public accesses the system, are there controls implemented to protect the integrity of the application and the confidence of the public?
17. Audit Trails
    - 17.1 Is activity involving access to and modification of sensitive or critical files logged, monitored, and possible security violations investigated?

Exhibits

Appendix A.9 presents photocopies of material from SSAG.

3.3 Capability Maturity Community

The models in this community are based on the notion of the Maturity Model, which we will explain below. This community has only one member: SSE-CMM.

3.3.1 SSE-CMM

The “Systems Security Engineering Capability Maturity Model” (SSE-CMM) [109], published in 1999, is process-centric, based on the hypothesis that bettering the process will better the product. This is an application of Humphrey’s [60] application of Deming’s model of process control [42]: if the system is in “statistical process control,” then its output is predictable; if a process that is in statistical control is bettered, then, according to the model, the product will simultaneously be bettered.

The generic model consists of a sequence of “maturity levels,” each of which is characterized by a set of activities. The sets of activities are intended to be cumulative: the activities of level n are subsumed by the activities of level n+1. The theory is that an organization whose maturity level is n is likely to produce a better product or service than an organization whose maturity level is less than n. An organization uses the model by orchestrating a sequence of developmental steps that will, over time, increase its maturity level. Note that the focus is on the process, and only secondarily on the product.

SSE-CMM defines 5 “Capability Levels,” each consisting of “Common Features” (there are 11 total Common Features, numbered 1.1 through 5.1), and 22 “Process Areas” (numbered PA01 through PA22). These are combined to show a maturity level in a “Summary Chart” ([109], page 43), as exemplified in Table 13.

Table 13 Example SSE-CMM Summary Chart

Common Features	5.1				
	…				
	2.2		▨		
	2.1	▨	▨		
	1.1	▨	▨		▨
		PA01	PA02	…	PA22
		Process Areas			

The darkened cells in Table 13 indicate Common Features that are being adequately performed for various Process Areas for an example organization. Note that the darkened cells are contiguous and begin with the lowest Common Feature. The Common Features are cumulative: it should be impossible to adequately perform a higher Common Feature and simultaneously inadequately perform a lower Common Feature. The Table shows that our example organization performs the first two Common Features for PA01 adequately, the first three Common Features for PA02, but only the first Common Feature for PA22. If all Common Features were of equal importance to the organization, then this chart would indicate that the organization should work on PA22 first, then PA01, then PA02. SSE-CMM’s value is that it can make visual the current position of an organization and enable the organization to more easily prioritize efforts and track its progress.

This approach is part of a community led by the Software Engineering Institute (SEI) [106] at Carnegie Mellon University (CMU) [24] that has developed a variety of process-centric models [16], which they refer to as Capability Maturity Models ®, such as

- Capability Maturity Model Integration (CMMISM),
- the SW-CMM ® Capability Maturity Model for Software,
- the P-CMM People Capability Maturity Model,
- the SA-CMM Software Acquisition Capability Maturity Model, the SE-CMM Systems Engineering Capability Maturity Model, and
- the IPD-CMM Integrated Product Development Capability Maturity Model.

SSE-CMM is sponsored by the National Security Agency (NSA), the Office of the Secretary of Defense, and the Communications Security Establishment in Canada, with approximately 60 organizations participating in its development. Although SSE-CMM is in its second version, there is no encouragement from the documentation of commitments for support. The assumption we have to make is that it will not be supported.

SSE-CMM is outside the control objectives community that traces its roots to COSO. The “Participating Organizations” do not appear to include any from that community. SSE-CMM compares itself to none of those organizations. And the concept of “controls” that is so fundamental to that community appears in only one Process Area: PA01 “Administer Security Controls.”

SSE-CMM provides an “Appraisal Method” [110], the full title of which is the “System Security Engineering Capability Maturity Model (SSE-CMM) Appraisal Method” and is abbreviated to SSAM. The method is finely detailed, specifying roles and phases (i.e., planning, preparation, onsite, and reporting), with direction on (a) administering the 89 page, Yes / No / Don’t Know questionnaire for the set of Best Practices, (b) gathering evidence, (c) the meetings to be held (including slides for the opening and closing briefings), and (d) the schedule (to the minute) of the five-day on-site visit, all of which require a total of 1002 man-hours (1/2 man-year). Others would call this an “audit.”

Organization

SSE-CMM consists of two independent hierarchies, one for the Capability Dimension and a second one for the two Process Areas. The hierarchy for the Capability Dimension is shown in Table 14.

Table 14 SSE-CMM Capability Dimension Organization

Tier	Name	Elements
Top	Capability Levels	5
Middle	Common Features	12
Bottom	Generic Practices (GP)	29

The top and middle tiers of the Capability Dimension are shown below:[20]

```
Capability Level 1[21] – Performed Informally
    Common Practice 1.1 – Base Practices are Performed
Capability Level 2 – Planned and Tracked
    Common Practice 2.1 – Planning Performance
    Common Practice 2.2 – Discipline Performance
    Common Practice 2.2 – Verifying Performance
    Common Practice 2.2 – Tracking Performance
Capability Level 3 – Well Defined
    Common Practice 3.1 – Defining a Standard Process
    Common Practice 3.2 – Perform a Defined Process
    Common Practice 3.3 – Coordinate Practices
Capability Level 4 – Quantitatively Controlled
    Common Practice 4.1 – Establishing Measurable Quality Goals
    Common Practice 4.2 – Objectively Managing Performance
Capability Level 5 – Continuously Improving
    Common Practice 5.1 – Improving Organization Capability
    Common Practice 5.2 – Improving Process Effectiveness
```

[20] Copyright © 1999 System Security Engineering Capability Maturity Model (SSE-CMM) Project.

[21] Appendix C compares the names of the maturity levels used by various items presented in this report.

The hierarchy for the Process Areas is shown in Table 15.

Table 15 SSE-CMM Process Area Organization

Tier	Name	Elements
Top	groups, named as follows: "Security Base Practices" (also listed as "Security Engineering Process Area"), and "Project and Organizational Process Area"	2
Middle	Process Areas (PA)	22
Bottom	Base Practices (BP)	128

The top and middle tiers of the Process Areas are shown below:[22]

```
Security Base Practices
    PA01[23] Administer Security Controls
    PA02 Assess Impact
    PA03 Assess Security Risk
    PA04 Assess Threat
    PA05 Assess Vulnerability
    PA06 Building Assurance Argument
    PA07 Coordinate Security
    PA08 Monitor Security Posture
    PA09 Provide Security Input
    PA10 Specify Security Needs
    PA11 Verify and Validate Security
Project and Organizational Base Practices
    PA12 Ensure Quality
    PA13 Manage Configurations
    PA14 Manage Project Risk
    PA15 Monitor and Control Technical Effort
    PA16 Plan Technical Effort
    PA17 Define Organization’s Systems Engineering Process
    PA18 Improve Organization’s System Engineering Processes
    PA19 Manage Product Line Evolution
    PA20 Manage Systems Engineering Support Environment
    PA21 Provide Ongoing Skills and Knowledge
    PA22 Coordinate with Suppliers
```

[22] Copyright © 1999 System Security Engineering Capability Maturity Model (SSE-CMM) Project.

[23] PA is an abbreviation for "Process Area."

Exhibits

Appendix A.10 presents photocopies of material from SSE-CMM.

4 Other Models

> The goal in designing information security is to minimize the total costs of the security procedures, including the losses which the organization shall inevitably occur. [54]
>
> Security is a process, not a product. [103]

In this Section we present other models, in addition to those presented in Section 3. In particular,

- the CIA model,
- proprietary models,
- checklists,
- principles (except for GAPP (see Section 3.2.1)),
- SAC,
- a risk assessment method known as CSA,
- OCTAVE,
- the Common Criteria,
- a number of “attack” taxonomies, and finally,
- a list of other models that we know in name only.

Some of the items are included for historical purposes. Photocopied material from several of these models is shown in Appendix B.

4.1 The CIA Model

Information security, a subset of information assurance, is often referred to as “computer security,” and is usually defined to consist of three parts: confidentiality, integrity, and availability. This is acronymically referred to as the CIA model (or CIA security model).

It is difficult to cover a landscape with only three tiles, so to speak, so there has been continued dissatisfaction with this model. That dissatisfaction is evidenced by proposed synonymic sets of terms, perhaps in hopes that different names will increase the coverage, such as

- disclosure, integrity, and denial of service [111], or
- leakage, corruption, and denial [35], or
- disclosure of information, corruption of information, and denial of service [58], or
- exposure, erroneous output, and denial of service [79], or
- disclosure, modification, and delay [80], or
- exclusivity, integrity, and assured service [90], or
- confidentiality & possession, integrity & authenticity, and availability & utility [89], or
- unauthorised disclosure, modification, and loss of use ([37], part 1, page 2), or

- damaging disclosure of the asset to unauthorised recipients (loss of confidentiality), damage to the asset through unauthorised modification (loss of integrity), or unauthorised deprivation of access to the asset (loss of availability) ([37], part 1, page 14).

Each of these suggested sets of terms may help us understand the nature of the terms better, but they do not increase the number of tiles.

Moving in the other direction, since integrity can provide confidentiality [97], the CIA model could actually be reduced to only two tiles.[24] This is similar to a model for a long life: stay healthy and avoid accidents. Sound advice, to be sure, but it leaves a person wanting details.

4.2 Proprietary Models

Several of the big accounting firms have their own models, such as ESA and ISF. Since these are proprietary, they have the appearance of insufficient breadth and depth.

The “Enterprise Security Architecture” (ESA) [11], for example, appears to be proprietary to PriceWaterhouseCoopers, as the “Information Security Framework” (ISF) [56] appears to be proprietary to Arthur Andersen. These approaches, and others from the big accounting firms, may provide breadth, depth, and be maintained, but because they are proprietary it is difficult to evaluate them. (The big accounting firms have also been involved with non-proprietary efforts. For example, PriceWaterhouseCoopers has “supported and sponsored” development of CobiT, presented in Section 3.1.2. The same firm, when it was known as Price Waterhouse, was the “project researcher” for SAC, presented in Section 4.5. Deloitte & Touche is the “Principal Author” of ITCG, presented in Section 3.1.6. We do not know what packages Ernst & Young and KPMG use or have supported.)

Levine, for example, describes 19 “auditing and related packages,” some of which, we presume, are of this type [77]. Who knows how many others there are?

4.3 Checklists

Checklist models are lists of specific questions, which, taken in the aggregate, are intended to provide information assurance. Each question in a checklist is intended to be sufficiently concise that an answer can be confined to a small, pre-defined set, such as Yes / No, or Yes / No / Don’t Know, or with a narrow range of integers, such as 1 through 4. The questions can be weighted, and a (subjective) security index in the form of a ratio can be calculated by dividing the sum of the weights of the questions answered “Yes” by the sum of the weights of the questions answered “No.”

The appealing aspect of these models is their straightforward application.

We present a number of checklists below. In the interest of space, only the structure of each checklist is shown, with a limited number of control questions included. The integers in parenthesis indicate the number of items in each subtree.

[24] Schneier goes even further, reducing to one tile by arguing that the three “all boil down to access control” [103].

4.3.1 CIAO Practices

The Critical Infrastructure Assurance Office (CIAO) published the “Practices for Securing Critical Information Assets” [20] in 2000. Though the title uses the word “practices,” it is a checklist, as will be seen below. This is “intended to assist agency personnel who are responsible for developing and implementing information security policy, rather than those involved in devising actual technical solutions.... It is not intended to be either definitive or complete. It is a compilation of good information.” ([20], page 1) The document has Chapters on security policies, identifying assets, “tools and practices,” and incident planning. Direction is given on performing an assessment, including the “CIAO Infrastructure Asset Evaluation Survey” ([20], page 10) and a “Vulnerability Audit Questionnaire” that is a two-tiered taxonomy, the top tier of which we show in its entirety below (we also show a few of the second-tier items):

1. Policy
    a. Does your organization have a written security policy?
    b. Does the policy identify all individuals responsible for implementing that policy and what their duties are?
    --5 additional items not shown
2. Risk management
3. Account management
    a. What is the procedure for establishing accounts? What level of supervisor approval is required?
    b. Who has root access to the information on your systems?
    --5 additional items not shown
4. Configuration management
5. Authentication
6. Session controls
    a. Is logoff at the end of the day required?
    --5 additional items not shown
7. Network security
8. Modems
9. Cryptographic technology capability
10. System administration
11. Incident response capability
12. Auditing
13. Viruses
14. Contingency planning
15. Backups
16. Maintenance
17. Labeling
18. Media sanitizing/disposal
19. Physical security
20. Personnel Security
21. Training and awareness

The “tools and practices” Chapter provides dozens of “sound practices,” such as “Do not arouse unnecessary interest in your critical facilities. For example, do not include them on visitor tours.” and what firewalls can and cannot do (([20], page 27).

4.3.2 Garfinkel & Spafford

Appendix A of Garfinkel & Spafford's book on UNIX and Internet security, published in 1996, is an index to the book but reads like a checklist [52]. A few of the approximately 300 items in the checklist are shown below:

- Assess your environment. What do you need to protect? What are you protecting against?
- Be sure that every person who uses your computer has his or her own account.
- Never write SUID / SGID shell scripts.
- Never use *rot13* as an encryption method to protect data.
- Make regular backups.
- If you need to set up an account that can run only a few commands, use the *rsh* restricted shell.
- Develop a physical security plan that includes a description of your assets, environment, threats, perimeter, and defenses.
- Routinely examine your *inetd* configuration file.

Although this checklist is focused on Unix, it is large enough and broad enough to fit in this category. However, Garfinkel & Spafford do not provide a way to quantify one's security status via their checklist.

4.3.3 Levine

Levine, in a generic paper on auditing computer security published in 1995, presented 95 controls in a two-tiered taxonomy.The entire top tier of the structure, along with an item or two of the second tier, is shown below [76]:

```
Job Functions
    Who may enter the computer room?
Computer Operations
    Who reviews the logs?
Software Testing
Systems Development: New Systems
Application Program Modifications
Testing
Immediate Modifications
Acceptance and Implementation
    How does the company ensure that all unauthorized use of the
      libraries is detected?
```

4.3.4 Vallabhaneni

Vallabhaneni in 1989 presented a two-tiered taxonomy with five items at the top tier. The entire top tier of the structure, along with an item or two of the second tier, is shown below [114]:

```
Directive (management actions) (18)
```

```
        Establish a computer security management (steering) committee
    Preventive (standards, guidelines, methods, practices) (44)
        Administer a good user ID and password program
    Detective (feedback about preventive controls) (32)
        Require all employees to wear badges
    Corrective (repairing errors) (14)
    Recovery (backup & recovery from interruption) (8)
```

4.3.5 GAO Audit Guide

The U.S. General Accounting Office in 1988 provided an “audit guide” for “evaluating internal controls in computer-based systems” [47]. This was intended to be a comprehensive guide. Three sets of checklists were provided, with sub-categories in each, effectively forming a three-tiered taxonomy (several third-tier items are shown):

```
    1. Top Management controls
        Q1 Executive ADP Management Committee (7)
            Does the agency have an executive ADP[25] management
            committee?
        Q2 Internal Audit (25)
            Is the agency’s ADP-related internal audit function
            documented?
        Q3 External Audits and Studies (20)
            Has the agency been included in a Government-wide ADP
            review?
    2. General Controls over the Data processing Function
        Q4 Organizational Controls (8)
            Is the ADP function independent from other agency
            operations?
        Q5 System Design, Development, and Modification Controls (138)
        Q6 Data Center Management Controls (56)
        Q7 Data Center Protection Controls (102)
        Q8 System Software Controls (127)
        Q9 Hardware Controls (41
    3. Controls over the Computer Application
        Q10 Data Origination Controls (27)
        Q11 Data Input Controls (136)
        Q12 Data Processing Controls (125)
        Q13 Data Output Controls (121)
```

4.3.6 Wood’s Comprehensive Controls Checklist

Wood et al. in 1987 developed a “Comprehensive Controls Checklist” for Los Alamos National Laboratories [115]. This has the most control questions (857) of any we reviewed. They provide a three-tiered checklist.

[25] Automated Data Processing.

Here are the entire the top and middle tiers, and several bottom-tiered items:[26]

```
Security
    Personnel Policies (35)
        Are computer security related policies generally
        understood by staff?
    Systems Development (37)
        Is the system development process supported by a
        structured development and documentation methodology?
    Training/Awareness (21)
    Organization Structure (26)
    Physical Access (57)
    Data and Program Access (105)
    Input/Output (100)
    Processing Operations (85)
    Database and Systems Software (81)
    Telecommunications (120)
    Visual Display Terminal Human Factors (71)
Survivability
    Environment (45)
    Backup and Recovery (74)
```

A system of “weight-importance,” as described above, is provided to enable quantification of the review.

4.3.7 Krauss

Krauss in 1980 developed a two-tiered “audit and field evaluation” guide intended to be comprehensive [75]. The purpose of the guide is to provide for the reader “a systematic review of EDP[27]-related security and controls.”

The top tier consists of 11 items, including controls for personnel (66), physical access (161), operations (76), contingency plans (63), maintenance (54), data bases (101), communications (114), access control (89), insurance (17), planning (45), and applications (58).

Here are two examples of bottom-tiered items:

```
(2.002.0) Are data processing employees required to wear
          identification badges while they are on the premises?
(8.003.0) Is a current copy of the operating system, other systems
          software packages, and the parameter libraries stored in
          a secure off-site location?
```

[26] Reprinted with permission from Lawrence Livermore National Laboratory. Credit must be given to the University of California, Lawrence Livermore National Laboratory, and the Department of Energy under whose auspices the work was performed, when this information or a reproduction is used. The U.S. Government retains the right to non-exclusive, royalty-free license in and to any copyright covering this material.

[27] Electronic Data Processing.

Krauss provides a system of “suggested weights” and range values that provide a simple way to quantify the results.

4.3.8 System-Specific Checklists

On a smaller scale are system-specific checklists. These checklists present problems and solutions for specific systems. For example, the “UNIX Computer Security Checklist” from the Australian Computer Emergency Response Team discusses what to do with certain files, such as /etc/hosts.equiv and $HOME/.rhosts, and how to protect the root account, or what to do about tcp_wrapper, sendmail, and anonymous ftp [9]. These checklists have depth, certainly, but they do not have breadth and are not maintained. Another example of similar material is Curry’s paper [41].

4.4 Principles

These models are sets of principles which characterize good information systems. NIST’s GAPP [51] (see also Section 3.2.1), is an example of this type of model.[28] We present additional examples here:

- one set from OECD,
- a second from NIST,
- a third set by IFAC,
- a fourth by Wood,
- two more from the GAO,
- one by Gaston, and
- a final one by Meadows.

4.4.1 OECD

The Organization for Economic Cooperation and Development (OECD) developed a set of information security principles in its “Guidelines for the Security of Information Systems”[87]. Both GASSP [53] (see also Section 3.2.2) and GAPP [51] (see also Section 3.2.1) are based on this set of principles. They are listed below, with explanatory notes included:

Accountability

--assign it

Awareness

Ethics

Multidisciplinary

--represent everyone’s interests

Proportionality

--balance cost of controls against cost of risks

Integration

[28] GAPP is included in Section 3 as a representative of the principles community (see Figure 3).

--make security pervasive
Timeliness
Reassessment
--do it periodically
Democracy
--respect human rights and dignity

4.4.2 NIST’s Engineering Principles for IT Security

NIST’s “Engineering Principles for Information Technology Security” (EP-ITS) consists of 33 principles and is intended “to aid in designing a secure information system.” ([44], page 5) The principles focus on technical controls, but recognize that “a system security design should also consider non-technical issues, such as policy, operational procedures, and user education.” ([44], page 5) Although EP-ITS is “derived primarily” from NIST’s GAPP document [51], EP-ITS provides principles from a “system-level” as opposed to an “organization-level.” Accompanying each principle is a paragraph describing the meaning and importance of the principles, as well as an indication on where the principle applies in a five-part life-cycle (not shown below). These are the principles:

Principle 1 Establish a sound security policy as the “foundation” for design.
Principle 2 Treat security as an integral part of the overall system design.
Principle 3 Clearly delineate the physical and logical security boundaries governed by associated security policies.
Principle 4 Reduce risk to an acceptable level.
Principle 5 Assume that external systems are insecure.
Principle 6 Identify potential trade-offs between reducing risk and increased costs and decrease in other aspects of operational effectiveness.
Principle 7 Implement layered security (Ensure no single point of vulnerability).
Principle 8 Implement tailored system security measures to meet organizational security.
Principle 9 Strive for simplicity.
Principle 10 Design and operate an IT system to limit vulnerability and to be resilient in response.
Principle 11 Minimize the system elements to be trusted.
Principle 12 Implement security through a combination of measures distributed physically and logically.
Principle 13 Provide assurance that the system is, and continues to be resilient in the face of expected threats.
Principle 14 Limit or contain vulnerabilities.
Principle 15 Formulate security measures to address multiple overlapping information domains.
Principle 16 Isolate public access systems from mission critical resources (e.g., data, processes, etc.).
Principle 17 Use boundary mechanisms to separate computing systems

and network infrastructures.

Principle 18 Where possible, base security on open standards for portability and interoperability.

Principle 19 Use common language in developing security requirements.

Principle 20 Design and implement audit mechanisms to detect unauthorized use and to support incident investigations.

Principle 21 Design security to allow for regular adoption of new technology, including a secure and logical technology upgrade process.

Principle 22 Authenticate users and processes to ensure appropriate access control decisions both within and across domains.

Principle 23 Use unique identities to ensure accountability.

Principle 24 Implement least privilege.

Principle 25 Do not implement unnecessary security mechanisms.

Principle 26 Protect information while being processed, in transit, and in storage.

Principle 27 Strive for operational ease of use.

Principle 28 Develop and exercise contingency or disaster recovery procedures to ensure appropriate availability.

Principle 29 Consider customer products to achieve adequate security.

Principle 30 Ensure proper security in the shutdown or disposal of a system.

Principle 31 Protect against all likely classes of “attacks.”

Principle 32 Identify and prevent common errors and vulnerabilities.

Principle 33 Ensure that developers are trained in how to develop secure software.

4.4.3 IFAC

The International Federation of Accountants (IFAC) list principles of information security in “Managing Security of Information” [63]:

Accountability – Responsibility and accountability must be explicit.

Awareness – Awareness of risks and security initiatives must be disseminated.

Multidisciplinary – Security must be addressed taking into consideration both technological and non-technological issues.

Cost-effectiveness – Security must be cost-effective.

Integration – Security must be coordinated and integrated.

Reassessment – Security must be reassessed periodically.

Timeliness – Security procedures must provide for monitoring and timely response.

Societal Factors – Ethics must be promoted by respecting the rights and interests of others.

4.4.4 Wood's "Principles of Secure Information Systems Design"

Wood's "Principles of Secure Information Systems Design" [116] is enumerated here, with occasional explanatory notes included):[29]

Cost effectiveness

Simplicity

Override

--do not allow it under normal circumstances;

Overt design and operation

--if the design is covert, then the people involved have less chance of understanding it and thus of implementing / maintaining it properly;

Least privilege

Entrapment

Independence of control and subject

--don't let the developer use the system;

Universal application

--make the control measures widely applicable;

Acceptance of control subjects

--if the users do not understand the reason for the control, they will resist;

Sustainability

Auditability

--how else can you know if your controls are effective?

Accountability

Defensive depth

--the more controls that are involved, the better;

Isolation and compartmentalization

Least common mechanism

--this is the other end of the spectrum from single-point of failure; e.g., use a ring topology instead of a star;

Control the periphery

Completeness and consistency

Default to denial

Parameterization

--enables a "moving target;"

Hostile environment

--assume it;

Human involvement

--do not assume that any computer can function entirely by itself;

Secure image

--do not look vulnerable;

Low profile

[29] Reprinted from COMPUTERS AND SECURITY, Vol 9, Charles Cresson Wood, "Principles of Secure Information Systems Design," Pages 13-24, Copyright (1990), with permission from Elsevier Science.

--e.g., put computers in windowless rooms.

Each principle is described in a paragraph or two. No further details are provided. The minimal level of detail would make maintaining these principles quite easy, though we do not know of any organization that does so.

4.4.5 GAO's Learning from Leading Organizations

The U. S. General Accounting Office (GAO) published "Executive Guide: Information Security Management: Learning from Leading Organizations" [48] in May 1998, which we abbreviate as "LfLO" in Figure 1. The publication is marked "Exposure Draft" so some caution is advised. However, what GAO did sets the document apart from the others presented in this report, and what they found is interesting. The GAO used a more empirical approach, as opposed to the seemingly theoretical approach used by all of the other models we present. That is, the GAO looked at what organizations actually do to provide information assurance, and then, from that, the GAO distilled principles and practices. This approach is based on first determining organizations that are "recognized as having strong information security programs"—here is where the theory lurks. The study produced a two-tiered taxonomy consisting of five "risk management principles" and 16 "practices," a photocopy of which is shown in Appendix B.1. The study can be thought of as a check on GASSP, a summary of which the GAO study includes in an appendix.

Exhibits

Appendix B.1 presents photocopies of material from LfLO.

4.4.6 GAO's "Practices of Leading Organizations"

A companion to the GAO study above is a second GAO's study [49], this one on information security risk assessment, but again from "leading organizations," which we abbreviate as "PoLO" in Figure 1. This latter study identifies seven "critical success factors," along with the outline of the process, the tools, and the benefits, all shown in one Figure, a photocopy of which is shown in Appendix B.2. The simplicity of the results invites comparison with other risk assessment approaches, such as OCTAVE (see Section 4.6.2).

Exhibits

Appendix B.2 presents photocopies of material from PoLO.

4.4.7 Gaston

S. J. Gaston, in his book on information security [54], presents nine principles of information security:[30]

[30] Reproduced with the permission of the Canadian Institute of Chartered Accountants.

Senior management should view information security from an overall perspective, recognizing its contribution in achieving the organization’s broader goals.

Information security should be viewed as a part of the overall system of internal control.

The access rights and privileges of customers and other third parties should be adequately controlled.

The differences between data and information[31] should be recognized and provided for in the information security policy.

“Believed systems”[32] must be recognized and carefully provided for from an information security perspective.

As the organization’s dependency on information security evolves and grows, the information security policies and standards must be periodically revisited and strengthened where necessary.

Information security should be viewed from a customer’s perspective to ensure the organization provides the security and ease of use the customer expects when dealing with the organization electronically.

Senior management should obtain an executive level understanding of basic security principles to ensure security issues are addressed in a consistent and logical manner and in keeping with broader corporate issues and goals.

Senior management should have a basic understanding of the Internet and its security challenges and opportunities.

4.4.8 Meadows’ Taxonomy

Meadows’ paper, “An Outline of a Taxonomy of Computer Security Research and Development” [80], is a taxonomy of “computer science research and development” as of 1992. Meadows defines computer security as “any means for ensuring that a computer-based system performs a function in the face of an intruder or intruders who are actively trying to prevent it from doing so.” With a little latitude this is a definition of information assurance. It turns out that the taxonomy is a superset of the CIA model. Unfortunately, the taxonomy that Meadows presents she describes as an “outline” only.

The taxonomy is reproduced below, with our explanatory comments, usually in Meadows’ own words, preceded by two dashes:[33]

1. Systems
    1.1 Components

[31] Gaston defines “data” as the “individual pieces that enable us to conduct individual business transactions or manage individual economic events,” and “information” to be “aggregated data that is used...to manage the business and make overall business decisions.” ([54], pages 36-7)

[32] “A ‘believed system’ is one where we transact business based solely on information supplied by our computer applications and do no further checking before entering into a transaction or exchanging funds.” ([54], page 39)

[33] The material below is from Catherine Meadows, “An Outline of a Taxonomy of Computer Security Research and Development.” Proceedings of the 1992-1993 ACM Workshop on New Security Paradigms, pp. 33-35.

--the entire system is “all in one piece;”

1.2 Composed Systems

1.2.1 Hierarchical Composition

--each component relies on another to enforce security;

1.2.2 Flat Composition

--each component enforces its own security policy;

--Meadows does not include it but there is a third option, namely a heterogeneous composition which is a mixture of hierarchical and flat;

2. Policies

--this is a “crude” (and historical) division; note that this is the CIA model;

2.1 Exclusivity

--protect from unauthorized use; secrecy is a subclass, and confidentiality is a subclass of that;

2.2 Integrity

--protection from unauthorized modification;

2.3 Assured Service

--protection from denial of service;

3. Techniques

--techniques to enforce security policy, e.g., encryption;

3.1 Within Systems

--techniques for enforcing security within a system;

3.1.1 Access Control

--e.g., reference monitors, covert channel analysis;

3.1.2 Inference Prevention

3.2 Without System

--techniques for enforcing security against intrusion from outside;

3.2.1 Intrusion Detection

3.2.2 Authentication

--e.g., passwords, biometric authentication, cryptographic authentication;

3.3 Between Systems

--techniques for enforcing security between systems, such as key distribution, intersystem authentication protocols, secure communication devices;

3.3.1 Secure Communication Between Systems

4. Assurance

--assurance that the system enforces the policy;

4.1 Formal and Semi-Formal Methods

--note: a “semi-formal” method requires a human to do part of the proof;

4.2 Testing

--e.g., Tiger Teams;

4.3 Evaluation

--a “meta”-assurance technique: what do we have to do to the system before we believe it is secure?

5. Interactions with other System Requirement

--i.e., trade-offs with other system parameters, usually at odds with security;

5.1 Interactions with Performance

--e.g., how do you provide security if the system’s performance requirements conflict with the constraints imposed by security?

5.2 Interactions with Consistency

5.3 Interactions with Dependability

5.4 Interactions with Human Factors

--prevent security from making the system "user-hostile;"

4.5 SAC

"Systems Auditability and Control" (SAC) [100] has been developed and is maintained by the Institute of Internal Auditors Research Foundation. The latest version was published in 1994. SAC is immense: 1,663 pages spread over 14 "modules" (i.e., volumes). SAC is a body of knowledge designed to help internal auditors (i.e., auditors who are employees of the organization that they audit) improve controls. SAC does this by explaining the technology and related "audit concerns," but not specifying auditing details. It appears that each edition of SAC determines "Major Research Finding," which it then uses to provide information needed by management and internal auditors. These are the findings from the most recent edition:[34]

- Compatibility of information systems with organizational objectives is management's primary concern.
- Data security and contingency planning are top management control concerns.
- Internal auditors report improved systems controls.
- Internal auditors identify key systems areas for improved controls.
- Internal auditors plan to increase coverage of information technology components.
- Management places greater emphasis on internal controls.
- Internal auditors provide greater support to executive and information systems management.
- Changing technology provides new control and audit technologies. ([100], pages 1-3 through 1-5)

SAC educates the auditor not only on how to develop an audit but also on how to configure controls. However, the closest the material itself in SAC comes to an auditing level is in the Case Study, "Auditing Telecommunications," in Volume 8 "Telecommunications." This 19-page study provides a set of questions constituting an "Interview Guide," and a second set of questions constituting a "Field Questionnaire."

One of SAC's achievements is its sensible definition of risk, which includes fraud, business interruption, errors, customer dissatisfaction, poor public image, and ineffective and inefficient use of resources ([100], page 2-19). Controls and risk are inextricably connected, since the purpose of the former is to mitigate the latter.

COSO (see Section 3.1.4) states that one of "principle objectives" of SAC is "providing guidance on information systems and related control activities." ([37], page 31, footnote). One of SAC's

[34] From Systems Auditability and Control by Price Waterhouse, Copyright 1994 by The IIA Research Foundation, 249 Maitland Avenue, Altamonte Springs, Florida 32710-4201 U.S.A. Reprinted with Permission.

conclusions, again according to COSO, is that "the most important management challenge in the 1990s is to integrate the planning, design and implementation of systems with the organization's overall strategy." ([37], page 61).

SAC is in the process of being updated. The new title is "Electronic Systems Assurance and Control" and is abbreviated "eSAC." The Executive Summary (7 pages) and the eSAC Model (9 pages) are both available for download at www.theiia.org (click on Technology). (Appendix A of the eSAC Model document relates control objective frameworks, namely COSO, SysTrust, and CobiT, to eSAC.)

4.5.1 Exhibits

Appendix B.4 presents photocopies of material from SAC.

4.6 Risk Assessment Methods

We review two risk assessment methods here, Control Self-Assessment (CSA) and OCTAVE.

4.6.1 Control Self-Assessment (CSA)

The traditional approach to the assessment of risk is for auditors to perform an audit. While auditors know about audits, they are limited if they do not know the culture and particulars of each area for which they are asked to perform an audit. The Control Self-Assessment (CSA) method, also known, especially in Canada, as Control / Risk Self-Assessment (CRSA)[35], uses employees who are working in an area to assess risks and controls in that area [59]. CSA is intended to "augment" the audit function by using auditors, usually, to facilitate the assessment of risk, usually in the form of a workshop, by those "in the trenches," the people who are the experts in that area. This is where the "self" in CSA comes in. The auditor is responsible for the process, which includes arranging for the workshop, determining the focus of the workshop, guiding the participants through the process, providing training on fundamental concepts such as "objectives," "risk," and "controls," and providing verification of the workshop results. The auditor also shepherds the report to completion so that management and staff can use it as a guide. However, it is the workshop participants that do the real work: they are the ones that identify risks and the ones who evaluate and propose changes to the controls. As The IIA describes it, "CSA is conducted within a *structured environment* in which the process is thoroughly *documented* and the process is *repetitive* and as an incentive for continuous improvement." [95] (emphasis in the original)

CSA was initiated at Gulf Canada in 1987 [95]. It has subsequently been endorsed by The IIA. The IIA supports COSO's recommendations (and CoCo), so the definition and categories of internal control promulgated by CSA are those developed by COSO. "About half" of those who use CSA also use a control framework, such as COSO [59]. The approach is not proprietary: there is no one "best practice" since it is tailored by organizations for their needs. It is not clear

[35] It is know in other areas of the world by at least 10 other names, the acronyms for which are DSA, FSA, MAP, MSA, CAMP, CMP, PARC, BSA, BRA, DARE.

how widespread is the use of CSA. The IIA, in 1998, referred to it as “relatively new and growing.” [95]

There are three primary ways of performing a CSA:

- “facilitated town meetings” (also known as workshops),
- questionnaires, and
- “management-produced analysis” [95].

The workshop format is the most popular. It consists of a half-day meeting with about a dozen people, conducted by an auditor. The “management-produced analysis” is a catch-all category, including any method that is not one of the other two.

There are four different workshop formats:

- objective-based,
- risk-based,
- control-based, and
- process-based.

Each format approaches the three concepts of objectives, risks, and controls from a different angle, but the goal of developing a plan that will improve the effectiveness of controls is the same. An objective-based workshop, for example, focuses on an objective: do the controls in place give reasonable assurance that the objective will be reached? A process-based workshop considers a series of activities “from end-to-end, such as the purchasing process...” [59].

There is enormous sense in CSA. It is essentially a teaching tool in which participants learn to think in terms of objectives, risks, and controls. Through this process, which is intended to be repeated with the regularity of audits, the participants can continuously improve in their ability to hone their work to furthering the objectives of the organization. CSA thus supports the general trend to employee empowerment. As The IIA puts it,

> Regardless of who provides the facilitation, The IIA believes CSA improves the control environment of an organization by:
>
> > Increasing awareness of organizational objectives and the role of internal control in achieving goals and objectives.
> >
> > Motivating personnel to carefully design and implement control processes and continually improve operating control processes.” [95]

The only missing element of CSA is the consultant. For example, a participant could presume that there is no risk in putting a dial-in modem on their computer at work. However, a consultant on this matter could, in a workshop, provide insight into the risks involved and suggestions on controls. It should be noted that the consultant would not be able to provide help with objectives or the choice of controls: these can be decided only by the organization itself.

Hubbard [59] suggests a control framework for use in CSA. Known as CARD*menu*$^{\text{TM}}$, developed by CARDdecisions, Inc. [17], this framework is a three-tiered taxonomy, as summarized in Table 16.

Table 16 CARD*menu* Organization

Tier	Name	Elements
Top	(unnamed)	8
Middle		66
Bottom		10

The taxonomy provides a listing of objectives, such as “1.1 Definition of Corporate Mission & Vision,” and “2.1 Accountability / Responsibility Mechanisms,” that, we presume, every healthy organization would want to review via some approach such as CSA. Even without amplification of the one-line descriptions in the taxonomy, the list could provide excellent guidance on coverage in a CSA.

4.6.2 OCTAVE

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) is a “self-directed information security risk evaluation” ([4], page 5), where risk involves asset, threat, and vulnerability.

An OCTAVE evaluation proceeds in three “Phases” (steps), consisting of a total of eight “Processes,” that can be characterized very roughly as follows:

1. determine what can threaten you,
2. determine where you are weak,
3. determine how to protect the places where you are both threatened and weak.

These are the three “Phases” and the eight “Processes:”[36]

Phase 1: Build Asset-Based Threat Profiles

Process 1: Identify Senior Management Knowledge

Process 2: Identify Operational Area Knowledge

Process 3: Identify Staff Knowledge

Process 4: Create Threat Profiles

Phase 2: Identify Infrastructure Vulnerabilities

Process 5: Identify Key Components

Process 6: Evaluate Selected Components

Phase 3: Develop Security Strategy and Plans

[36] Special permission to reproduce the names of the 3 Phases and 8 Processes of OCTAVE, (c) 2001 by Carnegie Mellon University, is granted by the Software Engineering Institute.

Process 7: Conduct Risk Analysis

Process 8: Develop Protection Strategy

The first three Processes gather assets from senior managers, operational managers, and staff. The OCTAVE Threat Profiles, developed in Process 4, are trees consisting of up to five levels. The root is an asset. The second level consists of the possible access methods. The third level is an actor, e.g., insider or an outsider. The fourth level is the motive, e.g. accidental or deliberate. And the fifth level is the outcome, e.g., disclosure, modification, loss / destruction, and interruption. For each asset, a Threat Profile should be created. If there is a path from the asset to the outcome, then there is a problem. The problem can be precluded if an edge on the path can be broken.

Process 5 correlates the assets identified in Processes 1-3 with the current network. The focus is on the "access" level of the Threat Profiles, in particular network access that can be identified via a topology diagram, as opposed to access problems that poor staff training might create, for example. Process 6 calls for running vulnerability evaluation tools, presumably on the "key components" identified in the previous Process.

The goal of the risk analysis in Process 7 is to determine high / medium / low rankings for the impact of each "outcome" for each identified threat, where outcome is as defined above, namely, disclosure, modification, loss / destruction, and interruption. These are described via "Risk Profiles," which are Threat Profiles with an additional lowest level that identifies impact (high / medium / low). Process 8 consists of two workshops: develop protection strategy, and protection strategy selection.

During Phase 1 and 3, participants are expected to use "catalogs" of information of three types: catalog of practice—shown below—threat profiles, and catalogs of vulnerabilities. Two examples of catalogs of vulnerabilities include the CERT® Knowledgebase [19] and the Common Vulnerabilities and Exploits (CVE) database [38].

The OCTAVE "criteria" are "essential elements, or requirements." ([4], page 2) The criteria consist of

- 10 "principles" (e.g., self-direction, adaptable measures, defined process) in three categories (i.e., information security risk evaluation principles, risk management principles, and organization & cultural principles),
- 15 "attributes" (e.g., RA[37].1 Analysis Team, RA.2 Augment Analysis Team Skills, RA.3 Catalog of Practices), and
- 11 "outputs" (e.g., RO[38]1.1 Critical Assets).

Perhaps most interesting from the standpoint of this report is the Catalog of Practices. These Practices read very much like many of the models we have presented in this report. And they are organized, just as we would expect, into tiers, as shown in Table 17.

[37] "RA" is an abbreviation of Attribute Requirement.

[38] "RO" is an abbreviation of Requirement Output.

Table 17 OCTAVE Catalog of Practice Organization

Tier	Name	Elements
Top	Strategic Practices (SP), and Operational Practices (OP)	2
Second	(unnamed)	9
Third		40
Bottom		45

The structure is a lopsided tree, with only two levels below Strategic Practices, but three levels below Operational Practices, hence the small number of Elements in the bottom Tier.

The “Method Implementation” [86] is a formal approach, with processes consisting of guidelines, workshops, activities, workbooks, complete with estimated completion times—sometimes to the minute—and supplementary slide shows, fully explained in 18 volumes, reminiscent of SSE-CMM’s Appraisal Method (see Section 3.3.1) in its level of detail. SEI is developing “An OCTAVE-consistent Method for Small Organizations,” and other organizations could develop “Other Methods Consistent with the OCTAVE Criteria” ([4], page 2).

The OCTAVE approach as a method of “managing information security risks” is presented in Alberts & Dorofee’s recent book [5]. The book’s main contribution is in providing context and rationale for the use of OCTAVE. For example, Chapter 2 of the book is entitled, “Principles and Attributes of Information Security Risk Evaluations.”

A photocopy of the entire top and second tiers (and part of the third tier) of the Catalog of Practice ([86], Volume 15, page A-3) is shown in Appendix B.3.

Exhibits

Appendix B.3 presents photocopies of material from OCTAVE.

4.7 Common Criteria

The Common Criteria (CC) has a different focus than the other models presented in this report: “The CC is applicable to IT security measures implemented in hardware, firmware, or software.” ([37], Part 1, page 1) That is, the CC is interested in “technology” and part of “process,” but not the “human” factor, to use the Center for Internet Security description of security [18].[39] The CC explicitly does not cover the human part:

> The CC does not contain security evaluation criteria pertaining to administrative security measures not related directly to IT security measures. However, it is recognised that a significant part of the security of a TOE [Target of Evaluation, i.e., an IT product or system under evaluation] can

[39] The CIS defines these three factors as follows: “technology (software and hardware), process (system and network administration) and human (end user and management behavior.)” [18].

> often be achieved through administrative measures such as organisational, personnel, physical, and procedural controls. ([37], Part 1, page 1)

The CC is the third generation of similar approaches. “In the early 1980’s, NSA developed the Trusted Computer System Evaluation Criteria (TCSEC or ‘Orange Book’)” ([113], page 2). TCSEC was built upon in Europe, Canada, and the US, for the second generation:

> In Europe, the European Commission published the “Information Technology Security Evaluation Criteria (ITSEC) in 1991 after joint development by France, Germany, the Netherlands, and the United Kingdom.
>
> In Canada, the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) were published in early 1993 as a combination of the ITSEC and TCSEC approaches.
>
> In the United States, NIST and NSA jointly developed the draft Federal Criteria for Information Technology Security (FC) version 1.0, which as also published in early 1993 as a second approach to combining the North American and European concepts for evaluation criteria. ([37], Part 1, page 1)

The third generation is the result of the five-year “CC Project,” the name of the effort of the seven participating organizations

- Canadian Security Establishment,
- Service Central de la Sécurité des Systèmes d’Information (SCSSI) in France,
- Bundesamt für Sicherheit in der Informationstechnik (BSI) in Germany,
- Netherlands National Communications Security Agency,
- Communications-Electronics Security Group in the UK,
- National Institute of Standards and Technology (NIST) in the US, and
- National Security Agency (NSA) also in the US.

to create a common criteria. Version 1.0 of the CC was finished in 1996, and version 2.0 in 1998. It has been adopted by ISO and is known by that organization as International Standard 15408, “Evaluation Criteria for Information Technology Security.”

The CC is intended to be used to describe requirements and evaluate products. The documentation consists of three parts [37]:

> Part 1: Introduction and General Model
>
> Part 2: Security Functional Requirements
>
> Part 3: Security Assurance Requirements

The set of functional requirements and the set of assurance requirements are the CC primitives. A set of functional and/or assurance requirements is a “package.” A package is an “intermediate combination,” between the low-level requirements and the “Protection Profile” and “Security Target” discussed below. The CC defines seven “packages.” These seven packages are sets of assurance requirements known as Evaluation Assurance Levels (EALs), labelled EAL1 through EAL7:

EAL1 functionally tested
EAL2 structurally tested
EAL3 methodically tested and checked
EAL4 methodically designed, tested and reviewed
EAL5 semiformally designed and tested
EAL6 semiformally verified design and tested
EAL7 formally verified design and tested.

It is intended that security-product consumers will write Protection Profiles (PP) that are basically collections of packages, specifying what consumers want. A PP would include a EAL, which specifies the level of assurance desired. A PP thus defines a market niche.

It is similarly intended that security-product producers will write Security Targets (ST), like PPs, that are basically collections of packages, against which a product, referred to as a "Target of Evaluation" (TOE), is to be evaluated. An ST could be little more than a PP, if a producer has developed a TOE for a previously defined market niche. An "accredited, independent laboratory" would perform an evaluation to answer the question, "Does the given TOE fulfill the given ST?" If the answer is yes, then the evaluation would be submitted to an "evaluation authority" (one of the founding organizations for the CC, listed above) for validation. (NIST and NSA jointly operate the National Information Assurance Partnership (NIAP). The principle purpose of NIAP is to operate as one of these evaluation authorities.)

So consumers can generate PPs to define their market niche, identifying market demand, and producers can generate STs to provide assurance of their products, identifying market supply. Between the two a market based on evaluated, needed products are created.

PPs and STs themselves can be evaluated to ensure that they are "correct, complete, and internally consistent." ([113], page 7)

One of the intents of the CC is that evaluation authorities recognize each other's evaluations. "The anticipated outcome is a 'level playing field' for multi-national IT product manufacturers, leaving to a much wider availability of useful IT security products to secure the global information infrastructure." ([113], page 10)

4.8 Attack Taxonomies

These taxonomies classify attacks on computer systems. Precluding successful attacks is certainly part of information assurance.

Amoroso defines an attack taxonomy as "any generalized categorization of potential attacks that might occur on a given computer system" [6]. These taxonomies help in assessing system security, for example, by directing penetration tests based on the range of attacks provided by the attack taxonomy. For simplicity's sake we include taxonomies on "security-related incidents" and computer "misuse" in this category, an instance of each of which we include below. These taxonomies can be based on thousands[40] of such occurrences. Unfortunately, for our purposes, these taxonomies do not describe how these attacks (or incidents or misuse) are to be defended against or precluded in general, though that may be obvious for particular attacks. Attack taxonomies usually do not include the problems that can occur due to nature, such as hurricanes, or the systemic problems due to inattentive management or poor personnel screening practices.

A representative taxonomy for attack taxonomies is presented below, followed by an instance of a security-related incidents taxonomy, followed in turn by an instance of a "system of descriptors" for misuse.

4.8.1 Perry & Wallich

We present here, in tabular form, the attack taxonomy developed by Perry & Wallich [92]. Attackers are shown in the columns and prominent areas of vulnerabilities in the rows; each table cell shows a type of attack. Table 18 shows the Perry & Wallich table with several likely types of attacks included.

Table 18 Perry & Wallich Attack Taxonomy[a] (Some likely attacks included)

	Operators	Programmers	Data Entry	Internal	Outside	Intruders
Physical Destruction	Bombing; Short circuits					
Information Destruction	Erasing disks	Malicious software	False data entry		Malicious software	Via modem[b]
Data Diddling		Malicious software				
Theft of Services		Theft as user		Unauthorized action	Via modem	
Browsing	Theft of media			Unauthorized action	Via modem	
Theft of Information				Unauthorized action	Via modem	

[a] The material in this table is from T. Perry & P. Wallich, "Can Computer Crime Be Stopped?" IEEE Spectrum, Vol. 21, No. 5, 1984. © 1984 IEEE. Reprinted with permission.

[b] An updated taxonomy would include direct Internet connection here.

[40] For example, about 3,000 cases were analyzed in Neumann & Parker's study [84], and 4,299 incidents were analyzed in Howard's [57].

4.8.2 Howard & Longstaff

Howard & Longstaff present a taxonomy for “security-related incidents.” They define an incident to be a superset of an “attack,” which in turn they define to be a superset of an “event” ([58], see also [57]). The taxonomy has seven parameters—attackers, tools, vulnerabilities, actions, targets, unauthorized results, and objectives—with between three to eleven values for each parameter, organized as follows:

1. an event consists of an “action” and a “target;”
2. an attack consists of a “tool,” a “vulnerability,” an event (previously defined), and an “unauthorized result;” and
3. an incident consists of an “attacker,” an attack (previously defined), and an “objective.”[41]

Here is the table:

Table 19 Computer and Incident Taxonomy (Sheet 1 of 3)

Attackers	Hackers
	Spies
	Terrorists
	Corporate Raiders
	Professional Criminals
	Vandals
	Voyeurs

[41] Not to be confused with “control objective” as used in Section 2.

Table 19 Computer and Incident Taxonomy (Sheet 2 of 3)

Attack(s)	Tool		Physical Attack
			Information Exchange
			User Command
			Script or Program
			Autonomous Agent
			Toolkit
			Distributed Tool
			Data Tap
	Vulnerability		Design
			Implementation
			Configuration
	Event	Action	Probe
			Scan
			Flood
			Authenticate
			Bypass
			Spoof
			Read
			Copy
			Steal
			Modify
			Delete
		Target	Account
			Process
			Data
			Component
			Computer
			Network
			Internetwork
	Unauthorized Result		Increased Access
			Disclosure of Information
			Corruption of Information
			Denial of Service
			Theft of Resources

Table 19 Computer and Incident Taxonomy (Sheet 3 of 3)

Objectives	Challenge, Status, Thrill
	Political Gain
	Financial Gain
	Damage

4.8.3 Neumann & Parker

Neumann & Parker [84] analyze “about 3,000” cases of what they refer to as “misuse,” arriving at the following nine classes, arranged in order of decreasing “distance” to the computing machinery itself:[42]

1. External misuse
   (e.g., dumpster diving)
2. Hardware misuse
   (e.g., eavesdropping)
3. Masquerading
   (e.g., spoofing)
4. Setting up subsequent misuse
   (e.g., “pest” programs such as Trojan Horses)
5. Bypassing intended controls
   (e.g., password attacks)
6. Active misuse of resources
   (e.g., denial of service, salami attacks)
7. Passive misuse of resources
   (e.g., covert channels)
8. Misuse resulting from inaction
   (e.g., selling un-degaussed media)
9. Use as an aid to other misuses
   (e.g., factoring very large integers).

These nine classes can be ranked based on prevalence of instances, starting with the most prevalent, and partitioned into three clusters:

first cluster:

6. Active misuse of resources
7. Passive misuse of resources

second cluster

3. Masquerading
5. Bypassing intended controls
4. Setting up subsequent misuse
2. Hardware misuse

[42] The material below is from P. G. Neumann, D. B. Parker, “A summary of computer misuse techniques.” Proceedings of the 12th National Computer Security Conference, pp. 396-407. Baltimore, Maryland, October 1989. © 1989 IEEE. Reprinted with permission from IEEE.

```
1. External misuse
```

third cluster:

```
8. Misuse resulting from inaction
9. Use as an aid to other misuses
```

The two categories in the first cluster are insider attacks and are “by far the most prevalent” [84].

Neumann & Parker describe their work as a “system of descriptors rather than a taxonomy.”

4.8.4 Other Instances

Lindqvist & Johnsson [79] present a taxonomy of intrusion techniques and a separate taxonomy of intrusion results based on Neumann and Parker’s nine classes. Their “techniques taxonomy” uses three top-tier categories

```
bypassing intended controls,
active misuse of resources,
passive misuse of resources.
```

and their “results taxonomy” uses the CIA model (Section 4.1) for the top-tier categories:

```
exposure,
erroneous output,
denial of service.
```

Benjamin, et al. [10], present a two-tiered attack taxonomy, with two items on the top tier (attacks motivated by acquiring information, and attacks motivated by disrupting communication) and nine items on the second tier. The items listed in the disrupting attack category are only the “principal forms” of this type of attack. In other words, the taxonomy is not intended to be comprehensive.

Howard & Longstaff [58] review six categories of possible taxonomies: lists of terms, lists of categories, results categories, empirical lists, matrices, and action-based taxonomies. Some of the items in these categories are inadequate as taxonomies, as Howard & Longstaff point out.

Other people focus on threats. For example, Bernstein et al. present nine classes of Internet threats [11]:[43]

```
eavesdropping,
masquerade,
replay,
data manipulation,
misrouting,
trapdoor/trojan horse,
viruses,
repudiation, and
```

[43] Reprinted with permission from John Wiley & Sons.

```
    denial of service.
```

Still others focus on “problems.” For example, Schneider et al. partition “network failures” into the following four categories (and sub-categories) [101]:[44]

```
    environmental disruption,
        link failures,
        congestion,
    operational errors,
    software and hardware failures, and
    malicious attacks,
        attacks on the telephone network,
            routing attacks,
            database attacks,
        attacks on the internet,
            name server attacks,
            routing system attacks,
            protocol design and implementation flaw.
```

Mitre provides a four-tiered taxonomy of attacks, the organization of which is shown in Table 20 [81].

Table 20 Mitre Organization

Tier	Name	Elements
Top	Control Activities	6
Second		~35
Third		~140
Bottom		~280

4.9 Miscellaneous Models

The following are models that we know in name only, many of which come from CobiT’s “Primary Reference Material” ([29], Appendix III, pp. 85-6):

- Turnbull,
- King [74],
- SAS 55,
- SAS 78,
- Cadbury [15],
- KonTraG,
- UNEDO and UN Guidelines,

[44] Reprinted with permission from Trust in Cyberspace. Copyright 1999 by the National Academy of Sciences. Courtesy of the National Academies Press, Washington, D.C.

- ITIL IT Management Practices,
- IBAG Framework,
- PCIE Model Framework,
- IFAC International Information Technology Guidelines—Managing Security of Information,
- Denmark Generally Accepted IT Management Practices,
- C & L Audit Guide SAP R/3,
- ISO IEC JTC1/SC27 Information Technology,
- Recommended Practice for EDI,
- TickIT,
- ESP Baseline Control—Microcomputers,
- Standards for Internal Control in the Federal Government (GAO/AIMD-00-21.3.1),
- ISO/ICT TR 1335-n Guidelines for the Management of IT Security (GMITS)
- Vienot (reference in [98], page 3).

5 Conclusions

> So, it is vital to create a top-level strategy for mitigating your organizations's exposure to security threats. Many factors are critical in this, but none is as important as a clear overall picture of important objectives. [82]

This report presented information control models. Each model can be thought of as a definition of information assurance, as a taxonomy, and as an answer to the following questions:

> What do I need to do to make my system sufficiently reliable and secure, based on my organizations assessment of the costs of security measures versus the value of operating reliable systems for my customers?
>
> How much is enough? What method can I use to determine the minimum level of due care based on best practice benchmarks needed to reduce my enterprise risk to an acceptable level?
>
> Whom can I trust to tell me what I need to do and to help me protect my systems and networks? [18] (bold in the original)

This report focused on a subset of information control models known as control frameworks. Those models (and ones from the two other "communities" of models (see Figure 3)) include BS 7799, CobiT, CoCo, COSO, FISCAM, GAPP, GASSP, ITCG, SSAG, SSE-CMM, and SysTrust. To provide contrast, other types of information control models were also presented in this report.

The purpose of this report is to help readers increase their information security via the rigor of an information control model, in particular a control framework.

Acknowledgments

Thanks to Lisa Wishard of the Sandia Technical Library for her help in reference material collection, to Yolanda Aragon for data entry, and to Jennifer DePoy, Rolf Carlson, John Espinoza, Dave Harris, Lisa Kennicott, Laney Kidd, John Dillinger, Bill Young, John Covan, and Christine Morgan, all from Sandia National Laboratories, for their review.

Abbreviations and Colloquial Names

Note: Abbreviations in the list below that are annotated with an asterisk (*) are abbreviations created for (and likely unique to) this report.

AICPA	American Institute of Certified Public Accountants [3]
CICA	The Canadian Institute of Chartered Accountants [21]
CISA	Certified Information Systems Auditor [22]
CobiT	Control Objectives for Information and Related Technology [32]
CoCo	Criteria of Control Board [31]
CONCT	Control Objectives for Net Centric Technology [39]
COSO	Committee of Sponsoring Organizations of the Treadway Commission [40]
EP-ITS	Engineering Principles for Information Technology Security [44]
GAPP	generally accepted principles and practices [51]
GASSP	Generally Accepted System Security Principles [53]
IFAC	International Federation of Accountants [63]
ISACA	Information Systems Audit and Control Association [65]
ISACF	Information Systems Audit and Control Foundation [66]
ITCG*	Information Technology Control Guidelines [71]
ITGI*	Information Technology Governance Institute [73]
LfLO*	Learning from Leading Organizations [48]
NIST	National Institute of Standards and Technology [85]
PoLO*	Practices of Leading Organizations [49]
SAC	Systems Auditability and Control [100]
SSAG*	Security Self-Assessment Guide for Information Technology [107]
SSE-CMM	Security Systems Engineering Capability Maturity Model [108]
SysTrust	AICPA / CICA SysTrust Principles and Criteria for System Reliability [111]
The IIA	Institute of Internal Auditors [64]

References

[1] Julia Allen, The CERT ® Guide to System and Network Security Practices. Addison-Wesley. Boston, MA. 2001. ISBN 0-201-73723-X.

[2] Amelia Financial Systems Limited, “Operational Risk: The Last of the Risk Frontiers? An Operational & Technical Framework.” 46 pages. http://www.amelia.co.uk.

[3] AICPA: American Institute of Certified Public Accountants. http://www.aicpa.org/index.htm.

[4] Christopher J. Alberts, Audrey J. Durofee, “OCTAVE^{SM} Criteria,” Version 2.0. CMU/SEI-2001-TR-016. ESC-TR-2001-016. December 2001. 128 pages.

[5] Christopher Alberts, Audrey Dorofee, “Managing Information Security Risks: The OCTAVE^{SM} Approach.” Addison-Wesley. Boston, MA. June 2002. 471 pages.

[6] Edward Amoroso, Fundamentals of Computer Security. Prentice Hall PTR. Upper Saddle River, NJ. 1994. ISBN 0-13-108929-3.

[7] AS/NZS 4360:1999 “Risk Management.” ISBN: 0-7337-2647-X. http://www.standards.com.au/.

[8] AS/NZS 4444:1999 Information Security Management - Code of Practice for Information Security Management. The standard is published in two parts, similar to BS 7799 [12]. Australian and New Zealand Standard Committee. http://www.standards.com.au/.

[9] Australian Computer Emergency Response Team, “UNIX Computer Security Checklist” Version 1.1. Last Update 19-Dec-1995.

[10] R. Benjamin, B. Gladman, B. Randell, “Protecting IT Systems from Cyber Crime.” The Computer Journal, vol. 41, no. 7, 1998, pp. 429-443.

[11] Terry Bernstein, Anish B. Bhimani, Eugene Schultz, Carol A. Siegel, Internet Security For Business. John Wiley & Sons, Inc. New York, NY. 1996. ISBN 0-471-13752-9.

[12] BS 7799: BS 7799-1:1999 “Information security management—Part 1: Code of practice for information security management. 45 pages. BS 7799-2:1999 “Specification for information security management systems.” 11 pages. British Standards Institute. http://www.bsi.org.uk/. (First published in February 1995.)

[13] BS 7799 c:cure Web site http://www.c-cure.org.

[14] David Brewer, “Les criteres d’homologation de la securite des systemes d’information.” White Paper presented at the Eurosec ‘98 Conference, March 16, 1998, Paris, France. (Available on-line in English at http://www.gammassl.co.uk/topics/hot9.html.)

[15] Cadbury Commission, “Report of the Committee on the Financial Aspects of Corporate Governance.” December 1992. 89 page. Available at http://www.worldbank.org/html/fpd/privatesector/cg/codes.htm.

> This report is intended for Boards of Directors. The report how the board should operate, including a section on internal controls, and how audits should be done. The “heart” of the report is its two page “Code of Best Practice,” which has four sections: Board of Directors, Non-Executive Directors, Execu-

tive Directors, and Reporting & Controls. The code defines corporate governance at the highest level. The fundamentals of the report have been incorporated in subsequent models.

[16] Capability Maturity Models at the Software Engineering Institute of Carnegie Mellon University: http://www.sei.cmu.edu/cmm/cmms/cmms.html.

[17] CARDdecisions, Inc. (Collaborative Assurance & Risk Design^{TM}). http://www.carddecisions.com/.

[18] The Center for Internet Security. http://www.cisecurity.org/.

[19] CERT® Knowledgebase. http://www.cert.org.kb/.

[20] CIAO: “Practices for Securing Critical Information Assets.” Critical Infrastructure Assurance Office. 1800 G Street, N.W., Suite 8-130, Washington D.C. 2006. January 2000. 92 pages.

[21] CICA: The Canadian Institute of Chartered Accountants. http://www.cica.ca/cica/cicawebsite.nsf/public/homepage.

[22] CISA: Certified Information Systems Auditor. http://www.isaca.org/cert1.htm. See also [65].

[23] CISSP: Certified Information System Security Professional. Offered by the International Information Systems Security Certification Consortium, Inc (ISC^2). http://www.isc2.org.

[24] CMU: Carnegie Mellon University. http://www.cmu.edu/.

[25] “CobiT Audit Guidelines.” 3rd Edition. July 2000. 226 pages. CobiT Steering Committee and the IT Governance Institute.

[26] “CobiT Control Objectives.” 3rd Edition. July 2000. 148 pages. CobiT Steering Committee and the IT Governance Institute.

[27] “CobiT Executive Summary.” 3rd Edition. July 2000. 16 pages. CobiT Steering Committee and the IT Governance Institute.

[28] “CobiT Framework.” 3rd Edition. July 2000. 68 pages. CobiT Steering Committee and the IT Governance Institute.

[29] “CobiT Implementation Tool Set.” 3rd Edition. July 2000. 85 pages. CobiT Steering Committee and the IT Governance Institute.

[30] “CobiT Management Guidelines.” 3rd Edition. July 2000. 122 pages. CobiT Steering Committee and the IT Governance Institute.

[31] CobiT 2nd Edition: Control. 2nd edition. Objectives for Information and Related Technology (CobiT).” April 1998. Published by ISACF [66]. (Currently out of print).

[32] CobiT 3nd Edition: “Control Objectives for Information and Related Technology (CobiT).” 3rd Edition. July 2000. Published by ISACF [66]. ISBN 1-893209-13-X.

CobiT consists of the following six documents, listed here in the order that I suggest the reader consider them:

Executive Summary [27],

Framework [28],
Control Objectives [26],
Implementation Tool Set [29],
Management Guidelines [30], and
Audit Guidelines [25].

All of the above documents, with the exception of the Audit Guidelines, can be downloaded at no charge from the ISACA site [65].

[33] CoCo: "Guidance on Control." Criteria of Control Board. 1995. The Canadian Institute of Chartered Accountants (CICA) [21]. 32 pages. ISBN 0-88800-436-1.

[34] CoCo: "Preface to the Guidance issued by the Criteria of Control Board." 1995. 3 pages. Criteria of Control Board. 1995. The Canadian Institute of Chartered Accountants (CICA) [21]. ISBN 0-88800-441-9.

[35] Frederick B. Cohen, "Viruses, corruption, denial, disruption, and information assurance." Information Security —the Next Decade, May 1995. Chapter 37, pp. 495-509.

[36] 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.

[37] Common Criteria: "Common Criteria for Information Technology Security Evaluation." August 1999.
Version 2.1. Common Criteria Implementation Board (CCIB) at NIST.
Part 1: Introduction and General Model. CCIMB-99-031. 56 pages.
Part 2: Security Functional Requirements. CCIMB-99-032. 354 pages.
Part 3: Security assurance requirements. CCIMB-99-033. 208 pages.
http://csrc.nist.gov/cc/ccv20/ccv2list.htm.

[38] Common Vulnerabilities and Exploits (CVE) database. http://www.cve.mitre.org.

[39] CONCT: Control Objectives for Net Centric Technology. 1999. http://www.isaca.org/netcentric.htm.

CONCT consists of the following four documents:
Volume One: Framework (76 pages),
Volume Two: Intranet/Extranet/Internet (146 pages),
Volume Three: Data Warehouse (130 pages),
Volume Four: Online Transaction Processing (128 pages).

[40] COSO: Committee of Sponsoring Organizations of the Treadway Commission. "Internal Control—Integrated Framework." Volume 1: "Executive Summary, Framework, Reporting to External Parties. Addendum to 'Reporting to External Parties.'" Volume 2: "Evaluation Tools." American Institute of Certified Accountants, New Jersey, 1994. http://www.cpa2biz.com/CS2000/Home/default.htm.

[41] David A. Curry, "Improving the Security of your Unix System." SRI International. April 1990.

[42] W. Edwards Deming, Out of the Crisis, Massachusetts Institute of Technology, Center for Advanced Engineering Study, Cambridge MA, 1986.

[43] DTI: Department of Trade and Industry and British Standard Institute. "A Code of Practice for Information Security Management," London, 1993, 1995.

[44] EP-ITS: "Engineering Principles for Information Technology Security (A Baseline for Achieving Security)." Gary Stoneburner, Clark Hayden, Alexis Feringa. NIST Special Publication 800-27. June 2001. 21 pages.

[45] "Federal Information Technology Security Assessment Framework." NIST. November 20010. 10 pages. (Appears as Appendix C of SSAG [107].)

[46] FISCAM: "Federal Information Systems Control Audit Manual. Volume I: Financial Statement Audits." Accounting and Information Management Division, U.S. General Accounting Office. January 1999. GAO/AIMD-12.19.6. 284 pages. http://www.gao.gov/special.pubs/ai12.19.6.pdf.

[47] GAO Black Book: "Evaluating Internal Controls in Computer-Based Systems: Audit Guide (Black Book)," United States General Accounting Office. June 1988.

[48] GAO, "Executive Guide: Information Security Management: Learning from Leading Organizations." United States General Accounting Office. Exposure Draft. May 1998. GAO/AIMD-98-68. 68 pages.

[49] GAO, "Information Security Risk Assessment: Practices of Leading Organizations." Exposure Draft. United States General Accounting Office. August 1999. GAO/AIMD-99-139. 50 pages.

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

[51] GAPP: Marianne Swanson, Barbara Guttman, "Guide for Developing Security Plans for Information Technology Systems." NIST Special Publication 800-18, December 1998.

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

[53] GASSP: "GASSP (Generally Accepted System Security Principles)." International Information Security Foundation (I^2SF), June 1999. 74 pages. http://web.mit.edu/security/www/gassp1.html.

[54] S. J. Gaston, Information Security — Strategies for Successful Management. The Canadian Institute of Chartered Accountants. Toronto, Ontario, Canada. 1996. ISBN 0-88800-459-1.

[55] Gary Hardy, "Standards—The Need for a Common Framework." COMPSEC International 95, 12th World Conference on Computer Security, Audit and Control, 25-27 October 1995, London, UK. pp. 540-547.

[56] Tom Hayden, Peter Schablik, "Information Technology Risk Assessment." Session 32, Annual Conference & Expo on Control and Audit of Information Technology. October 15-17, 2001. Boston, MA.

[57] John D. Howard, "An Analysis of Security Incidents on the Internet, 1989-1995." Ph.D. Dissertation. Carnegie Mellon University, April 1997. 292 pages.

[58] John D. Howard, Thomas A. Longstaff, "A Common Language for Computer Security Incidents." SAND98-8667, October 1998. 25 pages.

[59] Larry Hubbard, Control Self-Assessment: A Practical Guide. The Institute of Internal Auditors. 2001. 105 pages. ISBN 0-89413-441-8.

The Appendix includes The IIA's professional practices pamphlet on CSA [95].

[60] W. S. Humphrey, “Characterizing the Software Process,” IEEE Software, Vol. 5, No. 2, March 1988, pp. 73-79.

[61] Arthur E. Hutt, Seymour Bosworth, Douglas B. Hoyt, Computer Security Handbook. Third Edition. John Wiley & Sons, Inc. New York, NY. 1995. ISBN 0-471-1907-0.

[62] IA-CMM: “INFOSEC Assessment Capability Maturity Model. Version 2.1. February 2002.” 100 pages. http://www.nsa.gov/isso/iam/index.htm.

[63] IFAC: “Managing Security of Information.” January 1998. 20 pages. http://www.ifac.org.

[64] The Institute of Internal Auditors (The IIA). http://www.theiia.org.

[65] ISACA: Information Systems Audit and Control Association. http://www.isaca.org.

[66] ISACF: Information Systems Audit and Control Foundation. http://www.isaca.org.

[67] ISO: International Standards Organization. http://www.iso.ch/iso/en/stdsdevelopment/tc/tclist/TechnicalCommitteeStandardsListPage.TechnicalCommitteeStandardsList?COMMID=4006.

[68] Internet Engineering Task Force, “Site Security Handbook.” RFC 1244. July 1991. (101 pages.)

> This document is intended to be a “starting place for further research.” However, the document goes a long ways to providing a thorough basis for a system administrator and manager to assert control over computer security.

[69] “An Introduction to Computer Security: The NIST Handbook.” Special Publication 800-12. October 1995.

[70] ISO 17799. http://www.iso17799software.com/. (This standard is based on BS 7799 [12].)

[71] ITCG: Information Technology: Control Guidelines. 3rd Edition. 1998. (Previously published as “Computer Control Guidelines.”) 414 pages. The Canadian Institute of Chartered Accountants (CICA). [21] Toronto, Ontario, Canada. ISBN 0-88800-494-X.

[72] IT Governance Institute, “Information Security Governance: Guidance for Guidance for Boards of Directors and Executive Management.” 28 pages. 6 refs. http://www.ITGovernance.org/resources.htm. (See also IT Governance Institute, “Board Briefing on IT Governance.” 44 pages. 8 refs. http://www.ITGovernance.org/resources.htm.)

[73] ITGI: Information Technology Governance Institute. (See [65].)

[74] King Committee. The King Report on Corporate Governance. Chapter 20, “The Code of Corporate Practices and Conduct”. (November 29, 1994). Institute of Directors in Southern Africa, tel. +27-11/ 643-8086, fax +27-11/ 484-1416. P. O. Box 908, Parklands, 2121, South Africa. (Chapter 20 is available on-line at http://www.worldbank.org/html/fpd/privatesector/cg/codes.htm.

[75] Leonard I. Krauss, SAFE: Security Audit and Field Evaluation for Computer Facilities and Information Systems. Amacom, New York, 1980. ISBN 0-8144-5526-3.

[76] D. E. Levine, “Auditing Computer Security.” Chapter 9 of Arthur E. Hutt, Seymour Bosworth, Douglas B. Hoyt, editors, Computer Security Handbook. Third Edition. John Wiley & Sons, Inc. New York, NY. 1995. ISBN 0-471-1907-0.

[77] D. E. Levine, “EDP Auditing and Related Packages.” Appendix 15 of Arthur E. Hutt, Seymour Bosworth, Douglas B. Hoyt, editors, Computer Security Handbook. Third Edition. John Wiley & Sons, Inc. New York, NY. 1995. ISBN 0-471-1907-0.

[78] Tom Lillywhite, “How to protect your information—an introduction to BS 7799.” Management Services, January 1999, pp. 20-21.

[79] Ulf Lindqvist, Erland Jonsson, “How to Systematically Classify Computer Security Intrusions.” 1997 IEEE Symposium on Security and Privacy. May 1997, Oakland, California. pp. 154-163.

[80] Catherine Meadows, “An Outline of a Taxonomy of Computer Security Research and Development.” Proceedings of the 1992-1993 ACM Workshop on New Security Paradigms, pp. 33-35.

[81] Mitre Corporation, “Defense-Information Assurance Red Team Methodology.” MP 99B000018. May 1999.

[82] Patrick McBride, Jody Patilla, Craig Robinson, Peter Thermos, Edward P. Moser, Secure Internet Practices: Best Practices for Securing Systems in the Internet and e-Business Age. CRC Press. 2002. Boca Raton, Florida. ISBN 0-8493-1239-6. 209 pages.

[83] National Research Council, Dr. David Clark (MIT), Committee Chair, Computers at Risk: Safe Computing in the Information Age, National Academy Press, 1991.

[84] P. G. Neumann, D. B. Parker, “A summary of computer misuse techniques.” Proceedings of the 12th National Computer Security Conference, pp. 396-407. Baltimore, Maryland, October 1989.

[85] NIST: National Institute of Standards and Technology. http://www.nist.gov/. In particular, the Computer Security Resource Center (CSRC) at NIST: http://csrc.nist.gov/.

[86] OCTAVE^{SM} Method Implementation Guide, Version 2.0. June 2001. 18 Volumes (@ 1,400 pages).

Volume 1: Introduction
Volume 2: Preliminary Activities
Volume 3: Process 1 — Identify Senior Management Knowledge
Volume 4: Process 2 — Identify Operational Area Management Knowledge
Volume 5: Process 3 — Identify Staff Knowledge
Volume 6: Process 4 — Create Threat Profiles
Volume 7: Process 5 — Identify Key Components
Volume 8: Process 6 — Evaluate Selected Components
Volume 9: Process 7 — Conduct Risk Analysis
Volume 10: Process 8 — Workshop A — Develop Protection Strategy
Volume 11: Process 8 — Workshop B — Protection Strategy Selection
Volume 12: Asset Profile Workbook
Volume 13: After the Evaluation
Volume 14: Bibliography and Glossary
Volume 15: Appendix A — OCTAVE Catalog of Practices
Volume 16: Appendix B — OCTAVE Data Flow
Volume 17: Appendix C — Complete Example Results

[87] OECD: Organization for Economic Cooperation and Development, “Guidelines for the Security of Information Systems,” 1992, updated July 1, 1997. 24 pages. http://www1.oecd.org/dsti/sti/it/secur/prod/e_secur.htm#4.

[88] Derek J. Oliver, “Is your business c:cure?” IS Audit & Control Journal, Vol, VI, 1999, pp. 23-26.

[89] Donn B. Parker, Fighting Computer Crime: A New Framework for Protecting Information. John Wiley & Sons. New York, NY. 1998. ISBN 0-471-16378-3

[90] Rod Parkin, “IT Security—An Implementation Strategy.” COMPSEC International 95, 12th World Conference on Computer Security, Audit and Control, 25-27 October 1995, London, UK. pp. 350-363.

[91] Thomas R. Peltier, Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. CRC Press, Boca Raton, Florida. 2002. ISBN 0-8493-1137-3.

[92] T. Perry & P. Wallich, “Can Computer Crime Be Stopped?” IEEE Spectrum, Vol. 21, No. 5, 1984.

[93] Donald L. Pipkin, Information Security: Protecting the Global Enterprise. Prentice-Hall PTR. Upper Saddle River, NJ. 2000.

[94] Michael E. Porter, Competitive Advantage: techniques for analyzing industries and competitors. Free Press, New York, New York. 1980. ISBN 0029253608.

[95] Professional Practices Pamphlet 98-2, “A Perspective on Control Self-Assessment.” The Institute of Internal Auditors. Altamonte Springs, Florida. 1998.

[96] Patrice Rapalus, CSI Director, as quoted in Richard Power’s “2001 CSI/FBI Computer Crime and Security Survey.” Computer Security Journal, Volume XVII, November 2, 2001, pp. 29-51.

[97] Ronald L. Rivest, “Chaffing and Winnowing: Confidentiality without Encryption.” MIT Lab for Computer Science. March 18, 1998. http://theory.lcs.mit.edu/~rivest/chaffing.txt.

[98] James Roth, “Control Model Implementation: Best Practices.” The Institute of Internal Auditors Research Foundation. Altamonte Springs, Florida. 1997. ISBN 0-89413-390-X. 455 pages.

Roth’s book reviews COSO and CoCo, then presents excerpts from questionnaires of COSO implementations from 25 organizations. This is an excellent way to understand what COSO is and how it has been used.

[99] Zella G. Ruthberg, et al., “Guide to Auditing for Controls and Security: A System Development Life Cycle.” NIST Special Publication 500-153. April 1988.

[100] SAC: The Institute of Internal Auditors Research Foundation. “Systems Auditability and Control.” 1994. 1,663 pages in 14 Volumes. ISBN 0-89413-317-9.

Module 1: Executive Summary (33 pages)
Module 2: Audit and Control Environment (67 pages)
Module 3: Using Information Technology in Auditing (143 pages)
Module 4: Managing Computer Resources (137 pages)
Module 5: Managing Information and Developing Systems (102 pages)

Module 6: Business Systems (149 pages)
Module 7: End-User and Departmental Computing (91 pages)
Module 8: Telecommunications (118 pages)
Module 9: Security (138 pages)
Module 10: Contingency Planning (72 pages)
Module 11: Emerging Technologies (280 pages)
Module 12: Master Index (44 pages)
Module 13: Advanced Technology Supplement (261 pages)
Client/Server Implementation: A Management Case Study (28 pages)

[101] Fred B. Schneider, Editor, "Trust in Cyberspace." National Academy Press. 1999. ISBN 0-30906558-5.

[102] Bruce Schneier, "Risks of Relying on Cryptography." Inside Risks Column, CACM, October 1999, Vol. 42, No., 10, pp. 144.

[103] Bruce Schneier, "Secrets & Lies: Digital Secrecy in a Networked World." John Wiley & Sons, Inc. New York, NY. 2000. ISBN 0-471-25311-1.

[104] S.C.O.R.E: Security Consensus Operational Readiness Evaluation. http://www.sans.org/SCORE/.

[105] Arie Segev, Jaana Porra, Malu Roldan, "Internet Security and the case of Bank of America." CACM, October 998, Vol. 41, No. 10, pp. 81-87.

[106] SEI: Software Engineering Institute at Carnegie Mellon University. http://www.sei.cmu.edu/

[107] SSAG: "Security Self-Assessment Guide for Information Technology Systems." Marianne Swanson. NIST Special Publication 800-26. November 2001. 15 body pages, 73 appendix pages.

The questionnaire has been automated and can be downloaded at no cost from http://csrc.nist.gov/asset. It is advisable to download the User Manual first because it describes the system requirements to run the software.

[108] SSE-CMM: Systems Security Engineering - Capability Maturity Model. http://www.sse-cmm.org/.

[109] SSE-CMM: "Model Description Document." Version 2.0. April 1, 1999. 322 pages. System Security Engineering — Capability Maturity Model. http://www.sse-cmm.org/.

[110] SSE-CMM: "Appraisal Method." Version 2.0. April 16, 1999. Approximately 180 pages. System Security Engineering — Capability Maturity Model. http://www.sse-cmm.org/

[111] SysTrust: AICPA/CICA SysTrust Principles and Criteria for Systems Reliability. Version 2.0. January 2001. 71 pages. (The criteria alone, 3 pages, is available on-line at http://www.aicpa.org/assurance/systrust/start2.htm.)

[112] Harold F. Tipton, Micki Krause, editors, Information Security Management Handbook, 4th Edition, 2000. CRC Press, Boca Raton, Florida. 3 volumes. ISBN 0-8493-9829-0, 0-8493-0800-3, and 0-8493-1127-6, respectively.

[113] Eugene F. Troy, "Common Criteria: Launching the International Standard." November 24, 1998. 11 pages. http://csrc.nist.gov/cc/info/infolist.htm.

[114] S. Rao Vallabhaneni, “Auditing Computer Security.” John Wiley & Sons, Inc. New York, NY. 1989. ISBN 0-471-62604-X.

[115] Charles Cresson Wood, William W. Banks, Sergio B. Guarro, Abel A. Garcia, Viktor E. Hampel, Henry P. Sartorio, “Computer Security: A Comprehensive Controls Checklist.” John Wiley & Sons, 1987. ISBN 0-471-84795-X.

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

[117] Charles Cresson Wood, “Best Practices in Internet Commerce Security.” PentaSafe Security Technologies, Inc. Houston, Texas. 2001. 92 pages.