SANDIA REPORT

SAND2006-7179
Unlimited Release
Printed January 2007

The Evolving Story of Information Assurance at the DoD

Philip L. Campbell

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2006-7179
Unlimited Release
Printed February 2007

The Evolving Story of Information Assurance at the DoD

Philip L. Campbell, 5616

Abstract

This document is a review of five documents on information assurance from the Department of Defense (DoD), namely 5200.40, 8510.1-M, 8500.1, 8500.2, and an "interim" document on DIACAP [9]. The five documents divide into three sets: (1) 5200.40 & 8510.1-M, (2) 8500.1 & 8500.2, and (3) the interim DIACAP document. The first two sets describe the certification and accreditation process known as "DITSCAP"; the last two sets describe the certification and accreditation process known as "DIACAP" (the second set applies to both processes). Each set of documents describes (1) a process, (2) a systems classification, and (3) a measurement standard. Appendices in this report (a) list the Phases, Activities, and Tasks of DITSCAP, (b) note the discrepancies between 5200.40 and 8510.1-M concerning DITSCAP Tasks and the System Security Authorization Agreement (SSAA), (c) analyze the DIACAP constraints on role fusion and on reporting, (d) map terms shared across the documents, and (e) review three additional documents on information assurance, namely DCID 6/3, NIST 800-37, and COBIT®.

Keywords: information assurance, certification, accreditation, confidentiality, integrity, availability.

This page intentionally almost blank.

Table of Contents

List of Figures

List of Tables

This page intentionally almost blank.

1 Introduction

This section first provides context for information assurance at the DoD and then proceeds with the "evolving story."

1.1 Context

DITSCAP is the current certification and accreditation (C&A)—both terms are defined below—process for the DoD. DIACAP is a new process that has not yet been officially signed at the DoD Secretary level: DIACAP is currently in "interim" status. The Intelligence Community within the federal government uses a different process, described in DCID 6/3 [8]. FISMA [11] mandates the development of C&A documents for non-DoD and non-intelligence-community systems. NIST SP 800-37, -53, and -60 ([24], [25], and [26]), as a group, fulfill that mandate, as shown in Table 1. The focus of this document is on C&A for the DoD.

Table 1 Federal C&A

Federal entity[a]	C&A process or document(s) that describes that process	Comments
DoD	DITSCAP/DIACAP	
Intelligence community	DCID 6/3	See Appendix E.1 beginning on page 67 herein for more information.
Other federal agencies	OMB A-130, NIST SP 800-37, -53, -60	See Appendix E.2 beginning on page 72 herein for more information.

a. Appendix E.3 beginning on page 74 herein describes an example of what the private sector could use for C&A.

1.2 The Evolving Story

This document focuses on five information assurance (IA) documents from the Department of Defense (DoD). For ease of reference this document uses tags for those documents, as shown in Table 2 below.

Table 2 Document Tags (Sheet 1 of 2)

Tag	Document
5200.40	Department of Defense INSTRUCTION NUMBER 5200.40, December 30, 1997, SUBJECT: DoD Information Technology Security Certification and Accreditation Process (DITSCAP). 68 pages.
8510.1-M	Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP). Application Manual. July 31, 2000. 157 pages.

Table 2 Document Tags (Sheet 2 of 2)

Tag	Document
8500.1	Department of Defense DIRECTIVE NUMBER 8500.1, October 24, 2002, SUBJECT: Information Assurance (IA). 25 pages.
8500.2	Department of Defense INSTRUCTION NUMBER 8500.2, February 6, 2003, SUBJECT: Information Assurance (IA) Implementation. 102 pages.
Interim-DIACAP[a]	[9]

a. The "Interim-DIACAP" term is intended to help distinguish the July 6, 2006 document [9] and the DIACAP process itself. An earlier version of the document bore the number "8510.bb."

The first two documents—5200.40 and 8510.1-M—present the DoD Information Technology Security Certification and Accreditation Process (DITSCAP). The next two documents—8500.1 and 8500.2—are used both by DITSCAP and the DoD Information Assurance Certification and Accreditation Process (DIACAP). The last document—Interim-DIACAP—presents the DoD Information Assurance Certification and Accreditation Process (DIACAP), as depicted in Figure 1.

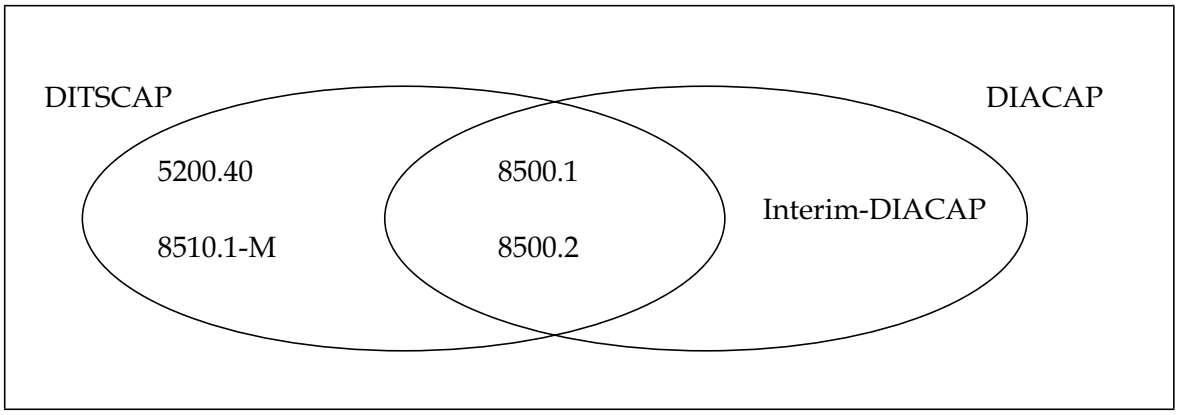

Figure 1 DITSCAP & DIACAP

The documents do not reflect two alternatives to certification and accreditation (C&A) so much as they reflect a transition that suggests an evolving story which becomes evident if we note that Interim-DIACAP cancels both 5200.40 and 8510.1-M (Interim-DIACAP, pages 1 & 11)[1] and

1. Because DIACAP is not yet approved, neither 8500.1 nor 8500.2 reference DIACAP, as we would expect. However, if and when DIACAP is approved, we can expect that new versions of both 8500.1 and 8500.2 will be released, with references to DITSCAP replaced with references to DIACAP.

if we map the five documents to their publication dates, as shown in Figure 2.

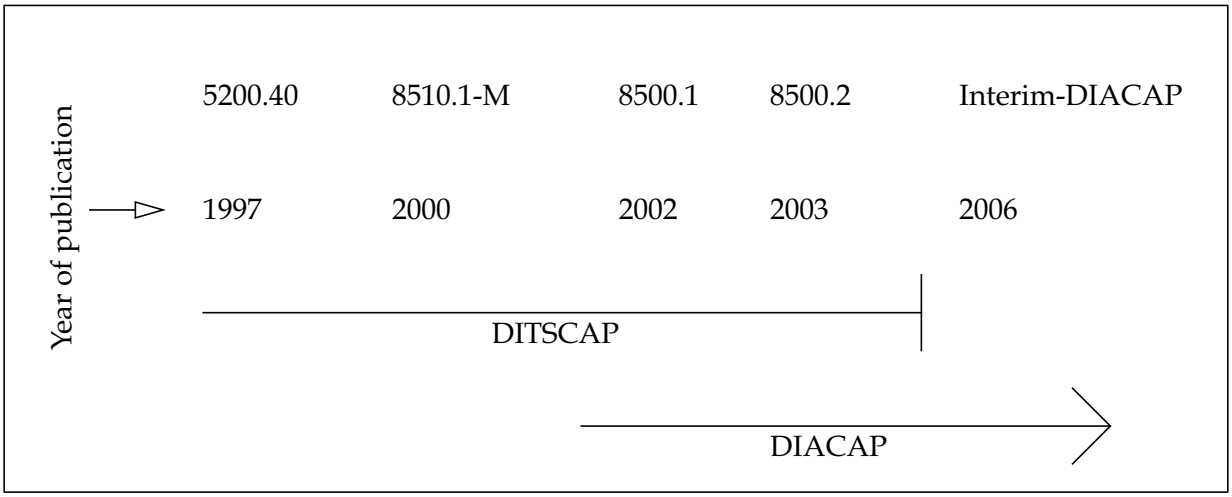

Figure 2 Transition

All five of the documents are concerned with C&A. 5200.40 emphasizes a step-by-step approach using a document called the "System Security Authorization Agreement" (SSAA) which is used to record and guide actions that will provide IA throughout the system life-cycle. By extrapolation, some time prior to 5200.40 the approach to IA may have been a one-time review—a "fire and forget" approach. If that is the case, then 5200.40 may have been the document that introduced the idea of maintaining IA throughout the life-cycle.

8510.1-M introduces the use of questions by which IA could be established. These questions are organized into Checklists for different areas, such as "System Architecture Analysis" and "Software, Hardware, and Firmware Design Analysis." In addition, 8510.1-M introduces "levels" corresponding to the degree of IA needed: Level 1 systems requires minimal IA, Level 4 system requires maximum IA, and Level 2 and Level 3 require intermediate IA.

8500.1 and 8500.2 introduce "IA Controls"[2] which are similar in scope to the questions introduced in 8510.1-M but are objectives instead. That is, an IA Control describes what the relevant safeguards and activities should provide.

Finally, Interim-DIACAP introduces the concept of placing the IA Controls at the focal point of the provision of IA, so the story continues. Meanwhile, a similar evolution may be unfolding within the intelligence community: the Director of National Intelligence is in the middle of a "re-vitalization" of C&A.[3]

1.3 Principles

The principles underlying DITSCAP and DIACAP stem from the basis of their respective

2. See Section 3.2.3 on page 27 below for a definition of "IA Control."

3. See http://www.dni.gov/dniwww/C&A.html.

approaches. The principles are similar but different, which is just as we would expect, given that the latter seems to have evolved from the former. Both DITSCAP and DIACAP are concerned with C&A and both are concerned with the Production phase of a system's life-cycle, but the principles themselves are not the same. DITSCAP rests on two principles:

1. IA is established via agreement between the four people who assume the four, key roles.
2. IA requires attention not only during a system's Design and Development Phases but also during its Production Phase.

DIACAP also rests on two principles:

1. IA is established via IA Controls.
1. IA Controls need to be maintained.

DIACAP's principles are more precise, and their focus on IA Controls is more obvious. DIACAP thus leans toward frameworks such as CoBiT (see Appendix E.3). In a similar vein BSI [1] provides a set of safeguards to counter various threats, where the threats are grouped for products, such as Lotus Notes. ISO 15408 [13][4] presents a catalogue of security functions, a catalogue of assurance requirements, and a method of grouping items from both catalogues so that the effectiveness of a "component or system" ([23], page 4) can be evaluated based on a given grouping.

The reason for the evolution from DITSCAP to DIACAP is clear. The Global Information Grid (GIG)[5] requires standardization of protection levels for systems that interconnect, and the DoD anticipates that almost everything will eventually interconnect. This implies that there should be a standard for determining a protection level to enable uniformity across interconnections. The standard that DIACAP provides is the set of baseline IA Controls specified in 8500.2.

So in general DITSCAP is an agreement-based approach and DIACAP is a compliance-based approach. DITSCAP also uses compliance and DIACAP also uses agreement, but in both cases these are subsidiary.

1.4 Document Sets

The five documents divide into three sets of documents:

- 5200.40 & 8510.1-M,
- 8500.1 & 8500.2, and
- Interim-DIACAP [9].

All three sets of documents present (or refer to a document that presents)

1. a process,

4. ISO 15408 is ISO's adoption of the Common Criteria for Information Technology Security Evaluation, colloquially known simply as the "Common Criteria" [6].

5. The GIG is described in 8500.2, E2.1.21, page 18 and in Interim-DIACAP, E2.1.29, page 17. The "Defense Information Infrastructure" (DII) is described in 5200.40, E2.1.17, page 9 and 8510.1-M, DL1.1.25, page 11.

2. a systems classification, and

3. a measurement standard.

The triad for the first set of documents (5200.40 & 8510.1-M) is as follows:

1. the process is DITSCAP

2. the systems classification consists of four levels based on seven characteristics, and

3. the measurement standard is a set of Checklists of questions.

The triad for the second set of documents (8500.1 & 8500.2) is as follows:

1. the process is "the DoD C&A process" (8500.2, pages 43 & 47)[6],

2. the systems classification consists of nine elements, based on the Cartesian product of three "Mission Assurance Categories" (i.e., importance of the system's integrity and availability to its mission) and three "Confidentiality Levels," and

3. the measurement standard is a set of IA Controls.

The triad for the last document (Interim-DIACAP) is as follows:

1. the process is DIACAP,

2. the systems classification is the same as that provided by 8500.1 & 8500.2,

3. the measurement standard is the same as that provided by 8500.1 & 8500.2.

The triad for the three sets of documents are summarized in Table 3 below.

Table 3 Document Sets

	5200.40 & 8510.1-M	8500.1 & 8500.2	Interim-DIACAP
Process	DITSCAP	"the DoD C&A process"	DIACAP
Systems Classification	Four Levels, based on seven characteristics	Nine elements, based on the Cartesian product of three Mission Assurance Categories (MAC) and three Confidentiality Levels	
Measurement Standard	A set of Checklists containing questions	A set of IA Controls	

1.5 Organization

The remainder of this report is organized as follows. In Section 2 the first set of documents is summarized. In Section 3 the second set of documents is summarized. In Section 4 the third set

6. 8500.2 lists 5200.40 as a reference (reference (n), page 13) and 8500.2 lists "DITSCAP" in its list of acronyms (page 27), but the acronym "DITSCAP" does not appear anywhere else in 8500.2. 8500.2 includes a definition for IA C&A: "E2.1.25. IA Certification and Accreditation (IA C&A). The standard DoD approach for identifying information security requirements, providing security solutions, and managing the security of DoD information systems" (page 20). This would be the logical place to include the DITSCAP acronym, but it is not present.

of documents (consisting of only one document) is summarized.

Appendix A lists the DITSCAP Phases, Activities, and Tasks, based on 8510.1-M.

Appendix B notes discrepancies in the list of Phases, Activities, and Tasks provided by 5200.40 and by 8510.1-M.

Appendix C analyzes Interim-DIACAP's constraints on role fusion and on reporting.

Appendix D lists common terms across the five documents, as a measure of common focus.

Appendix E summarizes three additional IA documents, the first two from government agencies (namely the Director of Central Intelligence (DCI) and the National Institute of Standards and Technology (NIST)), which round out the government view on C&A, and the last from an international, non-profit organization (namely ISACA).

2 5200.40 & 8510.1-M

This section first describes DITSCAP, then reviews 5200.40, and then reviews 8510.1-M, presenting for each (1) the process, (2) the systems classification, and (3) the standard of measurement provided by each document.

2.1 DITSCAP

DITSCAP is an acronym for "DoD Information Technology Security Certification and Accreditation Process." Note that DITSCAP is a process. The four DITSCAP Phases consist of a number of "Activities" which, in turn, consist of a number of "Tasks" (a list is shown in Appendix A beginning on page 45 herein).

DITSCAP is an agreement-based approach. DITSCAP rests on two principles:

1. IA is established via agreement between the four people who assume the four, key roles.
2. IA requires attention not only during a system's Design and Development Phases but also during its Production Phase.

The above principles devolve into the following three operations:

1. Get agreement by all the role-players (i.e., stakeholders) (see Table 4), not just by a set of experts:

   > The key to the DITSCAP is the agreement between the IT system program manager, the DAA, the CA, and the user representative. (5200.40, E3.1.3, page 16)

2. Get the role-players to produce a formal, written agreement (i.e., the System Security Authorization Agreement (SSAA)), not just an informal, verbal agreement.
3. Get the role-players to agree at each stage in the system life-cycle, including production, and not just at the end of development, by using their formal, written agreement dynamically, not statically, adding details to the agreement or changing it as the process progresses.

The purpose of DITSCAP is to establish requirements (Phase 1) and then confirm that the system complies with those requirements (a) as the system develops and (b) as the system is maintained during production (Phases 2, 3, and 4). Both 5100.40 and 8510.1-M use four nouns—accreditation, certification, validation, and verification—in connection with this process. Accreditation is the act of accepting a system as certified; certification is the confirmation of compliance; verification is certification when performed while the system is under development (and during production); and validation is certification when performed after development has been completed and before production has begun. The following are the definitions from 5200.40:

> E2.1.2. Accreditation. Formal declaration by the DAA that an IT system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. (5200.40, page 8)
>
> E2.1.8. Certification. Comprehensive evaluation of the technical and non-technical security features of an IT system and other safeguards, made in support of the accreditation process,

Table 4 DITSCAP Roles

Roles	Abbreviation	Responsibilities
Designated Approving Authority	DAA	The person who accepts the residual risk E2.1.18. Designated Approving Authority (DAA or Accreditor). Official with the authority to formally assume the responsibility for operating a system or network at an acceptable level of risk. (5200.40, page 10) DL1.1.26. Designated Approving Authority (DAA or Accreditor) Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with design accrediting authority and delegated accrediting authority. (8510.1-M, page 11)
Certification Authority	CA	The technical expert (5200.40, E3.3.4.1, page 23) E2.1.9. Certification Authority (CA). The official responsible for performing the comprehensive evaluation of the technical and non-technical security features of an IT system and other safeguards, made in support of the accreditation process, to establish the extent that a particular design and implementation meet a set of specified security requirements. (5200.40, page, 9) DL1.1.12. Certification Authority (Certifier). Individual responsible for making a technical judgement of the system's compliance with stated requirements, identifying and assessing the risks associated with operating the system, coordinating the certification activities, and consolidating the final certification and accreditation package. (8510.1-M, page 9)
User Representative	(none used)	The person who represents the users (5200.40, E2.1.42, page 12) (8510.1-M, DL1.1.81, page 17)
Program Manager	(none used)	The person who is the focal point of the process E2.1.42. Program Manager. The person ultimately responsible for the overall procurement, development, integration, modification, or operation and maintenance of the IT system. (5200.40, page 12). DL1.1.58. Program Manager. The person ultimately responsible for the overall procurement, development, integration, modification, or operation and maintenance of the IS. (8510.1-M, page 15)

to establish the extent that a particular design and implementation meets a set of specific security requirements. (5200.40, page 8)

E2.1.64. Validation. Determination of the correct implementation in the completed IT system with the security requirements and approach agreed on by the users, acquisition authority, and the DAA. (5200.40, page 14)

E2.1.65. Verification. The process of determining compliance of the evolving IT system specification, design, or code with the security requirements and approach agreed upon by the users, acquisition authority, and the DAA. (5200.40, page 14)

As will be explained below, DITSCAP consists of four "Phases." These Phases are to be applied in sequence, with the last Phase continuing through the maintenance part of the lifecycle. However, if, during any Phase, the "security posture" (undefined) significantly changes, then a new iteration of the Phases begins, as suggested by Figure 3.

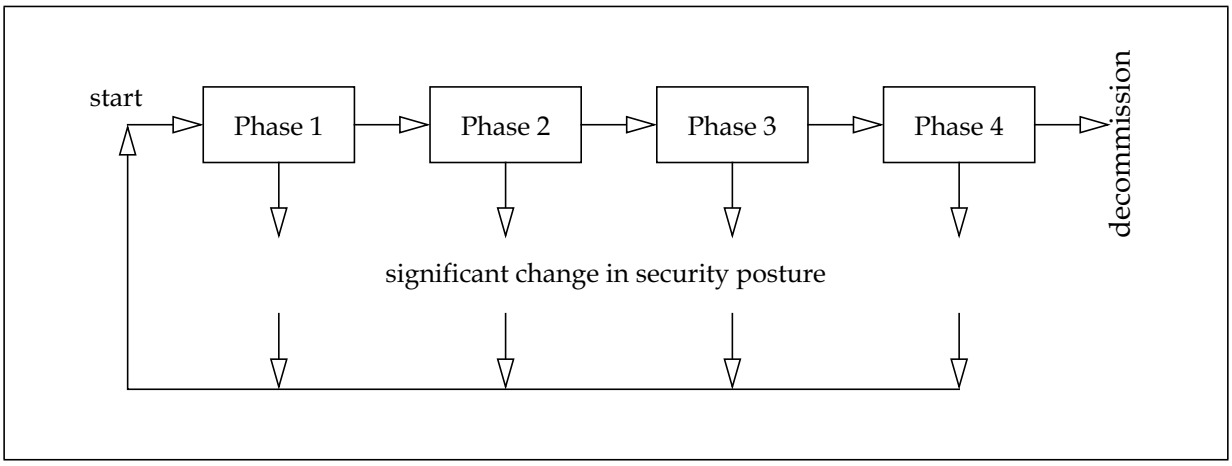

Figure 3 Iterative Nature of DITSCAP

At the coarsest level of granularity, DITSCAP consists of two types of Phases:

- a Definition type, in which the system and the development plan are described and which happens only once per DITSCAP iteration, and
- a Certification type, which can occur many times per DITSCAP iteration. DITSCAP is comprised of four Phases with the names Definition, Verification, Validation, and Post Accreditation.

The Definition Phase, which is Phase 1, is of the Definition type; the other three Phases—referred to as Phases 2, 3, and 4—are of the Certification type.

The job of the Definition Phase is the writing of and agreement by the stakeholders to the "binding" (8510.1-M, C2.1.1.6, page 29) System Security Authorization Agreement (SSAA). The SSAA is the "basis of agreement" (5200.40, E3.3.5.2, page 25). It "document[s] the conditions of C&A" (5200.40, E3.3.5, page 24) and is thus similar to a contract in that the DAA agrees to accredit (i.e., formally accept) the system if the system passes certification. At the same time, the SSAA is unlike a contract in that the DAA does not appear to be required to accredit the system even if the results of the certification step in Phase 3 are acceptable. The name that DITSCAP gives to this first Phase is Definition but the name obscures the contractual nature of the SSAA. The intent of the Phase would be clearer if the name were Agreement, for example.

The job of the other three Phases is certification. DITSCAP partitions the life-cycle into three parts which we could call development, acceptance, and production. There is a Phase for each part, named Verification, Validation, and Post Accreditation, respectively. Unfortunately, these names obscure the common theme of certification. The names also obscure the fact that Verification is done possibly many times during development but Validation is done only once, at acceptance. The name Post Accreditation, coming immediately after Validation, suggests that an Accreditation Phase has been overlooked, until one realizes that Validation *is* Accreditation,

in which case one wonders why the Validation Phase was not called Accreditation in the first place. The intent of the Phases would be more evident if the names were Certification during Development, Certification at Acceptance, and Certification during Production, for example, as suggested in Table 5 below.

Table 5 DITSCAP Given and Suggested Phase Names

Phase	Given Phase Name	Suggested Phase Name
1	Definition	Agreement
2	Verification	Certification during Development
3	Validation	Certification at Acceptance
4	Post Accreditation	Certification during Production

2.2 5200.40

This section presents (1) the process, (2) the systems classification, and (3) the standard of measurement provided by 5200.40.

2.2.1 Process for 5200.40

One of the recurring themes of 5200.40 is the word "agreement." The goal of almost all the Phases, Activities, and Tasks is to come to agreement, either about a definition or about certification. A second recurring theme is the word "tailor." DITSCAP can be adjusted to suit many needs. However, all activities in these phases are "mandatory" (5200.40, 6.4, page 5 (see also 8510.1-M, C2.1.2, page 29)), and none of the requirements agreed upon in Phase 1 can be tailored.

DITSCAP is intended to be "adaptable to any type of IT system and any computing environment and mission" (5200.40, 6.4, page 5) and apparently any program development strategy. 5200.40 describes four such strategies:

- **evolutionary**: design and implementation alternate in time, and subsequent designs are not defined at system inception (5200.40, E2.1.23, page 10);
- **grand design**: all of the design precedes all of the implementation (5200.40, E2.1.25, page 10);
- **incremental**: design and implementation alternate in time, but subsequent design is already defined at system inception (5200.40, E2.1.26, page 10);
- **other**: "variations and/or combinations" of the previous three strategies (5200.40, E2.1.41, page 12) (see also 8510.1-M, Chapter 7, pages 131-2).

2.2.2 Systems Classification for 5200.40

5200.40 includes a description of the "ITSEC [Information Technology Security] system classes." In this classification scheme, systems are grouped based on seven characteristics:

1. Interfacing Mode

2. Processing Mode
3. Attribution Mode
4. Mission-Reliance Factor
5. Accessibility Factor
6. Accuracy Factor
7. Information Categories (5200.40, Table E7-1, page 58)

For each characteristic a system is required to be assigned exactly one of a set of three or four mutually-exclusive values.[7] For example, for the Interfacing Mode characteristic, a system is either Benign, or Passive, or Active. This arrangement describes 9,216 classes.[8]

Mention is made in 5200.40 of "four certification levels" (5200.40, E3.3.3.6, page 22) that would provide "minimum-security requirements" (5200.40, E3.3.3.2, page 21). There does not appear to be even a set of names for the four certification levels in 5200.40. However, a name set does appear in 8510.1-M, as follows:

Level 1 - basic security review,
Level 2 - minimum analysis,
Level 3 - detailed analysis, or
Level 4 - comprehensive analysis. (8510.1-M, C2.1.3, page 30)

It is intended that each of the system classes should map to the four certification levels. Such a mapping does not appear to be presented in 5200.40. However, a mapping does appear in 8510.1-M, as shown in Section 2.3.2 below.

2.2.3 Measurement Standard for 5200.40

No measurement standard is described in 5200.40. However, a standard is described in 8510.1-M (see Section 2.3.3 below).

---

7. This count assumes no distinction between the five possible types of Sensitive information within the "Information Categories" characteristic.

8. $3 * 4 * 4 * 4 * 4 * 3 * 4 = 3^2 * 4^5 = 9 * (2^2)^5 = 9 * 2^{10} = 9 * 1{,}024 = 9{,}216$.

Unfortunately 8510.1-M describes a different number of system classes.

Both 5200.40 and 8510.1-M use the same number of characteristics (seven) and, for the first six characteristics, both documents use same number of alternatives. However, for the last characteristic, Information Categories, 5200.40 uses *four* alternatives (Unclassified, Sensitive, Collateral Classified, or Compartmented/Special Access Classified (5200.40, Table E7-1, page 58)) but 8510.1-M uses *six* alternatives (Unclassified, Sensitive, Confidential, Secret, Top Secret, Compartmented/Special Access Classified) (8510.1-M, Table C3.T9, page 53)). As a result, 8510.1-M describes 3/2 as many classes as 5200.40, namely $3 * 4 * 4 * 4 * 4 * 4 * 3 * 6 = 3^3 * 2^9 = 27 * 512 = 13{,}824$.

Within the Sensitive alternative, both 5200.40 and 8510.1-M use what we could call sub-alternatives. If we account for these, the two documents still describe different numbers of system classes. Within the Sensitive alternative 5200.40 uses *five* sub-alternatives (Privacy Act, Financially Sensitive, Administrative, Proprietary, or Other (5200.40, Table E7-1, page 58)), but 8510.1-M uses only *four* (Privacy Act, Financially Sensitive, Proprietary, Administrative/Other (8510.1-M, C3.4.8.2.1.1.7.2.1-4, pages 57-8)). If we factor these sub-alternatives into the number of classes, then 5200.40 describes $3 * 4 * 4 * 4 * 4 * 4 * 3 * 8 = 3^2 * 2^{11} = 9 * 2{,}048 = 18{,}432$ classes and 8500.1-M describes $3 * 4 * 4 * 4 * 4 * 4 * 3 * 9 = 3^4 * 2^8 = 81 * 256 = 20{,}736$ classes.

So, between the two documents, there are at least 9,216 system classes and not more than 20,736.

2.3 8510.1-M

8510.1-M is a clarification and expansion of 5200.40's description of DITSCAP. What 5200.40 describes in 26 pages in Enclosure 3, 8510.1-M describes in 104 pages in Chapters 3-7.[9] As I understand it, 8510.1-M takes precedence over 5200.40 in typical usage.

2.3.1 Process for 8510.1-M

For each Task within each Activity within each Phase, 8510.1-M provides the following five items: the objective, the description, the prerequisite tasks, the input, and the output. For each Phase the document lists the roles and responsibilities for the DAA, the CA, the user representative and the program manager. The names of the Phases, Activities, and Tasks are shown in Appendix A beginning on page 45 herein.

2.3.2 Systems Classification for 8510.1-M

8510.1-M provides names and minimal descriptions of the four levels of certification noted in 5200.40 (8510.1-M, Table C3.T8, page 53). Level 1 is established by the "completion of the minimum security checklist." Level 2 is differentiated from Level 1 by an "independent certification analysis," and Level 3 is differentiated from Level 2 by a "more in-depth, independent analysis," and Level 4 is differentiated from Level 3 by "the most extensive independent analysis" (ibid.).

8510.1-M also maps the system classes (see Section 2.2.2 above) defined by ITSEC to the four levels of certification. Each of the values for the seven characteristics is given a numeric value (8510.1-M, Table C3.T9, page 53). The sum of the values for all the characteristics falls in the range of 3-48 inclusive. Most of the sums map to one Level, but 20 of the sums map to two Levels (8510.1-M, Table C3.T10, page 59). It is not clear how to determine which Level is to be used in the case of those 20 overlapping values, though 8510.-1M does say that it should be done "as agreed to by the DAA, the Certifier [i.e., the CA], the program manager, or[10] user representative" (8510.1-M, C3.4.8.2.1.3, page 59), thereby following the agreement-philosophy of DITSCAP.

2.3.3 Measurement Standard for 8510.1-M

8510.1-M provides a set of Checklists, each set presented in a separate Table in Appendix 2 (8510.1-M, pages 146-57), for Phases 2 and 3 for Level 1 security. For Phase 2, there are six Checklists. There is no Checklist for Task 2-6 "Security Requirement Validation Procedures" (8510.1-M, C4.3.7, page 82) even though the "Input" for the Task 2-6, as shown on page 83 of 8510.1-M, calls for a Checklist. For Phase 3, there are Checklists for all eight of the Tasks.

The coverage of the Checklist Tables in Appendix 2 is shown below in Table 6.

---

9. I am not counting the Checklists in Appendix 2 of 8510.1-M in this page count.

10. Not "and"?

Table 6 Checklist Coverage

Level	Phase 1	Phase 2			Phase 3			Phase 4
		Task	Description	Appendix 2 Table	Task	Description	Appendix 2 Table	
1	(No certification analysis Activity in this Phase)	2-1[a]	page 68	T1	3-1	page 94	T7	(No checklists provided)
		2-2	page 70	T2	3-2	page 97	T8	
		2-3	page 74	T3	3-3	page 99	T9	
		2-4	page 77	T4	3-4	page 101	T10	
		2-5	page 79	T5	3-5	page 103	T11	
		2-6	page 82	(No Checklist provided)	3-6	page 105	T12	
		2-7	page 84	T6	3-7	page 107	T13	
		(There are only 7 Phase 2 Tasks)			3-8	page 108	T14	
2		(No Checklists provided)			(No Checklists provided)			
3								
4								

a. The following explanation of part of this first line of the table should be sufficient to explain the rest of the table: Task 2-1 is described on page 68 of 8510.1-M and the Checklist for this Task is shown in Table AP2.T1 in Appendix 2.

Each item in a Checklist consists of a question that is to be answered with one of three choices: Yes, No, or N/A. The following are the first two items in the Checklist for the first relevant Task in the certification activity for Phase 2:

> 1. Does the systems architecture documentation describe the architecture, including graphics, of the system and interconnections providing or supporting, system functions?
>
> 2. For a domain, does the systems architecture show how multiple systems link and interoperate and describe the internal construction and operations of particular systems within the architecture? (8510.1-M, Table AP2.T1, page 146)

There are 105 items in the six Checklists for Phase 2, and 92 items in the eight Checklists for Phase 3.

For each of the Tasks, there is a Task Description that describes how to perform the Task at each Level. The instructions for Level i+1, $1 \le i < 4$, are a superset—usually proper—of the instructions for Level i. For example, the instruction for Level 1 for Task 2-1, the first Task in the certification Activity in Phase 2, is simply

> Complete the Minimal Security Activity Checklist [for this particular Task].[11] (8510.1-M, C4.3.2.2.1, page 68)

For Level 2 the instruction is

> C4.3.2.2.2. Level 2. Complete the Minimal Security Activity Checklist. Analyze the system level information to evaluate the security architecture compliance with the approach stated in the SSAA. The system architecture must be evaluated for compliance with the security requirements. The interfaces between this and other systems must be identified and their ability to preserve the security integrity must be evaluated. The system architecture must be evaluated for consistency with other governing architectures (Department of Defense Intelligence Information System (DoDIIS) Reference Model. etc.). (8510.1-M, pages 68-9)

Presumably the instruction above is to be used to generate Checklists specifically for Level 2. However, no help is given on how we are to create those Checklists to guide our evaluation of an interface's "ability to preserve the security integrity," for example.

The Level 3 instruction, in this continuing example, changes one sentence in the Level 2 instruction and adds two, new sentences. Instead of the Level 2 sentence

> Analyze the system level information to evaluate the security architecture compliance with the approach stated in the SSAA.

the Level 3 sentence is

> Conduct a **detailed analysis** of the system level information to evaluate the security architecture compliance with the stated approach in the SSAA. (8510.1-M, C4.3.2.2.3, page 69, emphasis in the original)

The two new sentences are

> **Security test plans and procedures must be developed. Each security requirement identified in the SSAA must be validated through testing.** (8510.1-M, C4.3.2.2.3, page 69, emphasis in the original)

The Level 4 instruction changes the same sentence that the Level 3 instruction changed, and Level 4 adds one new sentence. The changed sentence now reads

> Conduct a **comprehensive analysis** of the system level information to evaluate the security architecture compliance with the stated approach in the SSAA. (8510.1-M, C4.3.2.2.4, page 69, emphasis in the original)

The new sentence is

> **The system analysis must include fault tree analysis, flaw hypothesis, or similar type of analysis.** (8510.1-M, C4.3.2.2.4, page 69, emphasis in the original)

At the end of the material for each Task is a list of suggested references for that particular Task.

---

11. The Checklist for this Task is in Table AP2.T1 on page 146.

The following is an example of a reference:

> C4.3.2.6.1. “Systems Engineering Management Guide” (Defense Systems Management College, January 1990 (reference n)) (8510.1-M, page 69)

This page intentionally almost blank.

3 8500.1 & 8500.2

This section reviews 8500.1 first, followed by 8500.2.

3.1 8500.1

This section presents (1) the process, (2) the systems classification, and (3) the standard of measurement provided by 8500.1.

3.1.1 Process for 8500.1

8500.1 states that 5200.40 provides the direction for certification and accreditation:

> 4.13. All DoD information systems shall be certified and accredited in accordance with DoD Instruction 5200.40 (reference (u)). (8500.1, page 6)

In addition, NSTISS Policy Number 11 [22] provides the direction for evaluation and validation of components and products:

> All IA or IA-enabled IT hardware, firmware, and software components or products incorporated into DoD information systems must comply with the evaluation and validation requirements of National Security Telecommunications and Information Systems Security Policy Number 11 (reference (w)). (8500.1, 4.17, page 7)

3.1.2 Systems Classification for 8500.1

8500.1 defines a nine-element systems classification which is the Cartesian product of three Mission Assurance Categories and three Confidentiality Levels. This systems classification is related to Information Assurance (IA) as follows. 8500.1 defines Information Assurance (IA) as a collection consisting of confidentiality, integrity, availability, authentication, and non-repudiation (8500.1, E2.1.17, page 20). 8500.1 continues, "Requirements for availability and integrity are associated with the information mission assurance category, while requirements for confidentiality are associated with the information classification or sensitivity and need-to-know" (i.e., Confidentiality Level) (8500.1, 4.7, page 4).

3.1.3 Measurement Standard for 8500.1

8500.1 notes that "Both sets of requirements [(1) for availability & integrity and (2) for confidentiality] are primarily expressed in the form of IA Controls" (8500.1, 4.7, page 4), which are not presented in 8500.1 but are shown in the Attachments to Enclosure 4 of 8500.2 (see Section 3.2.3 below). Authentication and non-repudiation seem to be minor concerns but are also taken care of: "The IA solutions that provide availability, integrity, and confidentiality also provide authentication and non-repudiation" (8500.1, 4.7, page 4).

3.2 8500.2

8500.2 implements 8500.1: "This Instruction implements the policies established in DoD Directive 8500.1 (reference (a))" (8500.2, 4, page 2).

The Global Information Grid, to which DoD systems are moving, is "inherently vulnerable to exploitation and denial of service" (8500.2, E3.1.1, page 30). "Complete confidence…cannot be achieved" (8500.2, E3.1.2, page 30). Thus, because we cannot eliminate risk, the best we can hope for is to manage it. This requires that we be able to assess needs, design purposefully, implement controls, test & verify, and manage change. Enclosure 4 of 8500.2 "establishes a baseline set of IA Controls to be applied to all DoD Information Systems" (8500.2, E3.2.2, page 31). The Information Assurance Technical Framework (IATF) [12] "is a common reference guide for selecting and applying adequate and appropriate IA and IA-enabled technology" (8500.2, E3.2.4, page 32).

This section presents (1) the process, (2) the systems classification, and (3) the standard of measurement provided by 8500.2.

3.2.1 Process for 8500.2

8500.2 states that "all elements of a DoD information system IA program shall be developed, implemented, and maintained through the DoD IA C&A process" (8500.2, E3.4.9, page 47). The process is DITSCAP.

3.2.2 Systems Classification for 8500.2

DoD information systems that require C&A are confined to the following four types[12]:

1. Automated Information System (AIS) Application,
2. Enclave,
3. Outsourced IT-Based Process, and
4. Platform IT Interconnection (8500.2, E2.1.17, pages 17-8).

C&A is not required for systems that are not one of the above four system types.

In order to determine the applicable set of IA controls, a different classification system is used, consisting of nine-elements and described in the next three paragraphs.

8500.2 defines three Mission Assurance Categories (MAC), based on (1) the importance of the data to the mission and (2) the impact of a loss of availability and/or integrity to the mission.

- In MAC I systems, the data is "vital" to the mission; the loss of either availability or integrity is "unacceptable."

12. These types are also defined in 8500.1.

- In MAC II systems, the data is "important" to the mission; the loss of integrity is still "unacceptable" but the loss of availability can be "tolerated" though only "for a short time."
- In MAC III systems, the data is "necessary" to the mission, and the loss of either availability or integrity "can be tolerated or overcome without significant impact on mission effectiveness or potential readiness" (8500.2, E2.1.38, pages 22-3).

8500.2 also defines three Confidentiality Levels, named Classified, Sensitive, and Public (8500.2, E2.1.8, page 16).

The Cartesian product of the three MAC levels and the three Confidentiality Levels produces a nine-element systems classification scheme, shown in Table 9 below.

3.2.3 Measurement Standard for 8500.2

The measurement standard presented in 8500.2 is a set of IA Controls. An IA Control is defined formally as follows:

> E2.1.26. IA Control. An objective IA condition of integrity, availability or confidentiality achieved through the application of specific safeguards or through the regulation of specific activities that is expressed in a specified format (i.e., a control number, a control name, control text and a control class). Specific management, personnel, operational, and technical controls are applied to each DoD information system to achieve an appropriate level of integrity, availability, and confidentiality in accordance with OMB Circular A-130 (reference (v)). (8500.2, page 20)[13]

An IA Control is defined informally as follows:

> E4.1.2. An IA Control describes an objective IA condition achieved through the application of specific safeguards or through the regulation of specific activities. The objective condition is testable, compliance is measurable, and the activities required to achieve the IA Control are assignable and thus accountable. (8500.2, page 48)

There are four parts to each IA Control:

1. a **Subject Area** (this appears to correspond to the "control class" of E2.1.26 (see above)),
2. a **Control Number**,
3. a **Control Name**, and
4. a **Control Text**,

13. This definition is the same as that used in 8500.1 (E2.1.19, page 20). Interim-DIACAP replaces the final phrase "OMB Circular A-130" with "DoDI 8500.2" ([9], E2.1.36, page 18). The reference to OMB A-130 appears to be an editing oversight: OMB A-130 is not imposed on the DoD. (Neither 5200.40 nor 8510.1-M provide a definition of IA Control.)

as described in Table 7 below.

Table 7 IA Control Parts[a]

Part	Description	Example
IA Control Subject Area	(The Subject Areas are listed in Table 8 below.)	"Enclave and Computing Environment"
IA Control Number (e.g., "ECCT-1")	The two-letter abbreviation of the Subject Area, followed by…	EC
	the two-letter abbreviation of the Control Name (see below in this table), followed by…	CT
	a dash, followed by…	-
	the integer that is the "Control Level" (i.e., the robustness level of the control[b]).	1
IA Control Name	This is name of the control.	"Encryption for Confidentiality (Data in Transit)"
IA Control Text	This describes the IA Control.	"Unclassified, sensitive data transmitted through a commercial or wireless network are encrypted using NIST-certified cryptography (See also DCSR-2)." (8500.2, page 95)

a. This table is adapted from Figure E4.F1 (8500.2, page 48).

b. "Robustness" refers to the "strength of a mechanism." There are three levels of robustness—High, Medium, and Basic—denoted with the integers 3, 2, 1, respectively. The integer indicates the "Control Level." Basic robustness corresponds to "good commercial practice" (8500.2, E3.2.4.3.4, page 33).

If there is an IA Control with Control Level 3, then there exists two additional IA Controls with similar Control Numbers but with Control Level 2 and Control Level 1.

If there is an IA Control with Control Level 2, then there exists one additional IA Control with a similar Control Number but with Control Level 1, and there *may* exist a second additional IA Control with a similar Control Number but with Control Level 3.

If there is an IA Control with Control Level 1, then there *may* exist an additional IA Control with a similar Control Number but with Control Level 2, and if that IA Control exists, then there *may* exist a second additional IA Control with a similar Control Number but with Control Level 3 (8500.2, E4.1.3.4, page 49).

The IA Controls are partitioned based on the eight Subject Areas that appear in Table 8 below (the Names of the IA Control Subject Areas in Table 8 appear in the same order as they do in the

Attachments to 8500.2).

Table 8 IA Control Subject Areas[a]

Name	Abbreviation	Number of IA Controls in the Subject Area
Security Design & Configuration	DC	31
Identification and Authentication	IA	9
Enclave and Computing Environment	EC	48
Enclave Boundary Defense	EB	8
Physical and Environmental	PE	27
Personnel	PR	7
Continuity	CO	24
Vulnerability and Incident Management	VI	3
		TOTAL = 157

a. This is a slight superset of Table E4.T1 on page 49 of 8500.2—I added the total. (I also reordered the columns.)

The IA Controls are not spread evenly across the Subject Areas. For example, the four most-populous Subject Areas comprise 83% of the total number of IA Controls.

As an example of an IA Control—in addition to the one shown in Table 7—the following is the first IA Control for the first Attachment, A1:

> DCAR-1 Procedural Review
>
> An annual IA review is conducted that comprehensively evaluates existing policies and processes to ensure procedural consistency and to ensure that they fully support the goals of uninterrupted operations. (8500.2, page 54)

The IA Control Subject Area for the example IA Control above is Security Design & Configuration, which we can determine by the appearance of the Subject Area's abbreviation, "DC" (see Table 8), in the IA Control Number, which is "DCAR-1." The Control Level is 1. The IA Control Name is Procedural Review. The IA Control Text is "An annual…uninterrupted operations," as shown above.

The following is the second IA Control in the first Attachment, A1:

> DCBP-1 Best Security Practices
>
> The DoD information system security design incorporates best security practices such as single sign-on, PKE, smart card, and biometrics. (8500.2, page 54)

Attachments A1, A2, and A3 provide the integrity and availability requirements for Mission Assurance Categories I, II, and III respectively; Attachments A4, A5, and A6 provide the confidentiality requirements for the three Confidentiality Levels, Classified, Sensitive, and

Public, respectively. The assignment of Attachments enables us to populate the nine-element systems classification, described in Section 3.2.2 above, with IA Controls, as shown in Table 9 below.

Table 9 8500.2 Systems Classification

MAC	Confidentiality Level		
	Classified	**Sensitive**	**Public**
I	A1 & A4	A1 & A5	A1 & A6
II	A2 & A4	A2 & A5	A2[a] & A6
III	A3 & A4	A3 & A5	A3 & A6

a. Table E4.T2 on page 50 in 8500.2, from which this table was derived, shows A3 in this cell, not A2 as shown here. A2 fits the pattern, not A3, and there is no note adjacent to Table E4.T2 explaining this deviation, so I assume that the correct entry is A2, not A3.

Given a MAC level and a Confidentiality Level we can use Table 9 to determine the two Attachments that specify the IA Controls we should use. Each element in Table 9 is referred to as a "baseline IA level" (8500.2, E4.1.1, page 48). The word "baseline" in this context appears to be shorthand for "these controls apply, in addition to whatever other security requirements apply."

There are 293 IA Controls listed in the six Attachments, as shown in Table 10, but only 157 are unique: some of the IA Controls are included in more than one of the six Attachments.

Table 10 Number of IA Controls[a]

Attachment	Subject		Confidentiality	Integrity	Availability	
A1	Mission Assurance Category	I		32	38	70
A2		II		32	38	70
A3		III		27	37	64
A4	Confidentiality Level	Classified	45			45
A5		Sensitive	34			34
A5		Public	10			10
Column Totals →			89	91	113	Grand Total = 293

a. The material in this table is gleaned from Attachments 1-6, pages 54-102, of Enclosure 4 in 8500.2.

8500.2 notes that the IA Controls "must be explicitly addressed as part of an information system

security engineering process" (8500.2, E3.4.2, page 41). The IA Controls "shall constitute the baseline requirements for IA certification and accreditation or reaccreditation" (8500.2, E4.1.9, page 53).

The IA Controls are different than the security functional requirements of the Common Criteria, for example. IA Controls are concerned with the "definition, configuration, operation, interconnection, and disposal of DoD information systems" (8500.2, E3.4.3, page 42); the Common Criteria, on the other hand, constitutes "an engineering language and method for specifying the security features of individual IT products" (ibid.).

This page intentionally almost blank.

4 Interim-DIACAP

This section first presents (1) the process, (2) the systems classification, and (3) the standard of measurement provided by Interim-DIACAP. This section then summarizes DIACAP, followed by a comparison of DIACAP with DITSCAP.

4.1 Process for Interim-DIACAP

DIACAP, as described by Interim-DIACAP [9], provides a process in the form of a series of "activities," each of which consists of one or more "tasks," and all of which may run "concurrently or at different frequencies" ([9], E3.5, page 31), as shown in Table 11. (The DIACAP process is compared with the DITSCAP process in Section 4.5.2 on page 38.)

Table 11 DIACAP Activities[a]

Activity	Task[b]
1. Initiate and Plan C&A	1.1 Register system with DoD Component IA Program
	1.2 Assign IA Controls
	1.3 Assemble DIACAP Team
	1.4 Initiate DIACAP Implementation Plan
2. Implement and Validate Assigned IA Controls	2.1 Execute DIACAP Implementation Plan
	2.2 Conduct Validation Activities
	2.3 Compile Validation results in DIACAP Scorecard
3. Make Certification Determination & Accreditation Decision	3.1 Make Certification Decision
	3.2 Issue Accreditation Decision
4. Maintain Authority to Operate and Conduct Reviews	4.1 Maintain Situational Awareness (Review of IA Controls must occur at least annually)
	4.2 Maintain IA Posture
5. Decommission	5.1 Retire system

a. This table uses the text of Figure E3.2 ([9], page 31).

b. For ease of reference, the tasks are given numbers in this Table (e.g., "1.1", "1.2"). The tasks are not numbered in Interim-DIACAP.

4.2 Systems Classification for Interim-DIACAP

Interim-DIACAP does not present a systems classification but simply refers to the one presented in 8500.2 (see Section 3.2.2 on page 26).

4.3 Measurement Standard for Interim-DIACAP

As with the systems classification, Interim-DIACAP does not present a measurement standard

but simply refers to the one presented in 8500.2 (see Section 3.2.3 on page 27).

4.4 DIACAP

DIACAP is a compliance-based approach. DIACAP rests on two principles[14]:

1. IA is established via IA Controls.
2. IA Controls need to be maintained.

The meaning of C&A is defined in terms of IA Controls:

> E2.1.25. DoD Information Assurance Certification and Accreditation Process (DIACAP). The Dod processes for identifying, implementing, validating, certifying, and managing IA capabilities and services, *expressed as IA controls*[15], and authorizing the operation of DoD information systems[16] in accordance with statutory, Federal and DoD requirements. ([9], page 15, emphasis added)

More succinctly, IA Controls are the "basis" for C&A ([9], E3.3.3, page 28).

The IA Controls for a given system are referred to as Assigned IA Controls and that set is defined as follows:

> E2.1.5. Assigned IA Controls. A list of all IA Controls that a DoD information system must address to achieve an adequate IA posture. Assigned IA Controls include all baseline DoD IA Controls, optional DoD IA Controls for special conditions or technologies, e.g., health information portability and privacy or cross security domain solutions, and DoD Mission Area Component and DoD information system supplements, if any. ([9], page 13)

The set of Assigned IA Controls thus consists of two subsets:

1. a set of "baseline" IA Controls, the membership for which is determined by 8500.2 (see Table 9 on page 30 herein), and
2. a set of additional IA Controls that may be peculiar to a given system.

Risk Management is to be achieved "through the implementation of assigned IA Controls" ([9],

---

14. neither of which is made explicit, unfortunately, in Interim-DIACAP.

15. This expression, "expressed as IA Controls," appears in exactly two other places in Interim-DIACAP: Paragraph 4.1 ([9], page 2), and Paragraph E3.1 ([9], page 27).

16. "E.2.1.46. Information System (IS). Set of information resources organized for the collection, storage, processing, maintenance use, sharing, dissemination, disposition, display, or transmission of information" ([9], page 19).

"E2.1.45. Information Resources. Information and related resources, such as personnel, equipment, funds, and information technology" ([9], page 19).

Checkland & Holwell [4] distinguish information technology (IT) from information systems (IS). An information system consists of people organized to take "purposeful action" as well as IT in the form of supporting technology, such as the radar and telephones used to support the British during the Battle of Britain (see [4], Chapter 5). IA of IT becomes particularly meaningful when it is considered in support of a particular IS. Perhaps a future step in the evolution of IA in the DoD will consider this dichotomy.

E2.1.61, page 21).

Each IA Control is given an "Impact Code" of High, Moderate, or Low, that indicates the impact "associated with non-compliance or exploitation" ([9], E2.1.42, page 19) of the IA Control. The Impact Code can also indicate "urgency with which corrective action should be taken" (ibid.).

To bring home the importance of IA Controls in Interim-DIACAP, consider that "IA posture"[17] is defined relative to compliance with IA controls (i.e., certification) ([9], E4.3, page 39; see also "Notional DIACAP Scorecard," E4.A2, page 43) and that residual risk is defined as follows

> E2.1.60. Residual Risk. Risk due to partial or unsatisfactory implementation of assigned IA Controls. ([9], page 21)

implying that if the assigned IA Controls are correctly determined and those Controls are completely and satisfactorily implemented, then there will be no residual risk.

DIACAP requires periodically (1) checking the safeguards and regulations associated with a system's assigned IA Controls ("at least annually" ([9], 4.8, page 3) and (2) the subsequent development and execution of plans that will rectify the safeguards and/or regulations found lagging during the periodic check. In this way, DIACAP maintains IA.

The DIACAP Knowledge Service (KS) "provides the DoDI 8500.2 IA Controls as well as the required, standardized DoD IA Controls implementation procedures, validation procedures and expected results for each IA Control" ([9], 6, page 10). KS is "DoD's official resource for implementing and executing the DIACAP" ([9], E5.1, page 54).

4.4.1 Documentation

DIACAP documentation is a Package with five parts:

1. System Identification Profile (SIP),
2. Implementation Plan
3. Supporting Documentation for Certification
4. DIACAP Scorecard, and
5. POA&M[18] (if required). ([9], Table E4.1, page 38)

A Package is to be "maintained throughout a system's life cycle" ([9], E4.1, page 38). This should happen as a natural consequence of the required, periodic re-validation of IA Controls and the inevitable resulting POA&M and related Implementation Plan (see below).

The SIP consists of up to 34 parts, all but one of which could be called fields because they require no creativity to complete. The one field that does require some creativity is item 7,

---

17. "An unacceptable IA posture results when the IA Controls compliance posture does not match that authorized by the Accreditation Decision" ([9], E4.A3.6, page 47). (An Accreditation Decision is one of four possibilities: Authorization to Operate (ATO), Interim Authorization to Operate (IATT), Interim Authorization to Test (IATT), and Denial of Authorization to Operate (DATO) ([9], E2.1.2, page 13).)

18. POA&M = Plan of Action and Milestones.

"System Description," which is "A narrative description of the system, its function, and uses" ([9], page 40).[19]

The Implementation Plan consists of (a) the list of assigned IA Controls and (b) their implementation status, (c) identification of responsible entities (e.g., who is the DAA for this system?), (d) the resources available for this Plan, and (e) the estimated completion date for each IA Control.

The Supporting Documentation for Certification consists of (a) validation results, (b) implementation "artifacts,"[20] and (c) "other," which I presume is a catch-all.

The DIACAP Scorecard shows the system's IA posture which includes the accreditation status (i.e., ATO, IATO, IATT, or DATO) and a list, if needed, of recent IA Controls with which the system has been non-compliant and a POA&M for the current non-compliant IA Controls ([9], page 43).

The POA&M (i.e., Plan of Action and Milestones) is a "management tool" that describes the "corrective actions" that will bring (or return) a system to, I presume, the ATO state. In other words, the POA&M is an action plan based on audit findings. The CA assigns to each IA Control, about which correction action needs to be taken, a Severity Code of CAT I, CAT II, or CAT III, that specifies the risk level and/or urgency with which the corrective action is to be addressed, where CAT I indicates greatest risk and CAT III least risk.

The DIACAP Package in its entirety can be referred to as the Comprehensive Package to distinguish it from the Executive Package which includes neither the Implementation Plan nor the Supporting Documentation for Certification.

4.4.2 Roles

DIACAP defines nine roles, shown in Table 12.

A single person may adopt multiple roles simultaneously as specified by a set of constraints provided by Interim-DIACAP. These constraints are explored in Appendix C.1 beginning on page 57 herein.

Interim-DIACAP also provides constraints on who may report to whom. These reporting constraints are explored in Appendix C.2 beginning on page 60 herein.

---

19. The SIP includes a "Mission Criticality" item (#13) with three categories: Mission Critical (MC), Mission Essential (ME), and Mission Support (MS) ([9], page 40). Not only are these categories not defined, they are not used anywhere else in the document. I am told that these terms appeared in older documents. Based on their usage, these terms appear to correspond to MAC I, MAC II, and MAC III, respectively. One would think that Mission Criticality would be input to the system categorization, along with the three Mission Assurance Categories and the three Confidentiality Levels, to form a 3 x 3 x 3 matrix to determine the set of baseline IA controls. Perhaps this will occur in the future.

20. "E2.1.4. Artifacts. System policies, documentation, plans, test results and the like that express or enforce the IA posture of the DoD information system, make up the C&A information, and provide evidence of compliance with the assigned AI Controls" ([9], page 13).

Table 12 DIACAP Roles

Role		Description
Name	**Abbreviation**	
Program or System Manager	PM or SM	The names for this role are as though PM and SM were synonymous, e.g., "Program Manager (a.k.a. System Manager)" (or "System Manager (a.k.a. Program Manager)"). (I think the concept would be clearer if it were written "PM/SM" (or "SM/PM").)
Designated Accrediting Authority	DAA	"This term is synonymous with Designated Approving Authority and Delegated Accrediting Authority" ([9], E2.1.19, page 15).
Certifying Authority	CA	"The senior official having the authority and responsibility for the certification of information systems governed by a DoD Component IA Program" ([9], E2.1.11, page 14).
User Representative	UR	"Individual or organization that represents the user community in the DIACAP" ([9], E2.1.69, page 22).
Chief Information Officer	CIO	(There is no entry in the set of definitions for CIO, though there is an entry in the set of acronyms.)
Principal Accrediting Authority	PAA	"The senior official having the authority and responsibility for information systems within a GIG [Global Information Grid] Mission Area" ([9], E2.1.57, page 21).
Senior Information Assurance Officer	SIAO	"Official responsible for directing an organization's information assurance program on behalf of the organization's CIO" ([9], E.2.1.63, page 21).
Information Assurance Manager	IAM	IAM "…may be used interchangeably with the title Information System Security Manager (ISSM)" ([9], E2.1.38, page 18).
Information Assurance Officer	IAO	"The individual responsible to the IAM for ensuring that the appropriate operational IA posture is maintained for a DoD information system or organization." ([9], E2.1.29, page 18)

4.5 DIACAP vis-à-vis DITSCAP

This section describes the differences between DIACAP and DITSCAP, reflected in the differences in documentation, process, definitions (of accreditation, certification, validation, and verification), and roles.

4.5.1 Documentation

Whereas DITSCAP focuses on agreement between the four roles, DIACAP focuses on IA Controls. This difference is reflected in the differences between the SSAA and the DIACAP Package. Generally speaking DITSCAP's SSAA is a description and does not reflect a plan,[21] whereas DIACAP's Package is a plan and only briefly a description. The SSAA has no obvious section that describes the system's protections. The Implementation Plan of the Package, on the other hand, focuses on those protections. The SSAA has no obvious section, excepting Appendix H "CA's Recommendations," on how weaknesses are to be addressed. The POA&M part of the Package, on the other hand, has no other purpose.

4.5.2 Process

The DIACAP activities are essentially the same as the DITSCAP Phases, with the exception that the last DIACAP activity, Decommission, is new with DIACAP, as shown in Table 13.

Table 13 DITSCAP Phases & DIACAP Activities Compared

DITSCAP Phase	DIACAP Activity
Phase 1, Definition	1. Initiate and Plan C&A
Phase 2, Verification	2. Implement and Validate Assigned IA Controls
Phase 3, Validation	3. Make Certification Determination & Accreditation Decision
Phase 4, Post Accreditation	4. Maintain Authority to Operate and Conduct Reviews
(No corresponding Phase)	5. Decommission

However, what is different is the nature of the activities. DITSCAP requires that Phase n be completed before Phase n+1 begins[22]. DIACAP, on the other hand, allows activities[23] to be running in parallel and at different frequencies.

4.5.3 Definitions

DITSCAP and DIACAP define several key terms differently. Concerning "accreditation," DIACAP discards DITSCAP's use of "acceptable level" of risk, and DIACAP specifies accreditation to be one of four possibilities. Concerning "certification," DIACAP makes the purpose clearer, namely "to establish compliance with IA controls." Concerning "validation," DITSCAP focuses on agreement and DIACAP focuses on test results. DITSCAP validation applies only to "completed" systems. Concerning "verification," DIACAP has no need of a

21. Yes, Section 7 of the SSAA is entitled "DITSCAP Plan," but the only subsection of that Section that calls for action is 7.2 "Tasks and milestones." This is qualitatively different than DIACAP's "Implementation Plan" and POA&M. (Three of the SSAA Appendices, namely J, K, and M, have "plan" in their title, but none of these are concerned with how the system's protections are to be evaluated or brought up to adequacy.)

22. Figure E3-1 (5200.40, page 17) is a flowchart for all the activities in all of the DITSCAP Phases. All paths through the flowchart describe a sequential execution of nodes; no path initiates parallel execution.

23. except, of course, Decommission.

definition because DIACAP's "validation" applies to a system at any point in the life-cycle. The DITSCAP and DIACAP definitions are shown in Table 14.

Table 14 DITSCAP/DIACAP Definitions (Sheet 1 of 2)

Term	DITSCAP	DIACAP
Accreditation	E2.1.2. Accreditation. Formal declaration by the DAA that an IT system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. (5200.40, page 8)	E.2.1.2. Accreditation Decision. An official designation from a DAA, in writing or digitally signed and made visible to the DoD CIO, regarding acceptance of the risk associated with operating a DoD information system and expressed as an Authorization to Operate (ATO), an Interim Authorization to Operate (IATO), and Interim Authorization to Test (ATT), or a Denial of Authorization to Operate (DATO). ([9], page 13)
	1. DIACAP discards DITSCAP's use of "acceptable level" of risk. 2. DIACAP specifies the decision to be one of four possibilities.	
Certification	E2.1.8. Certification. Comprehensive evaluation of the technical and non-technical security features of an IT system and other safeguards, made in support of the accreditation process, to establish the extent that a particular design and implementation meets a set of specific security requirements. (5200.40, page 8)	E2.1.9. Certification. A comprehensive validation of actual IA capabilities and services of a DoD information system, made as part of and in support of the DIACAP, to establish compliance with assigned IA controls based on standardized procedures. ([9], page 13)
	DIACAP makes the purpose clearer, namely "to establish compliance with assigned IA controls."	
Validation	E2.1.64. Validation. Determination of the correct implementation in the *completed* IT system with the security requirements and approach agreed on by the users, acquisition authority, and the DAA. (5200.40, page 14, emphasis added)	E2.1.70. Validation Procedure. Activity applied throughout the system life cycle, to confirm or establish by testing, evaluation, examination, investigation, or competent evidence that a DoD information system's assigned IA Controls are implemented correctly and are effective in their application. ([9], page 22)
	1. DITSCAP focuses on agreement; DIACAP focuses on the results of interaction with the system throughout the life cycle. 2. DITSCAP's validation applies only to "completed" systems; DIACAP's validation makes no similar, explicit constraint.	

Table 14 DITSCAP/DIACAP Definitions (Sheet 2 of 2)

Term	DITSCAP	DIACAP
Verification	E2.1.65. Verification. The process of determining compliance of the evolving IT system specification, design, or code with the security requirements and approach agreed upon by the users, acquisition authority, and the DAA. (5200.40, page 14)	(No definition provided in Interim-DIACAP.)
	Because DITSCAP's "validation" applies only to "*completed*" systems, DITSCAP needs a definition for testing *incomplete* systems. DITSCAP's "verification" fulfils that need. DIACAP's "validation," on the other hand, applies at any point in the life-cycle. As a result, DIACAP has no need of a DITSCAP-type definition for "verification."	

4.5.4 Roles

DITSCAP uses four roles: PM, DAA, CA, UR. The DITSCAP documents define two additional roles:

- an Information System Security Officer (ISSO) (5200.40, E2.1.31, page 11; 8510.1-M, DL1.1.42, page 13) and
- a Configuration Manager (5200.40, E2.1.15, page 9; 8510.1-M, DL1.2.22, page 10).

but those roles are not directly involved in the SSAA.

DIACAP uses eight roles: PM or SM, DAA, CA, UR, CIO, PAA, SIAO, and IAM.

References

[1] BSI - Bundesamt fur Sicherheit in der Informatinostechnik, IT Baseline Protection Manual, PBSI 7152 E1. October 2003 version. 2,380 pages. http://www.bsi.bund.de/gshb.

[2] Philip L. Campbell, "An Introduction to Information Control Models." SAND2002-0131. 82 pages. Sandia National Laboratories. Albuquerque, New Mexico.

[3] Philip L. Campbell, "A CobiT® Primer." SAND2005-3455. 35 pages. Sandia National Laboratories. Albuquerque, New Mexico. Available on-line at www.itgi.org: click on "Introduction to CobiT."

[4] Peter Checkland, Sue Holwell, Information, Systems, and Information Systems. John Wiley & Sons. Chichester, England. 1998. ISBN 0-471-95820-4.

[5] COBIT: IT Governance Institute, CoBit 4.0: Control Objectives, Management Guidelines, Maturity Models. December 2005. ISBN 1-933284-37-4. 207 pages.

(The latest version is "COBIT 4.0." The previous edition was "COBIT Third Edition" which came out in 2000. The second and first editions came out in 1998 and 1996, respectively.)

[6] Common Criteria Implementation Board (CCIB) at NIST, Common Criteria for Information Technology Security Evaluation." August 1999. Version 2.1. 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.

[7] COSO: Committee of Sponsoring Organizations of the Treadway Commission (COSO), "Internal Control—Integrated Framework." 1992. Available at www.cpa2biz.com.

[8] DCID 6/3: "Director of Intelligence Directive 6/3 Protecting Sensitive Compartmented Information Within Information Systems." Manual. 99 pages.

[9] DIACAP: "Interim Department of Defense Certification and Accreditation (C&A) Process Guidance." "SUBJECT: DoD Information Assurance Certification and Accreditation Process (DIACAP)." July 6, 2006. 57 pages.

[10] FIPS 199: Federal Information Processing Standards (FIPS) 199: "Standards for Security Categorization of Federal Information and Information Systems." December 2003.

[11] FISMA: The Federal Information Security Management Act of 2002 ("FISMA", 44 U.S.C. § 3541, et seq.) enacted in 2002 as Title III of the E-Government Act of 2002 (Pub.L. 107-347, 116 Stat. 2899).

[12] IATF: "Information Assurance Technical Framework IATF)." National Security Agency, Release 3.1, September 2002, or latest release. http://www.iatf.net.

[13] ISO/IEC 15408, Information Technology—Security techniques—Evaluation criteria for IT security. Part 1: Introduction and general model. First edition 1999-12-01. 53 pages. Part 2: Security functional requirements. First edition 1999-12-01. 343 pages. Part 3: Security assurance requirements. First edition 1999-12-01. 213 pages.

[14] ISO/IEC 17799:2005, "Information Technology—Code of Practice for Information Security Management." www.iso.org.

[15] IT Governance Institute, Audit Guidelines. July 2000. 226 pages.

Note: This document was written for COBIT 3rd Edition. This document is being updated for COBIT 4.0 and will be named IT Assurance Guide using COBIT. The current document supports "one generic audit process of control evaluation, compliance testing and substantiating risk" [17]. The updated document will provide support for "additional assurance techniques;" it will provide "more guidance" and will refer to the "full range of COBIT components."

[16] IT Governance Institute, Control Practices. 2004. 223 pages.

Note: This document was written for COBIT 3rd Edition and has not yet be updated for COBIT 4.0.

[17] Gary Hardy, Erik Guldentops, "COBIT 4.0: The New Face of COBIT." Information Systems Control Journal, Volume 6, 2005, pages 35-8.

[18] Charles LeGrand et al., "Global Technology Audit Guide (GTAG), Guide 1: Information Technology Controls." The Institute of Internal Auditors. 76 pages. Available at www.theiaa.org.

[19] Leslie Ann Macartney, "Information Security Harmonisation: Classification of Global Guidance." IT Governance Institute. 2005. ISBN 1-933284-05-6. 150 pages. Available at www.itgi.org.

[20] Mark W. Maier, Eberhardt Rechtin, The Art of Systems Architecting. Second Edition. CRC Press. Boca Raton, Florida. 2002.

[21] Jimmy Heschl, "COBIT Mapping: Overview of International IT Guidance, 2nd Edition." IT Governance Institute. 2006. 75 pages.

[22] National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, National Policy Governing the Acquisition of Information Assurance (IA) and IA-enabled Information Technology Products. January 2000.

[23] NIST, Common Criteria version 2: An Introduction. 10/98. 19 pages. http://csrc.nist.gov/cc/info/infolist.htm.

[24] NIST 800-37: Ron Ross, Marianne Swanson, Gary Stoneburner, Stu Katzke, Arnold Johnson, "Guide for the Security Certification and Accreditation of Federal Information Systems." NIST Special Publication 800-37. May 2004. 64 pages.

[25] NIST 800-53: Ron Ross, Stu Katzke, Arnold Johnson, Marianne Swanson, Gary Stoneburner, George Rogers, Annabelle Lee, "Recommended Security Controls for Federal Information Systems." NIST Special Publication 800-53. February 2005. 116 pages.

[26] NIST 800-60: William C. Barker, "Guide for Mapping Types of Information and Information Systems to Security Categories." NIST Special Publication 800-60. June 2004.

Volume 1: Guide for Mapping Types of Information and Information Systems to security Categories. William C. Barker. 45 pages.

Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to security Categories. William C. Barker, Annabelle Lee. 295 pages.

This page intentionally almost blank.

Appendix A DITSCAP Phases, Activities, and Tasks, Based on 8510.1-M

Both 5200.40 and 8510.1-M describe Phases, Activities, and Tasks for DITSCAP. (Neither 8500.1 nor 8500.2 discuss Phases, Activities, or Tasks.) However, the descriptions in the two documents differ (see Appendix B). Because 8510.1-M provides more depth in its description, I presume that it is the more authoritative source. Accordingly, Table 15 below shows the 4 Phases, the 13 Activities, and the 35 Tasks in DITSCAP, as presented in 8510.1-M.

The Tasks, as described in 8510.1-M, are tightly associated with a Phase but only loosely associated with an Activity: the number of each Task, e.g., "Task 1-2" (which is the second Task in the first Phase), includes a Phase number but no reference to an Activity number.[24] As a consequence, the Activities for each Phase are listed in Table 15 independently of the Tasks.

The page number for the start of each item is included in the Table as a rough indication of the space consumed in the description—by subtracting that number from the number for the subsequent Task. Most of the items take up only a page or two, but exceptions are notable. For example, Task 1-8 uses eight pages: that item describes the systems classification scheme.

24. If the Tasks were tightly associated with an Activity, then I would expect to see three integers in the number of each Task, e.g., "Task 1-2-3" (which would be the third Task in the second Activity in the first Phase).

Table 15 DITSCAP Phases, Activities, and Tasks[a] (Sheet 1 of 2)

Phases (& Activities)	Tasks
Phase 1. Definition (page 32) Activities: Preparation (page 35) Registration (page 36) Negotiation (page 38)	Task 1-1. Review documentation (page 39) Task 1-2. Prepare the system and functional description and system identification (page 39) Task 1-3. Register the system (page 42) Task 1-4. Prepare the environment and threat description (page 43) Task 1-5. Determine the system security requirements (page 46) Task 1-6. Prepare the system architecture description (page 50) Task 1-7. Identify the C&A organizations and the resources required (page 51) Task 1-8. Tailor the DITSCAP and prepare the DITSCAP plan (page 52) Task 1-9. Draft the SSAA (page 60) Task 1-10. Conduct certification requirements review (page 61) Task 1-11. Establish agreement on level of effort and schedule (page 61) Task 1-12. Approve Phase 1 SSAA (page 61)
Phase 2. Verification (page 65) Activities: SSA refinement (page 66) System development and integration (page 66) Initial certification analysis (page 66) Assess analysis results (page 67)	Task 2-1. System architecture analysis (page 68) Task 2-2. Software, hardware, and firmware design analysis (page 70) Task 2-3. Network connection rule compliance analysis (page 74) Task 2-4. Integrity analysis of integrated products (page 77) Task 2-5. Life-cycle management analysis (page 79) Task 2-6. Security requirements validation procedures (page 82) Task 2-7. Vulnerability assessment (page 84)

Table 15 DITSCAP Phases, Activities, and Tasks[a] (Sheet 2 of 2)

Phases (& Activities)	Tasks
Phase 3. Validation (page 90) Activities: SSAA refinement (page 91) Certification evaluation of the integrated system (page 91) Recommendation to DAA (page 92) DAA accreditation decision (page 93)	Task 3-1. Security test and evaluation (ST&E) (page 94) Task 3-2. Penetration testing (page 97) Task 3-3. TEMPEST and RED-BLACK verification (page 99) Task 3-4. COMSEC compliance verification (page 101) Task 3-5. System management analysis (page 103) Task 3-6. Site accreditation survey (page 105) Task 3-7. Contingency plan evaluation (page 107) Task 3-8. Risk management review (page 108)
Phase 4. Post Accreditation (page 112) Activities: System and security operation (page 113) Compliance validation (page 114)	Task 4-1. SSAA maintenance (page 115) Task 4-2. Physical, personnel, and management control review (page 116) Task 4-3. TEMPEST evaluation (page 117) Task 4-4. COMSEC compliance evaluation (page 119) Task 4-5. Contingency plan maintenance (page 120) Task 4-6. Configuration management (page 121) Task 4-7. Risk management review (page 123) Task 4-8. Compliance validation (page 126)

a. This list is based on the material in 8510.1-M.

This page intentionally almost blank.

Appendix B DITSCAP Discrepancies

5200.40 and 8510.1-M differ materially in at least two respects—the list of DITSCAP Tasks and the SSAA outline. Each of these is presented in a separate section below. Note that 8510.1-M precedes 5200.40 in typical usage (see Section 2.3 on page 20).

B.1 Tasks

There are two lists of DITSCAP Tasks in 5200.40, and there are two lists of DITSCAP Tasks in 8510.1-M. No two of the four lists agree. (Neither 8500.1 nor 8500.2 discuss Phases, Activities, or Tasks.)

Within 5200.40, of the eight Figures in Enclosure 3 that list Tasks, three of those Figures—namely E3-4, E3-11, and E3-16—do not match the list of Tasks in Table 8-1 (pages 67-8), as shown in Table 16 below.

Table 16 5200.40 Discrepancies

Discrepancy	Document Body	Table 8-1 (pages 67-8)
Different Wording	Task 4 in E3-4 (page 20), "Prepare the system architecture description and C&A boundary."	"Prepare the system architecture description."
	Task 7 in E3-4 (page 20), "Identify organizations that will be involved in the C&A and identify resources required."	"Identify organizations that will support the C&A."
Task Missing	Task 6 in Figure E3-11 (page 33), "Site accreditation survey."	(There is no corresponding Task in Table 8-1.)
	Task 5 in Figure E3-16 (page 40), "Compliance reverification."	(There is no corresponding Task in Table 8-1.)
Different Order	Task 1 in Figure E3-16 (page 40), "Physical security analysis." Task 2 in Figure E3-16 (page 40), "Review the SSAA."	"Review the SSAA." "Physical security analysis."
	Task 3 in Figure E3-16 (page 40), "Risk-based management review." Task 4 in Figure E3-16 (page 40), "Procedural analysis."	"Procedural analysis." "Risk-based management review."

In 8510.1-M, the Tasks in three of the four Tables in Chapters 3, 4, 5, and 6 do not match the list

of Tasks in the bodies of those Chapters, as shown in Table 17 below.

Table 17 8510.1-M Discrepancies

Discrepancy	Table	Chapter Body
Different Wording	Task 4 in C3.T3 (page 36), "Prepare the system architecture description and describe the C&A boundary."	Task 1-6 (page 50), "Prepare the system architecture description." Task 1-6 mentions describing the "accreditation boundary" (see C3.4.6.2.6).
	Task 2 in C4.T1 (page 67), "Software design analysis."	Task 2-2 (page 70), "Software, hardware, and firmware design analysis."
	Task 6 in C4.T1 (page 67), "Security requirements validation procedures preparation."	Task 2-6 (page 82), "Security requirements validation procedures."
Task Missing	A corresponding Task does not appear in Table C3.T3 (page 36).	Task 1-1 (page 39), "Review documentation."
	Task 7 in C6.T1 (page 114), "OSystem [sic] Security Management."	A corresponding Task does not appear in pages 121-3, where the Task would appear if it were present in the Chapter body.
Different Order	Task 4 in Table C3.T3 (page 36), "Prepare system architecture description and describe the C&A boundary." Task 5 in Table C3.T3 (page 36): "Determine the system security requirements."	Task 1-5 (page 46), "Determine the system security requirements." Task 1-6 (page 50), "Prepare the system architecture description."
	Task 6 in C3.T3 (page 36), "Tailor the DITSCAP tasks, determine the C&A level of effort, and prepare a DITSCAP plan." Task 7 in C3.T3 (page 36), "Identify organizations that will be involved in the C&A and identify resources required."	Task 1-7 (page 51), "Identify the C&A organizations and the resources required." Task 1-8 (page 52), "Tailor the DITSCAP and prepare the DITSCAP plan."
Different Description	Task 2 in C3.T4 (page 38), "Agree on the security requirements, level of effort, and schedule."	Task 1-11 (page 61), "Establish Agreement on Level of Effort and Schedule." Task 1-11 does not mention "security requirements."
Subsumption	The six Tasks in C6.T2 (page 114)—the title for the Table is "Compliance Validation Tasks"—are subsumed by Task 4-8 (page 126), "Compliance validation," in the Chapter body. (Table C6.T2 is repeated as Table C6.T5 (page 127), within the description of Task 4-8.)	

B.2 SSAA Outline

An outline for the SSAA is presented in both 5200.40 (pages 51-5) and in 8510.1-M (pages 142-5). The two outlines differ. In general, the outline in 8510.1-M is a simplification of the outline in 5200.40.

The SSAA outline in 8510.1-M drops

1. the Hardware, Firmware, and Software sub-sections[25] and the "TAFIM DGSA" sub-section in Section 3 "SYSTEM ARCHITECTURE DESCRIPTION,"
2. all of Section 4 "ITSEC SYSTEM CLASS,"
3. sub-sections under Section 5.5 "Network connection rules," under Section 6.1. "Identification of organizations," and under Section 6.2 "Resources," and
4. Section 6.4 "Roles and responsibilities," and
5. Section 7.1.5 "Tailoring summary."

The SSAA outline in 8510.1-M adds

1. eight sub-sections under Section 2.1 "Operating environment," and
2. Section 3.1 "System Architecture Description."

Of the 16 appendices in 5200.40, nine (Appendices B, C, D, E, I, J, L, M, and N) have the same name in 8510.-1M and three more (Appendices A, K, and O) have almost the same name in 8510.1-M. The remaining four appendices

- APPENDIX F. Certification results
- APPENDIX G. Risk assessment results
- APPENDIX H. CA's recommendation
- APPENDIX P. Accreditation documentation and accreditation statement

do not easily match appendices in 8510.1-M. The candidates from 8510.1-M are the following:

- Appendix P Test and Evaluation Report(s)
- Appendix Q Residual Risk Assessment Results
- Appendix R Certification and Accreditation Statement

The matching that makes sense to me is shown in Table 18. Note that Appendix R is matched in

25. I understand that these sub-sections—3.1, 3.2, and 3.3—should appear in an SSAA, even though 8510.1-M dropped them.

Table 18 to both APPENDIX H and APPENDIX P.

Table 18 Matching Appendices

5200.40	8510.1-M
APPENDIX F. Certification results	Appendix P Test and Evaluation Report(s)
APPENDIX G. Risk assessment results	Appendix Q Residual Risk Assessment Results
APPENDIX H. CA's recommendation	Appendix R Certification and Accreditation Statement
APPENDIX P. Accreditation documentation and accreditation statement	

8510.1-M adds two appendices:

- Appendix D System Concept of Operations
- Appendix E Information System Security Policy

Note that

- Appendix G Certification Test and Evaluation Plan and Procedures (Type only)

is for "type" accreditation, as opposed to "site" (for co-located systems) and "system" (for a single system).

The details of the differences are shown in Table 19.

Table 19 SSAA Outlines in 5200.40 & 8510.1-M (Sheet 1 of 4)[a]

5200.40	8510.1-M
1. MISSION DESCRIPTION AND SYSTEM IDENTIFICATION	
1.1. System name and description.	
1.2. System description.	
1.3. Functional description.	
1.3.1. System capabilities.	
1.3.2. System criticality.	
1.3.3. Classification and sensitivity of data processed.	
1.3.4. System user description and clearance levels.	
1.3.5. Life-cycle of the system.	
1.4. System CONOPS summary.	
2. ENVIRONMENT DESCRIPTION	
2.1. Operating environment.	
	2.1.1. Facility Description
	2.1.2. Physical Security

Table 19 SSAA Outlines in 5200.40 & 8510.1-M (Sheet 2 of 4)[a]

5200.40	8510.1-M
	2.1.3. Administrative Issues
	2.1.4. Personnel
	2.1.5. COMSEC
	2.1.6. TEMPEST
	2.1.7. Maintenance Procedures
	2.1.8. Training Plans
2.2. Software development and maintenance environment.	
2.3. Threat description.	
3. SYSTEM ARCHITECTURAL DESCRIPTION	
3.1 Hardware.	
3.2 Software.	
3.3 Firmware.	
	3.1 System Architecture Description
3.4. System interfaces and external connections.	
3.5. Data flow (including data flow diagrams).[b]	
3.6. TAFIM DGSA, (reference (m)), security view.	
3.7. Accreditation boundary.	
4. ITSEC SYSTEM CLASS	
4.1. Interfacing mode.	
4.2 Processing mode.	
4.3 Attribution mode.	
4.4. Mission-reliance factor.	
4.5. Accessibility factor.	
4.6. Accuracy factor.	
4.7. Information categories.	
4.8. System class level.	
4.9. Certification analysis level.	
5. SYSTEM SECURITY REQUIREMENTS	
5.1. National and DoD security requirements.	
5.2. Governing security requisites.	
5.3. Data security requirements.	
5.4. Security CONOPS.	

Table 19 SSAA Outlines in 5200.40 & 8510.1-M (Sheet 3 of 4)[a]

5200.40	8510.1-M
5.5. Network connection rules.	
5.5.1. To connect to this system.	
5.5.2. To connect to the other systems defined in the CONOPS.	
5.6. Configuration and change management requirements.[c]	
5.7. Reaccreditation requirements.	
6. ORGANIZATIONS AND RESOURCES	
6.1. Identification of organizations[d]	
6.1.1. DAA.	
6.1.2. CA.	
6.1.3. Identification of the user representative.	
6.1.4. Identification of the organization responsible for the system.	
6.1.5. Identification of the program manager or system manager.	
6.2. Resources.	
6.2.1. Staffing requirements.	
6.2.2. Funding requirements.	
6.3. Training for certification team.[e]	
6.4. Roles and responsibilities.	
6.5. Other supporting organizations or working groups.[f]	
7. DITSCAP PLAN	
7.1. Tailoring factors.	
7.1.1. Programmatic considerations.	
7.1.2. Security environment.	
7.1.3. IT system characteristics.[g]	
7.1.4. Reuse of previously approved solutions.	
7.1.5. Tailoring summary.	
7.2. Tasks and milestones.	
7.3. Schedule summary.	
7.4. Level of effort.	
7.5. Roles and responsibilities.	

Table 19 SSAA Outlines in 5200.40 & 8510.1-M (Sheet 4 of 4)[a]

5200.40	8510.1-M
Note: The appendices in the 5200.40 column are listed below in the order of their appearance in the 5200.40 outline, and the appendices in 8510.1-M that match the Appendices in 5200.40 have been moved to highlight that matching, so the appendices in 8510.1-M do not appear in alphabetical order. Note that Appendix R appears twice, across from both APPENDIX H and APPENDIX P. Note also that appendices in 8510.1-M that do not appear to match any appendix in 5200.40, such as Appendix D, are shown across from a grayed cell.	
APPENDIX A. Acronym list	Appendix A Acronyms
APPENDIX B. Definitions	Appendix B Definitions
APPENDIX C. References	Appendix C References
APPENDIX D. Security requirements and/or requirements traceability matrix	Appendix F Security Requirements and/or Requirements Traceability Matrix
	Appendix D System Concept of Operations
APPENDIX E. Security test and evaluation plan and procedures	Appendix H Security Test and Evaluation Plan and Procedures
	Appendix E Information System Security Policy
APPENDIX F. Certification results	Appendix P Test and Evaluation Report(s)
APPENDIX G. Risk assessment results	Appendix Q Residual Risk Assessment Results
	Appendix G Certification Test and Evaluation Plan and Procedures (Type only)
APPENDIX H. CA's recommendation	Appendix R Certification and Accreditation Statement
APPENDIX I. System rules of behavior	Appendix J System Rules of Behavior
APPENDIX J. Contingency plan(s)	Appendix L Contingency Plans
APPENDIX K. Security awareness and training plan	Appendix O Security Education, Training, and Awareness Plan
APPENDIX L. Personnel controls and technical security controls	Appendix M Personnel Controls and Technical Security Controls
APPENDIX M. Incident response plan	Appendix K Incident Response Plan
APPENDIX N. Memorandums of agreement — system interconnect agreements	Appendix N Memorandums of Agreement — System Interconnect Agreements
APPENDIX O. Application system development artifacts or system documentation	Appendix I Applicable System Development Artifacts or System Documentation
APPENDIX P. Accreditation documentation and accreditation statement	Appendix R Certification and Accreditation Statement

a. This table uses the section numbering of 5200.40. So, for example, Section 3.4. "System interfaces and external connections" of 5200.40 matches Section 3.2 of 8510.1-M. Differing section names are noted in footnotes.

b. The name for this section in 8510.1-M is simply “Data Flow.”

c. The name for this section in 8510.1-M is simply “Configuration Management Requirements.”

d. The name for this section in 8510.1-M is simply “Organizations.”

e. The name for this section in 8510.1-M is simply “Training.”

f. The name for this section in 8510.1-M is simply “Other Supporting Organizations.”

g. The name for this section in 8510.1-M is “IS Characteristics.”

Appendix C DIACAP Role Fusion and Reporting Constraints

The purpose of this Appendix is to point out the gaps in a particular area in DIACAP. However, those explicit gaps may be trivial for several reasons. (1) The gaps might already be filled by organizational structure not spelled out in DIACAP. (2) There may be plans to fill the gaps prior to DIACAP being signed. (3) The gaps might be "don't cares" and either the footnote to this effect has not yet been inserted or I have overlooked it.

This Appendix presents the constraints on two aspects of the eight roles defined in DIACAP (see Section 4.4.2 on page 36). First, it is permissible for a single person for certain roles for a single information system to play more than one of these roles simultaneously. I call this "role fusion," for lack of a better term. Second, certain roles may or may not be allowed to report to certain other roles. The constraints for these two aspects are expressed in a single table ([9], Table E3.1, page 32). Unfortunately neither set of constraints, as expressed in that one table, is sufficient, so many questions are left unanswered. Perhaps this will be rectified in a future version of Interim-DIACAP.

In this Appendix, the constraints on role fusion are presented first, followed by the constraints on reporting.

This information is relegated to an Appendix because I do not think it is necessary for an understanding of DIACAP. In addition, the material is confusing.

C.1 Role Fusion Constraints

DIACAP defines nine roles. Of the 36 role-pairs, role fusion constraints are provided for only 6, as shown in Table 20.

Table 20 Role Constraints (Given)

Constraint Number[a]	Constraint
3	CIO may be DAA
4	DAA may be CA
6	PAA may be DAA
8	PM/SM may *not* be CA
9	PM/SM may *not* be DAA
10	PM/SM may *not* be UR

a. The integer in this column is the number of the corresponding row in Table E3.1 ([9], page 32).

Table 21 shows the constraints from Table 20 in the context of possible constraints.

Table 21 Role Constraints[a] (Exhaustive)

	PM/ SM	DAA	CA	UR	CIO	PAA	SAIO	IAM	IAO
PM/SM		No (9)	No (8)	No (10)					
DAA			Yes (4)		Yes (3)	Yes (6)			
CA									
UR									
CIO									
PAA									
SAIO									
IAM[b]									
IAO[c]									

a. Cell [i,j] addresses the following question: "May the role in row i and the role in column j be played by the same person?"

It is not clear what the default is (i.e., if the cell is blank).

The parenthesized integers in various cells in this table refer to the constraint numbers shown in Table 20.

b. Previously known as ISSM.

c. Previously known as ISSO.

The role constraints are shown diagrammatically in Figure 4.

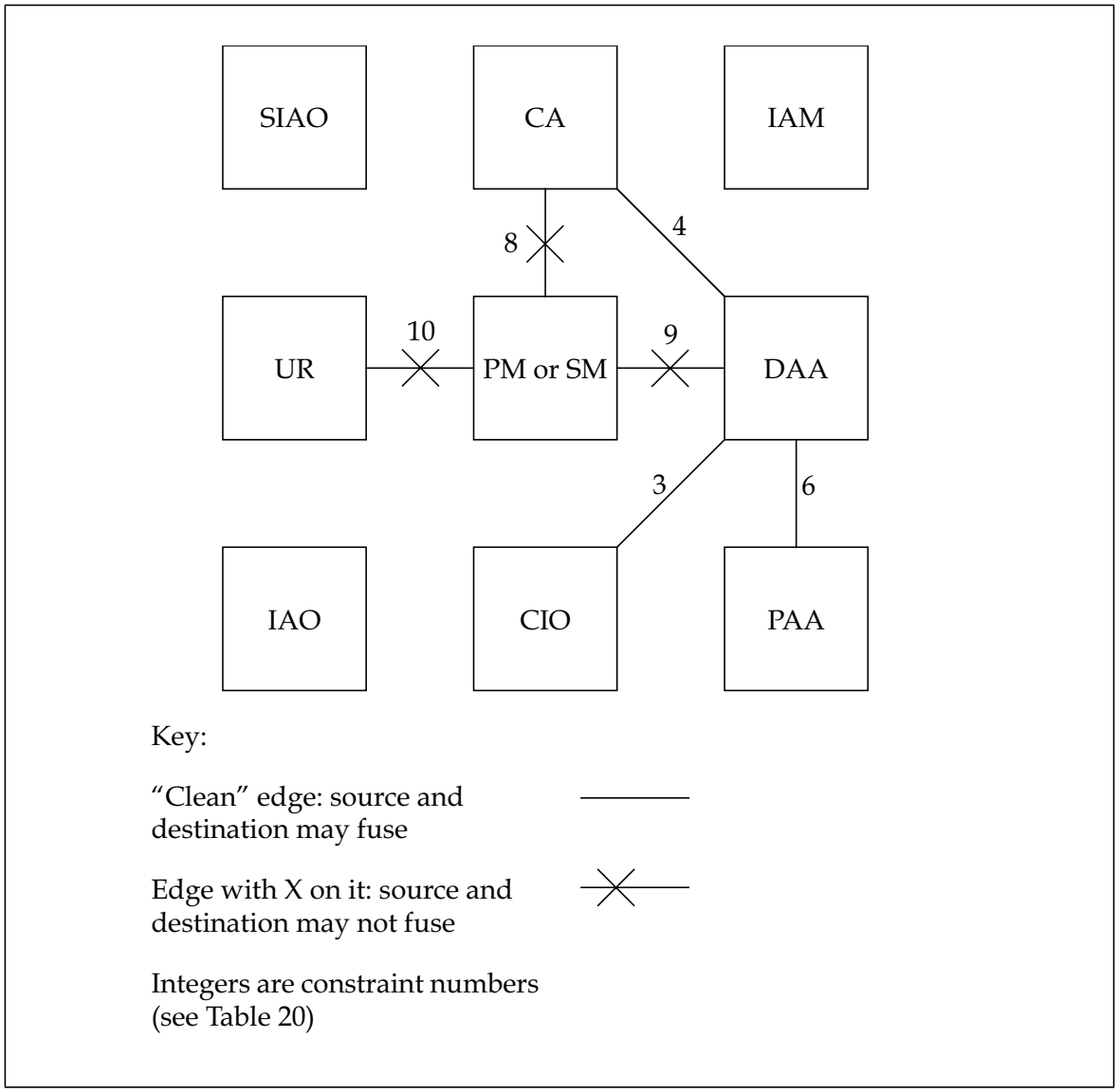

Figure 4 Role Constraints

The role fusion constraints leave many questions unanswered. For example, the constraints tell us nothing about SAIO, IAM, and IAO. In addition, is it true that one person could play the four roles of CA, DAA, CIO, and PAA? One hint about this is the definition of "DIACAP Team" as consisting of seven "officials" at a minimum: DAA, CA, SIAO, PM or SM, IAM, UR, and IAO ([9], E.2.1.24, page 15). If an "official" is a person and not a role, then this would imply that the DAA and CA roles, at least, cannot fuse. Which is it?

We can glean a little light on this matter from Section 5 "Responsibilities" of Interim-DIACAP. This section informs us that (1) the SIAO functions as the CA for all systems governed by that SAIO ([9], 5.13.4.1, page 8), (2) the CIO appoints the SAIO ([9], 5.12.1, page 7), and (3) the IAM

supports the PM or SM ([9], 5.17.1, page 10).

C.2 Reporting Constraints

Of the 36 reporting-pairs, reporting constraints are provided for only 10, as shown in Table 22.

Table 22 Reporting Constraints (Given)

Constraint Number[a]	Constraint	Comments
1	CA reports to DAA	(See Constraints 7a and 7b.)
2	CA does *not* report to PM/SM	
5	DAA does *not* report to PM/SM	
7a	PM/SM reports to DAA	Constraint 7 reads "PM or SM and CA both report to the DAA." This Constraint duplicates Constraints 1 and 13.
7b	CA reports to DAA	
11	PM/SM does *not* report to CA	
12	PM/SM reports to CIO	
13	PM/SM reports to DAA	(See Constraints 7a and 7b.)
14	UR reports to CIO	
15	UR does *not* report to PM/SM	
16a	UR reports to SIAO	Constraint 16 reads "User Representative reports to the SIAO/CA."
16b	UR reports to CA	

a. The integer in this column is the number of the corresponding row in Table E3.1 ([9], page 32).

Table 23 shows the constraints from Table 22 in the context of possible constraints.

Table 23 Reporting Constraints[a] (Exhaustive)

	PM/ SM	DAA	CA	UR	CIO	PAA	SAIO	IAM	IAO
PM/SM		Yes (7a, 13)	No (11)		Yes (12)				
DAA	No (5)								
CA	No (2)	Yes (1, 7b)			Yes (7a, 13)				
UR	No (15)		Yes (16b)		Yes (14)		Yes (16a)		
CIO									
PAA									
SAIO									
IAM									
IAO									

a. Cell [i,j] addresses the following question: "May the role in row i report to the role in column j?" It is not clear what the default is (i.e., if the cell is blank).

The parenthesized integers in various cells in this table refer to the constraint numbers shown in Table 20.

The reporting constraints are shown diagrammatically in Figure 5.

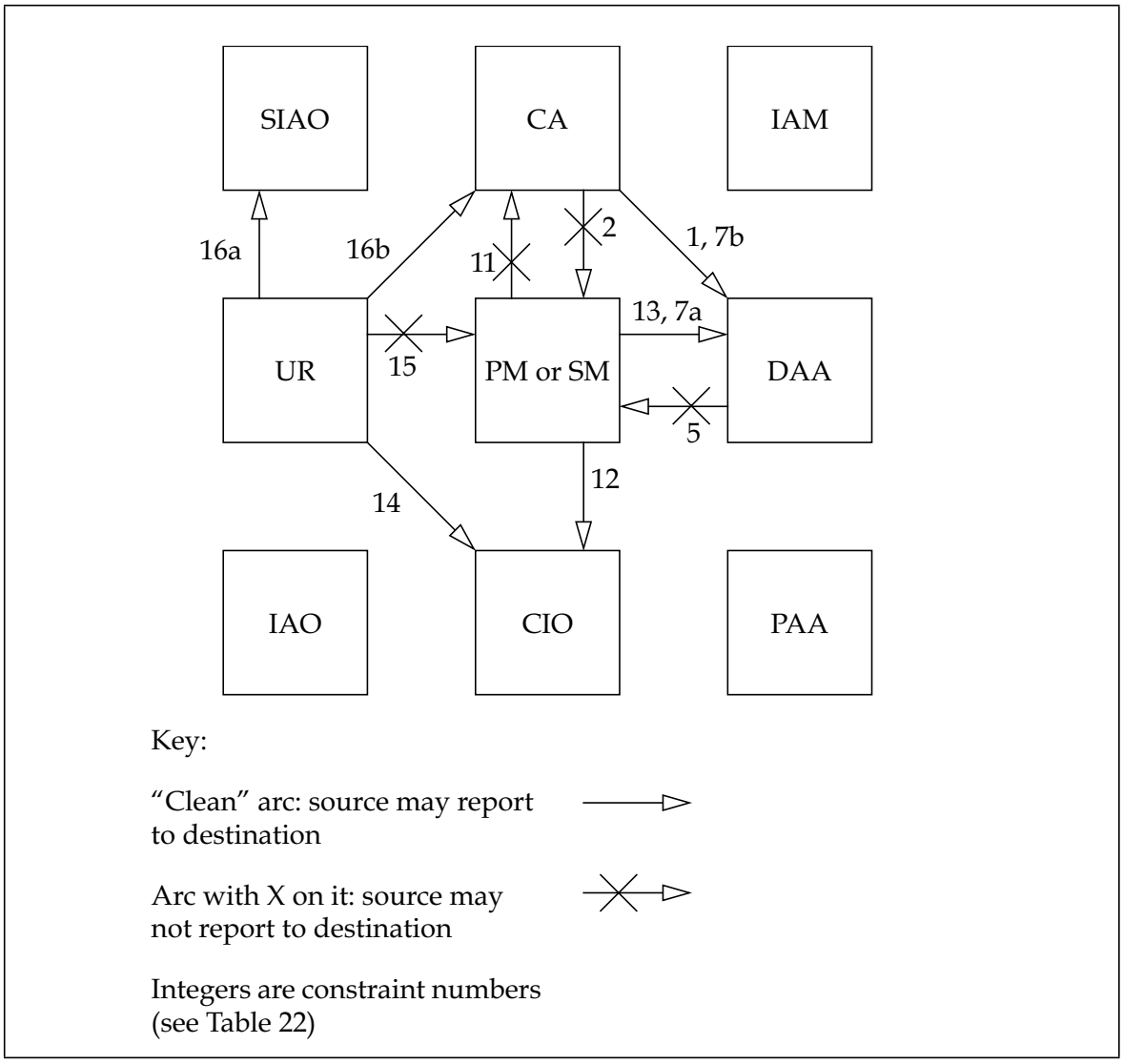

Figure 5 Reporting Constraints

As with the role fusion constraints, the reporting constraints leave many questions unanswered. For example, the constraints tell us nothing about reporting with respect to the IAM and PAA. In addition, there is confusion between the role fusion constraints and the reporting constraints. The role fusion constraints presented in Appendix C.1 suggest that the CA and DAA may be the same person, but the reporting constraints do not allow PM/SM to report to CA while they do allow PM/SM to report to DAA. If for a given information system the CA and the DAA are the same person, may PM/SM report to this person or not? or is the same person not allowed to assume both the CA and DAA roles?

Appendix D Common Terms

Based on the assumption that the terms defined in a document suggest the focus of the document, I selected 25 terms that appeared relevant and noted the documents that defined those terms.[26] Surprisingly, a definition for only one of my selected terms appears in all five documents: DAA.

The number of shared terms for each of the 10 document pairs is shown in Table 24.

Table 24 Terms Shared by Document Pairs

Document Pairs		Shared Terms	Comments
5200.40	8510.1-M	14	Greatest number of shared terms.
	8500.1	5	
	8500.2	1	Least number of shared terms.
	Interim-DIACAP	6	
8510.1-M	8500.1	6	
	8500.2	2	
	Interim-DIACAP	6	
8500.1	8500.2	5	
	Interim-DIACAP	4	
8500.2	Interim-DIACAP	5	

26. 5200.40 defines 67 terms;
8510.1-M defines 85 terms;
8500.1 defines 43 definitions;
8500.2 defines 55 terms; and
Interim-DIACAP defines 74 terms.

The number of shared terms is shown diagrammatically in Figure 6.

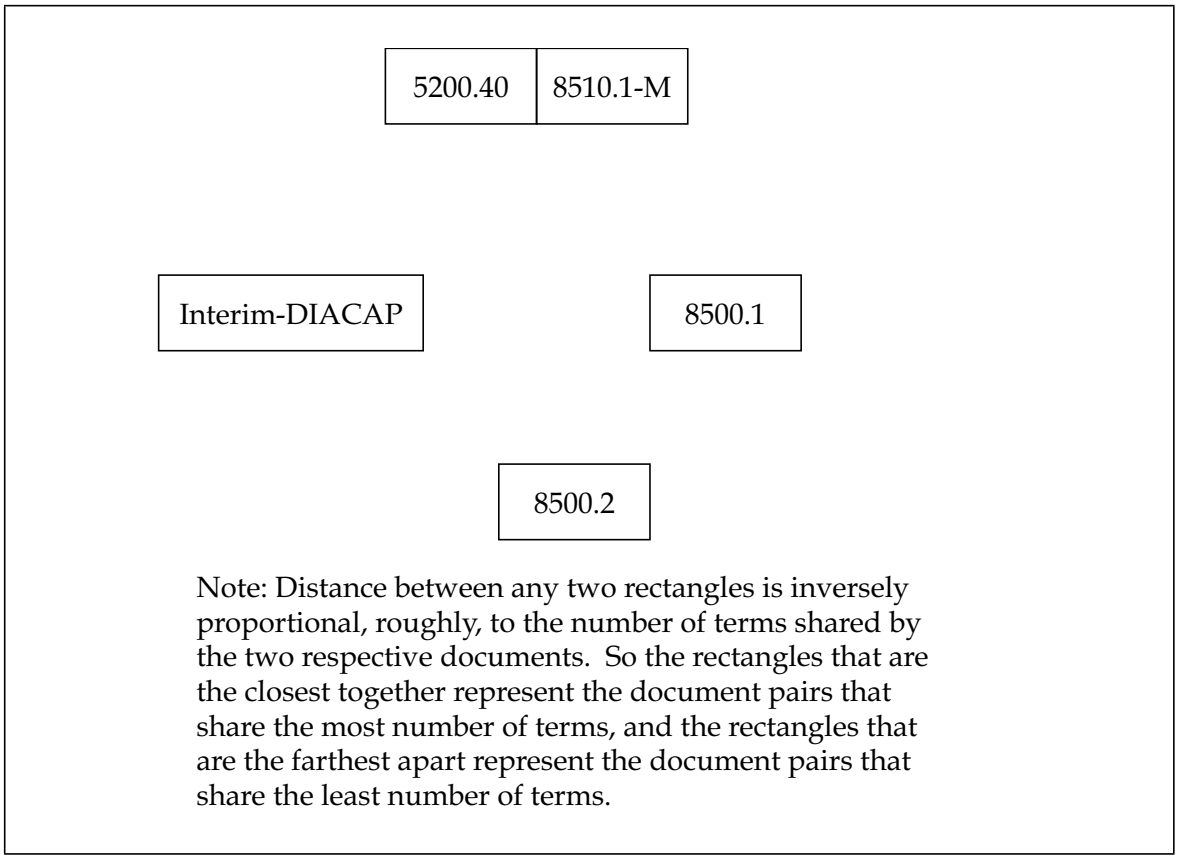

Figure 6 Term Sharing

There are three points that arise from Table 24 and Figure 6:

1. 5200.40 and 8510.1-M share the most number of terms—12—which is twice that shared by any other document pair.
2. The number of terms that 8500.1 and that Interim-DIACAP individually share with other documents varies the least of the documents.
3. The number of terms that 8500.2 shares varies the most of the documents.

One way to view Figure 6 is that 5200.40 and 8510.1-M present a cohesive story, that 8500.1 diverges from story, that 8500.2 diverges from even more, but Interim-DIACAP coalesces the story.

The presence/absence of a definition in the five documents for the terms I selected is shown in Table 25.

Table 25 Shared Terms

Term	Does the Definition appear in this Document?				
	5200.40	**8510.1-M**	**8500.1**	**8500.2**	**Interim-DIACAP**
Terms defined in all five documents					
Designated Approving Authority (DAA)	Yes				
Terms defined in any four documents					
Information Assurance (IA)	No	Yes			
Terms defined in any three documents:					
Integrity	Yes		Yes	No	
Authenticity (or Authentication)					
Availability					
Confidentiality					
Certification			No		Yes
Accreditation[a]					
Certification Authority (CA)[b]					
Program Manager					
IA Control	No		Yes		
Mission Assurance Categories					
Terms defined in any two documents:					
Accountability[c]	Yes		No		
Assurance					
DITSCAP					
System Security Authorization Agreement (SSAA)					
Verification (or Verification Phase)					
Validation	Yes	No			Yes
Robustness	No		Yes		No
Confidentiality Level			No	Yes	
Terms defined in any one document:					
Non-Repudiation	No		Yes	No	
Safeguard	No			Yes	No
Common Criteria					
Impact Code				No	Yes
Severity Code					

a. or Accreditation Decision.

b. or Certifying Authority.

c. i.e., Authentication and Non-Repudiation.

This page intentionally almost blank.

Appendix E Additional Documents

In order to provide context for the five documents reviewed in this report, this Appendix summarizes three additional, related documents:

1. DCID 6/3 [8],
2. NIST 800-37 [24], and
3. COBIT® [5].

The "process," "systems classification," and "measurement standard" for each of these additional documents is summarized in Table 26.

Table 26 Additional Documents

	DCID 6/3	NIST 800-37	COBIT
Process	11 steps	4 phases with 10 tasks and 31 subtasks	(None is provided.)
Systems Classification	5 "Protection Levels"	12 categories from FIPS 199 [10]	
Measurement Standard	80 "security features and assurances," organized into 36 areas	Controls from NIST 800-53 [25]	215 "control objectives"

Summaries of additional relevant documents can be found elsewhere ([2], [18], [19]).

E.1 DCID 6/3

DCID 6/3 provides "uniform policy guidance and requirements for ensuring adequate protection of certain categories of intelligence information [namely]…Sensitive Compartmented Information and special access programs for intelligence under the purview of the DCI[27]" ([8], 1.A.1, pages 3-4).

DCID 6/3 defines "information assurance" more aggressively than the other documents reviewed in this report:

> **Information Assurance**: Information Operations[28] that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.[29] This includes providing restoration of information systems

27. DCI = Director of Central Intelligence.

28. "Information Operations" is defined in turn as "Action taken to affect adversary information and information systems while defending one's own information and information systems" ([8], Appendix B).

29. DCID 6/3 presumes such things as "utility, user accountability, authenticity, possession, currency and non-repudiation" to be "some function" of confidentiality, integrity, and availability ([8], 1.H.3, page 6), thus providing the latter three provides the former six.

by incorporating protection, detection, and reaction capabilities. ([8], Appendix B)

E.1.1 Process for DCID 6/3

The DCID 6/3 way to "accredit an IS"[30] ([8], 1.F, page 5) is to use the following 11 steps:

1. Determine Levels-of-Concern [see Appendix E.1.2.1];
2. Determine Protection Level [see Appendix E.1.2.2];
3. Determine Interconnected System Requirements [this is needed if a system is to connect to another certified system, say, or it is a Web or file server, or it handles mobile code, or it engages in "collaborative computing"[31]] and Administrative Requirements [these are requirements for training, document marking, physical security, personnel security, etc.];
4. Identify Technical Security and Assurance Requirements [i.e., determine what controls apply];
5. Determine Required Documentation and Testing Activities [this is a function of the required controls];
6. Write the System Security Plan (SSP)[32];
7. Validate Security in Place [i.e., verify that the required controls are in place (we test them in the next step)];
8. Testing against Security Requirements;
9. Prepare Certification Package;
10. Forward Certification Package [to the DAA];
11. Accreditation Decision by DAA. ([8], 1.F.1-11, page 5)

Elsewhere in DCID 6/3 its "C&A process," as opposed to the 11 steps presented above, is cast in the mold of system development life-cycle phases. The operations in each phase do not cleanly correspond to the 11 steps, as shown in Table 27.

Multiple "separately accredited" systems may be connected to form an "interconnected IS." The terms of such a connection would be described in a document named the Interconnection Security Agreement (ISA) to which the DAAs of the individual systems must agree for the ISA to be in force. Among other things, the ISA describes one or more "Controlled Interfaces" (e.g., firewalls) that adjudicate communication between the interconnected systems.

---

30. IS = Information System.

31. I think this is colloquially referred to as "groupware". It is different than "collaborative systems" such as the Internet [20].

32. The SSP describes the planned or actual "operating conditions" of the system and its residual risk ([8], 1.F.6, page 5). The SSP appears to be similar to DITSCAP's SSAA except that the "*format and content of the SSP are at the discretion of the DAA*" ([8], Appendix C, emphasis in the original).

Table 27 DCID 6/3 Phases (Table 9.1, [8], pages 57-8)[a]

Phase	Operations[b]	Steps
Design and Development	Determine the category for the system. Based on the category, determine security requirements. Determine threats, vulnerabilities, risks, and countermeasures. Complete the "System Security Plan" (SSP).	1-6?
First Test and Evaluation (T&E I)	Develop "Certification Test Plan and Test Procedures" document.	7-8?
Second Test and Evaluation (T&E II)	Make plans to rectify gaps identified by running the tests described in the previous step. Complete the "Certification Package." Obtain accreditation.	9-11?
Operations and Maintenance (O&M)	Re-certify and re-accredit if changes so warrant.	Maybe 1-11
Disposal	Securely dispose of system.	

a. I have added the "Step" column at the right.

b. This is my own term—DCID 6/3 does not provide one—and I want to avoid "task" and "activity" which would suggest a connection here to DITSCAP and DIACAP.

E.1.2 Systems Classification for DCID 6/3

DCID 6/3 *uses* five partitions but it *defines* 62 partitions. The "Level-of-Concern" for a system consists of one of three "indicators" each for confidentiality, integrity, and availability. The High confidentiality indicator decomposes into five "Protection Levels." Hence there are 7 * 3 * 3 = 62 partitions.[33] The Levels-of-Concern is presented first in the material below, followed by Protection Levels, followed by a summary.

E.1.2.1 Levels-of-Concern

As noted above, the Level-of-Concern for a system consists of one of three indicators—High, Medium, and Basic—each for confidentiality, integrity, and availability. The Level-of-Concern for confidentiality is presumed to be independent of integrity and availability, likewise for integrity and for availability. The Level-of-Concern for confidentiality is based on the sensitivity of the information on the system. The Level-of-Concern for integrity is based on the "degree of resistance to unauthorized modification" ([8], 3.B.2.b, page 11) is required to protect the information. The Level-of-Concern for availability is based on the "degree of availability required" (ibid.) for the information.

33. The document notes 16 other factors that are part of a "complete IS certification" ([8], page 56). There does not appear to be a formal way provided for including those factors.

E.1.2.2 Protection Levels

The High Level-of-Concern for confidentiality decomposes into five Protection Levels. Protection Level 1 (abbreviated "PL1") does not provide as much protection as PL2, and PL2 does not provide as much protection as PL3, and so on, with PL5 providing the most protection. The five Protection Levels are defined based on three factors: required clearance(s), formal access approval(s), and need-to-know, as shown in Table 28.

Table 28 Five Protection Levels

<table>
<tr><th>Protection Level</th><th>Required Clearance(s)</th><th>Formal Access Approval(s)</th><th>Need-To-Know</th><th>Processing Mode[a]</th></tr>
<tr><td>1</td><td colspan="3">All[b]</td><td>Dedicated</td></tr>
<tr><td>2</td><td colspan="2">All</td><td>Some[c]</td><td>System High</td></tr>
<tr><td>3</td><td>All</td><td colspan="2">Some</td><td>Compartmented</td></tr>
<tr><td rowspan="2">4</td><td colspan="3">Some</td><td rowspan="4">Multilevel</td></tr>
<tr><td>"all users have at least a Secret clearance" ([8], 3.C.2.4, page 12) and there is Top Secret information in the system</td><td colspan="2"></td></tr>
<tr><td rowspan="2">5</td><td colspan="3">Some</td></tr>
<tr><td>"at least one user lacks any clearance for access to some of the information on the IS" ([8], 3.C.2.5, page 12) and there is Top Secret information in the system</td><td colspan="2"></td></tr>
</table>

a. Processing Mode is one of the seven system characteristics described in 5200.40 and in 8510.1-M. This column is added to this table to show the parallel between DCID 6/3 and those documents, as well as to acclimate readers who are already familiar with the various Processing Modes.

b. "All" means that all users have the required clearance(s) or the formal access approval(s) or the need-to-know, depending upon the parameter, for all of the information on the system.

c. "Some" means that some users (at least one) do not have the required clearance(s) or the formal access approval(s) or the need-to-know, depending upon the parameter, for all of the information on the system.

E.1.2.3 Summary

DCID 6/3 defines 7 * 3 * 3 = 62 partitions. However, the following passage

> *Since all systems accredited under the authority of this manual by definition process intelligence information, all systems accredited under this manual must be assigned a High Confidentiality Level-of-Concern*. ([8], 3.B.2.a, page 11, emphasis in the original)

lowers the number of partitions effectively to 5 * 3 * 3 = 45, because the Medium and Basic confidentiality Levels-of-Concern are eliminated, leaving only the five Protection Levels. And the preceding passage, along with the following passage,

> When a system has more than one kind of information in it [i.e., at least two different indicators for the three categories, such as High for confidentiality and Medium for integrity], the Level-of-Concern assigned is the *highest* Level-of-Concern for *any information* on the system. ([8], 3.B.1.a, page 11, emphasis in the original).

lowers the number of partitions even further to 5 * 1 * 1 = 5, namely the five Protection Levels, because the Medium and Basic indicators for both the integrity and availability Levels-of-Concern are eliminated. Nevertheless the DCID 6/3 provides "security features and assurance requirements" ([8], 3.D.1, page 12) for all three indicators for both integrity and availability, as well as for the five Protection Levels. It is not clear why these additional features and requirements are provided in the document but presumably it is for the same reason that the document speaks of determining the Level-of-Concern for a system, as well as the Protection Level, as part of application of DCID 6/3.[34]

E.1.3 Measurement Standard for DCID 6/3

DCID 6/3 provides lists of "security features and assurance requirements" for each Protection Level and for each Level-of-Concern for integrity and availability.[35] The "security features," sometimes referred to as "technical security features," appear to be what the document calls "protection mechanisms." The "assurance requirements," sometimes simply "assurances," appear to be more procedural, including ways to determine that the protections are operating as they should. However, there does not appear to be a definition of any of these terms anywhere in the document, including in the "Glossary of Terms" in Appendix B.

As an example of a "security feature," the following is the first such item for Protection Level 1:

> [**Access1**] Access control, including:
>
> a. Denial of physical access by unauthorized individuals unless under constant supervision of technically qualified, authorized personnel.

---

34. For example, at one point in the document we read, "Having determined the appropriate Levels-of-Concern and Protection Level for an IS, the DAA next needs to…" ([8], 3.D.1, page 12).

35. Explicitly missing from the document are security features and assurance requirements for Basic and Medium Confidentiality.

> b. Procedures for controlling access by users and maintainers to IS resources, including those that are at remote locations. ([8], 4.B.1.a, page 14, emphasis in the original).

Other categories of security features include identification & authentication, parameter transmission, recovery procedures, screen lock, session controls, data storage, and data transmission.

As an example of "assurance requirements," the following is the first such item for Protection Level 1:

> [**Doc1**] Documentation shall include:
>
> a. A System Security Plan.
>
> b. A Security Concept of Operations (CONOPS)…The CONOPS shall at a minimum include a description of the purpose of the system, a description of the system architecture,… ([8], 4.B.1.c, page 15, emphasis in the original)

In general the security features and assurance requirements for higher Protection Levels are a superset of those for lower Protection Levels, in the same way that the Checklists for 8510.1-M are cumulative. So, for example, for Protection Level 2 there is an "[Access2]," in addition to "[Access1]." However, for Identification and Authentication the pattern is different: there is an "[I&A1]" for Protection Level 1 but for Protection Level 2 there is no "[I&A1]" but there are "[I&A2]," "[I&A3]," and "[I&A4]," and for Protection Level 3 there is "[I&A2]," "[I&A4]," and "[I&A5]."[36]

E.2 NIST 800-37

NIST 800-37 could be described as a mix of DITSCAP and DIACAP. It has the phases of DITSCAP and the simplicity of DIACAP, along with DIACAP's simple Package, as opposed to DITSCAP's unwieldy SSAA. I could see no mention in the document of either DITSCAP or DIACAP in general or 5200.40, 8510.1-M, 8500.1, or 8500.2 in particular, although there is one mention of DCID 6/3 in the glossary.

E.2.1 Process for NIST 800-37

NIST 800-37 describes a four-phase process that map cleanly to DITSCAP's four phases and

36. The tables in Appendix D that show these requirements are at odds with what appears in the body of the document. For example, Appendix D shows that [I&A1] is required for all five Protection Levels.

almost as cleanly to DIACAP's five activities, as shown in Table 29.

Table 29 NIST 800-37 Phase or Activity Names

Phase or Activity	NIST 800-37	DITSCAP	DIACAP
1	Initiation	Definition	Initiate and Plan C&A
2	Security Certification	Verification	Implement and Validate Assigned IA Controls
3	Security Accreditation	Validation	Make Certification Determination & Accreditation Decision
4	Continuous Monitoring	Post Accreditation	Maintain Authority to Operate and Conduct Reviews
5			Decommission

The work to be done in each phase, whether it be NIST 800-37, DITSCAP, or DIACAP, is essentially the same.

NIST 800-37 partitions the four phases into 10 tasks and into 31 subtasks.

Meanwhile, NIST 800-37 uses a "security accreditation package" which consists of three parts:

1. the system security plan,
2. the security assessment report, and
3. the plan of action and milestones (Figure 2.3, page 22).

This is similar to the DIACAP Package in the simplicity of its categories and similarly unlike the DITSCAP SSAA.

E.2.2 Systems Classification for NIST 800-37

NIST 800-37 notes that the "effort for security certification and accreditation…should be scalable to the FIPS 199 security category of the information system" ([24], page 25), and each NIST 800-37 subtask includes "Supplemental Guidance for Low-Impact Systems" but that is the extent of the document's use of a systems classification.

Note: FIPS 199 defines the following structure by which the "SC" (i.e., "security category") of an "information type" can be defined by the following structure:

> SC information type = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)},
>
> where the acceptable values for potential impact are LOW, MODERATE, HIGH, or NOT APPLICABLE" ([10], page 7, emphasis in the original)[37]

37. That is, "impact" is a placeholder that can be replaced with "LOW", "MODERATE", etc., for a given system.

This creates 3 * 4 = 12 system categories.

E.2.3 Measurement Standard for NIST 800-37

NIST 800-37 does not include a list of controls. Rather it refers to the controls in NIST 800-53 [25].

NIST 800-37 directs that the implementation for those controls be judged based on the phrase shown in italics in the following passage:

> Security certification is a comprehensive assessment of the management, operational, and technical security controls in an information system made in support of security accreditation to determine the extent to which the controls are *implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements for the information system*. ([24], page 1, emphasis added)

The italicized phrase in the above passage appears at least 11 times in NIST 800-37 (on pages 1, 2, 8, 15, 18, 21, 32, 35, 35 (again), 37, and 45).

E.3 COBIT®

COBIT[38] is focused on IT governance. The organizational roles that are responsible for IT governance and what IT governance is are both described in the following passage:

> **IT governance is the responsibility of executives and the board of directors, and consists of the leadership, organisational structures and processes that ensure that the enterprise's IT sustains and extends the organisation's strategies and objectives.** ([5], page 6, emphasis in the original)

IT governance[39] is a proper superset of security. COBIT deals with efficiency, effectiveness, reliability, and compliance, in addition to the usual security triumvirate of confidentiality, integrity, and availability.[40]

COBIT describes itself well in the following two passages:

> COBIT has been developed and is maintained by an independent, not-for-profit research institute[41], drawing on the expertise of its affiliated association[42] members, industry experts, and control and security professionals. Its content is based on continuous research into IT best

38. "COBIT," "Information Systems Audit and Control Association", "ISACA," "IT Governance Institute", and "ITGI", are registered trademarks, and "COBIT Online" is a trademark, of ISACA and the IT Governance Institute.

39. Heschl provides a more succinct definition of IT governance: "the system by which the organisation's IT is governed and controlled" ([21], page 11).

40. The four topics—efficiency, effectiveness, reliability, and compliance—appear also in COSO [7].

41. The "IT Governance Institute" (ITGI) (www.itgi.org), established in 1998.

> practice and is continuously maintained[43], providing an objective and practical resource for all types of users. ([5], page 26)
>
> COBIT is based on the analysis and harmonisation[44] of existing IT standards and best practices and conforms to generally accepted governance principles. It is positioned at a high level, driven by business requirements, covering the full range of IT activities, and concentrating on what should be achieved[45] rather than how to achieve effective governance, management and control. Therefore, it acts an integrator of IT governance practices and appeals to executive management; business and IT management; governance, assurance and security professionals; as well as IT audit and control professionals. It is designed to be complementary to, and used together with, other standards and best practices. (ibid.)

Note that COBIT comes from a non-profit organization; it is continuously maintained; it is intended to be universal in its applicability; it is based on current standards; it focuses on ends, not means; it intends to be an integrator and complementary with other standards—all aspects which distinguish it from the seven other documents[46] reviewed in this report.[47]

The sections below—Process, Systems Classification, and Measurement Standard—follow the pattern for the review of the other documents in this report. However, the bulk of the information is in the last section. (A general introduction to COBIT is available [3].)

E.3.1 Process for COBIT

The presence of COBIT's set of control objectives (see Appendix E.3.3) enables the following "certification" conversation:

> System Owner: We satisfy this control objective by implementing those controls.
>
> Auditor: Based on the evidence I have gathered, my evaluation of your implementation of those controls is that they are {Choose one: inadequate, adequate} to satisfy this control objective.

However, COBIT is focused on governance, not certification. COBIT does not provide a process that compares with the phases, tasks, and subtasks provided by the other documents reviewed in this report. (Note that the above "conversation" does not address the importance (or unimportance) of the control objective in the context of the organization's overall objectives.)

---

42. ISACA (www.isaca.org), formerly the "Information Systems Audit and Control Association," grew out of the EDP Auditors Foundation, established in 1969.

43. See "COBIT Online" at www.itgi.org.

44. e.g., Macartney [19].

45. via the use of "control objectives" (see Appendix E.3.3).

46. namely 5200.40, 8510.1-M, 8500.1, 8500.2, DIACAP, DCID 6/3, and NIST 800-37. (DIACAP may prove to be the exception concerning being continuously maintained.)

47. In March 2005 COBIT was selected by the Commission of the European Communities (EC) as one of three "internationally accepted standards to be used to provide information security and control of its agricultural paying agencies" ([17], page 35). (The other two standards are ISO 17799 [14] and BSI [1].)

E.3.2 Systems Classification for CobiT

CobiT provides no systems classification. A classification could be developed based on CobiT. For example, systems could be classified based on the "maturity," measured on a scale of 0-5 (described in Appendix E.3.3.1) for each of the 34 processes (see Appendix E.3.3). However, such a systems classification note is explicitly not the purpose of CobiT's Maturity Model.

E.3.3 Measurement Standard for CobiT

CobiT consists, essentially, of 215 **control objectives** defined as follows:

> A statement of the desired result or purpose to be achieved by implementing control procedures in a particular process. ([5], page 191)

Control procedures—or simply **controls**—are defined as follows:

> The policies, procedures, practices and organisational structures designed to provide reasonable assurance that the business objectives will be achieved and undesired events will be prevented or detected ([5], page 191).

CobiT organizes its set of 215 control objectives into 34 "processes," organized, in turn, into four "domains." In addition, at the other end of the hierarchy, there are 1,547 "Control Practices," beneath the control objectives. The hierarchy is shown in Table 30.

Table 30 CobiT's Control Objective Hierarchy

Level	Name	Number of Elements at this Level
1	Domain	4
2	Process[a]	34
3	Control Objective[b]	215
4	Control Practice	1547[c]

a. Also known as "High-Level Control Objective."

b. Also known as "Detailed Control Objective" to distinguish from "High-Level Control Objective."

c. The number shown here is for the previous version of CobiT, the "3rd Edition." The Control Practices have not yet been converted to CobiT 4.0.

The four domains are named as follows, with the abbreviation for each shown in parentheses:

- Plan and Organise (PO),
- Acquire and Implement (AI),
- Deliver and Support (DS), and
- Monitor and Evaluate (ME).

The four domains correspond to "plan, build, run and monitor" ([5], page 14), respectively, or

Deming's plan-do-check-act (PDCA) cycle.

To give a flavor of control objectives, several examples are shown below. The fifth process in the "Deliver and Support" domain is DS5, named "Ensure Systems Security."[48] The first two control objectives are as follows:

> **DS5.1 Management of IT Security**
>
> Manage IT security at the highest appropriate organisational level, so the management of security actions is in line with business requirements.
>
> **DS5.2 IT Security Plan**
>
> Translate business information requirements, IT configuration, information risk action plans and information security culture into an overall IT security plan. The plan is implemented in security policies and procedures together with appropriate investments in services, personnel, software and hardware. Security policies and procedures are communicated to stakeholders and users. ([5], page 120, emphasis in the original)

The first two Control Practices under DS5.1 are as follows:

> 1. The need to prepare and maintain a technological strategic and tactical security plan is laid out in a policy.
>
> 2. The responsibility for the preparation, maintenance and approval of such strategic and tactical security plans (including succession plans) is identified, and the required skills for this task are available within the organisation. Senior management from across the organisation is involved. ([16], page 130)

The second process in the "Monitor and Evaluate" domain is ME2 "Monitor and Evaluation Internal Control." The control objectives within this process provide direction for what the other documents in this report call "certification." The names of the control objectives in that process are as follows:

- ME2.1 Monitoring of Internal Control Framework
- ME2.2 Supervisory Review
- ME2.3 Control Exceptions
- ME2.4 Control Self-assessment
- ME2.5 Assurance of Internal Control
- ME2.6 Internal Control at Third Parties
- ME2.7 Remedial Actions

ITGI has produced a set of "Audit Guidelines" [15] to assist in this task. Guidelines are

48. I have chosen to show the control objectives from this process, instead of the first one in COBIT, to align with the focus of the other documents in this report, namely security.

provided for each process. Included in the guidance is direction on whom to interview and what documents to obtain, what to consider when evaluating the controls, what to test, and how to evaluate the current risk.

The ME domain provides additional direction, as noted by the names of the three other processes in that domain:

- ME1 Monitor and Evaluate IT Performance
- ME3 Ensure Regulatory Compliance
- ME4 Provide IT Governance

COBIT can be overwhelming, so ITGI has provided a beginner's document entitled "COBIT *Quickstart*."

To enable measurement, COBIT provides a "Maturity Model" and performance goals and metrics. Each of these will be described in the next two sections.

E.3.3.1 Maturity Model

COBIT provides a "Maturity Model" along the lines developed by the Software Engineering Institute (SEI) for software development capability. There are six levels in the model:

0. Non-existent
1. Initial / Ad Hoc
2. Repeatable but Intuitive
3. Defined Process
4. Managed and Measurable
5. Optimised

COBIT includes a description of maturity at each level for each of the 34 processes. COBIT's maturity model is not for certification and thus is different than the models presented in the other documents reviewed in this report, as noted in the following passage:

> The COBIT maturity model focuses on capability, but not necessarily on performance. They are not a number for which to strive, nor are they designed to be a formal basis for certification levels with discrete levels that create thresholds that are difficult to cross. However, they have been designed to be always applicable, with levels that provide a description an enterprise can recognise as best fitting its processes. The right level is determined by the enterprise type, its environment and strategy. ([5], page 21)

Note that maturity is a function of cost vs. benefit and involves due diligence.

E.3.3.2 Performance Goals and Metrics

COBIT describes Key Performance Indicators (KPIs) (i.e., metrics) for activities within a process that drive Key Goal Indicators (KGI) (i.e., goals) in the process, and KPIs within the process that drive the IT organization, as suggested in Figure 7 ([5], page 121).

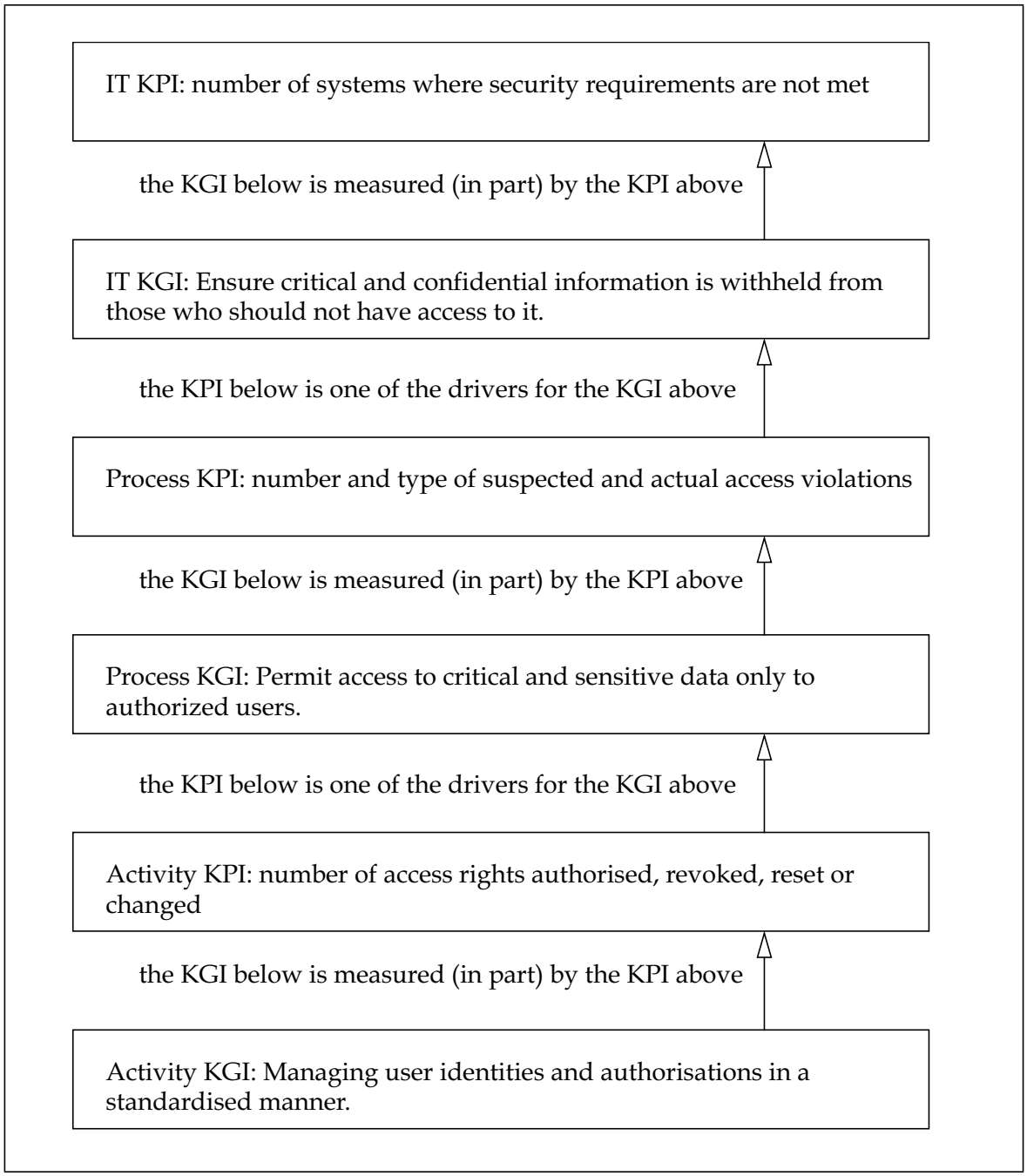

Figure 7 Some Key Performance Indicators (KPI) and Key Goal Indicators (KGI)

This page intentionally almost blank.

Distribution:

2	MS	0899	Technical Library, 4536
2	MS	9018	Central Technical Files, 8944