

Unifying The Body Of Knowledge: Why Global Business Requires A Single Model For Information Security

Dan Shoemaker, University of Detroit Mercy
Gregory Ulferts (Email: ulfertgw@udmercy.edu), University of Detroit Mercy
Jeanne David, University of Detroit Mercy
Robert Otten, Blue Cross/Blue Shield

1. Introduction

There is probably no better way to introduce this article than by means of a scenario contained in the Critical Infrastructure Protection Taskforce's *National Strategy to Secure Cyberspace* (Department of Homeland Security, 2002).

Consider this... A terrorist organization announces one morning that they will shut down the Pacific Northwest electrical grid for six hours starting at 4:00PM; they then do so. The same group then announces that they will disable the primary telecommunication trunk circuits between the U.S. East and West Coasts for a half day; they then do so, despite our efforts to defend against them. Then, they threaten to bring down the air traffic control system supporting New York City, grounding all traffic and diverting inbound traffic; they then do so. Finally, they threaten to cripple e-commerce and credit card service for a week by using several hundred thousand stolen identities in millions of fraudulent transactions. Imagine the ensuing public panic and chaos. What makes this scenario both interesting and alarming is that all of the aforementioned [types of] events have already happened, albeit not concurrently nor all by malicious intent. They occurred as isolated events, spread out over time; some during various technical failures, some during simple exercises, and some during real-world cyber attacks. (Excerpt from a letter to President Bush from 50 scientists, computer experts and former intelligence officials, UCSD/CAIDA, 2002, The Regents of the University of California)

The implication of this is clear. Every sector in the global economy, from energy, through transportation, finance and banking, telecommunications, public health, emergency services, water, chemical, defense, right down to the industrial, and agriculture sectors, is totally dependent on the reliable functioning of its IT assets. Thus anything that threatens these effectively poses a threat to our way of life. And accordingly, almost any effort expended to protect them is both justifiable and necessary. So the obvious question is... "What is the current state of affairs"? The Critical Infrastructure Taskforce sums that up in five global statements (Department of Homeland Security, 2002):

1. Cyber incidents are increasing in number, sophistication, severity and cost.
2. The nation's economy is increasingly dependent on cyberspace. This has introduced unknown interdependencies and single points of failure.
3. A digital disaster strikes some enterprise every day. Infrastructure disruptions have cascading impacts, multiplying their cyber and physical effects.
4. Fixing vulnerabilities before threats emerge will reduce risk.
5. It is a mistake to think that past levels of cyber damage are accurate indicators of the future. Much worse can happen.

In the U.S. the most recent annual FBI/Computer Security Institute survey found that eighty percent of the businesses had sustained financial losses as a result of security breaches, with the average being more than \$2 million (CSI, 2002). More than 60% of the companies In a nationwide survey conducted by the Government of Great Britain (DTI, 2001) had suffered an information security breach and an estimated 320,000 of those organizations

reported a "serious" breach. Furthermore the DTI study found that the majority of the firms that had experienced such a serious security incident thought there was nothing they could have done to prevent it. That is, they had the usual controls in place, such as passwords and firewalls yet they were still suffering significant losses.

The root cause for these failures, which was highlighted in both the U.S. and British studies, was a lack of understanding that information security is as much a strategic policy issue rooted in the business domain, as it is a technical concern. For instance, most of the security losses in the United States in the year 2002 came from the actions of people INSIDE the business, not external intrusions (CSI, 2002) In the British survey the finding was that, although eighty three percent of the companies in the DTI study used passwords and seventy five percent had virus protection, only sixty nine percent actually recognized that information was a business asset and only fourteen percent had a security policy in place.

Two examples cited in e-world (Moad, 2002) illustrate why business policy and procedure are as much a part of a good security package as firewalls and passwords. One of these involved an investment adviser who was allowed to keep his e-mail account when he left his former employer to work for a competitor. Using that account he was able to tap into e-mail discussions among ex-colleagues who were plotting how to steal back clients from him. In another case, a salesman at a large Wall Street brokerage was able to continue using his old e-mail account after changing companies. Through that account he was able to convince clients that the old company had been sold and that they needed to transfer their business to his new employer.

Two critical points must be stressed here. First, neither of these examples could have been prevented by technological means (e.g., they both represent a breakdown in human resources policy). And both of them involved a loss of competitive advantage to the companies where they occurred. Which introduces the three major assumptions that underpin this article:

1. Effective Information security requires an integrated set of business and technological processes.
2. Effective information security programs must be deliberately designed and deployed organization-wide through a strategic planning activity
3. Effective information security programs must be systematic, in the sense that they must embody an appropriate set of persistent and interacting components that function seamlessly as an integral part of the day-to-day operation of the business

It is necessary to satisfy ALL of these requirements because effective security is not a trivial problem. Cyberspace is full of threats that can vary from lone hackers through malicious insiders to organized criminal enterprises right up to terrorists and enemy nation states. And in addition it is a given that because of the nature of technology itself, new vulnerabilities and weaknesses will crop up daily. So to be safe, every organization must have a comprehensive, robust and continuously evolving protection stratege to deal with foreseen, and unforeseen, hazards as they appear.

However that preparedness does not happen by chance. It requires a formal organization-wide security planning and monitoring system that most organizations do not presently recognize the need for, let alone have. Nonetheless there are (at the present time)¹ at least three major initiatives underway to define a comprehensive conceptual frame of reference to build effective information security systems. These are (in no particular order of importance) the Generally Accepted System Security Principles (GASSP), ISO 17799 and COBIT. Each of these embodies fundamental best-practice principles that have been derived from the body of knowledge in information security protection. Each of these provides a useful set of high level control objectives, which can be tailored, to design and develop an effective organizational security response. And each of these has the potential to serve as the basis for a common global solution.

¹ This footnote is necessary because there are a number of projects in the "talking" stage worldwide that could mature into full-fledged initiatives. Preeminent among those are the "Common Criteria" (AKA ISO 15408) and the principles of the CISSP. One of the purposes of this article is to point out that the addition of one more proposed framework to an already crowded field will not help the situation.

The problem lies in the obvious fact that there are three or these, rather than one single agreed-on approach. Worse, each has its own group of adherents who tend to view the practitioners of the other models as “infidels”. As a consequence there is no authoritative recommendation about the correct approach, which is an extremely dysfunctional situation in the practical world. So clearly, the first step in effecting a resolution to this impasse is the careful study and comparison of the underlying principles and high-level control objectives to see where the common ground lies. That is the purpose of this article.

2. Purpose And Approach

The goal of this article is to compare the control objective recommendations of the GASSP, ISO 17799 and COBIT Standards to each other. The aim is to identify and characterize the commonality between these three approaches. The intention is to provide the basis for harmonizing their contents into a single standard, which can serve as the necessary unified global roadmap for the development and deployment of effective responses to the challenges of information protection.

Our approach was to map the principles embodied in each of these models, along with their attendant high-level control objectives to each other. But before we get to the results of this comparison, we are going to provide a short background on each model for the sake of anybody who is approaching the subject of standardized information security for the first time.

3. Background Of The Models

3.1. Generally Accepted System Security Principles (GASSP)

The origins of GASSP are directly traceable to a 1990 report issued by the U.S. National Research Council. In response to this report the private sector’s International Information Security Foundation (I²SF) along with the International Information Systems Security Certification Consortium (ISC) ² and the internationally based Common Criteria task force formulated the GASSP project (1992). Ten countries currently participate in this project and it is entering U.S. Federal government service through the auspices of NIST and the National Security Agency.

The stated intention of GASSP is to create an infrastructure that will mirror the much more commonly recognized Generally Accepted Accounting Principles (GAAP) that underwrite the international accounting profession. The model is based on and embodies information security concepts developed by the Organization for Economic Cooperation and Development (OECD). It incorporates into a hierarchy nine high-level items, which it calls “Pervasive Principles” and fourteen high-level control objectives, which it calls “Broad Functional Principles”. There are also “Detailed Principles” which underlie each of these Broad Functional Principles. These have yet to be developed.. Table One lists the nine Pervasive Principles (from GASSP v2, International Information Security Foundation).

Table 1: Pervasive Principles

- | | |
|----|--|
| 1. | Accountability – Security responsibility must be clearly defined and acknowledged |
| 2. | Awareness – All parties should have knowledge of principles and applicable threats |
| 3. | Ethics – Information should be used and security executed in an ethical manner |
| 4. | Multidisciplinary – Security should address the viewpoints of all interested parties. |
| 5. | Proportionality – Security should be proportionate to the risks |
| 6. | Integration – Security principles should be coordinated with organizational policies |
| 7. | Timeliness – Parties should respond in a timely manner to breaches and threats |
| 8. | Assessment – The risks should be periodically assessed |
| 9. | Equity – Management shall respect the rights and dignity of individuals |

3.2. ISO 17799:2000

This framework is the flagship of the International Standards Organization (ISO). Because of ISO’s universal reach and track record in the global standardization process this should be considered to be the world community’s commonly accepted Standard for information security. It has its origins as a British Standard 7799:1 in the same general timeframe as GASSP. However from an application standpoint it is more mature since it already encompasses detailed control objectives.

ISO 17799 embodies ten high level control objectives, which in essence function in the same inclusive fashion as the Pervasive Principles of GASSP. In addition, there is an accompanying guideline, BS 7799:2, which is indispensable to the use of 17799. That document specifies the 127 explicit controls, which are directly referenced to the high-level control objectives of 17799. It also specifies a very comprehensive and unambiguous risk assessment, and audit process that makes this standard relatively easy to implement and maintain. Table Two outlines the ten high level control objectives of ISO 17799 (ISO, 2000).

Table 2: High Level Control Objectives of ISO 17799	
1.	Security Policy – a full set of security policies will be published in a policy manual
2.	Organizational Security –an information security infrastructure will be created
3.	Asset Classification and Control – asset classification and management will occur
4.	Personnel Security – all necessary internal personnel security procedures will exist
5.	Physical and Environmental Security –physical security and control policies
6.	Communications and Operations Management –software security policies will exist
7.	Access Control –access control policy will exist
8.	Systems Development and Maintenance –security items for development process
9.	Business Continuity Management - contingency plans for business continuity
10.	Compliance – compliance with any regulatory and/or legal requirements

4. Control Objectives For Information And Related Technology (COBIT)

Control Objectives for Information and related Technology (COBIT 3rd edition) is a control framework that has been promulgated by the Information Systems Audit and Control Association and Foundation (ISACA/F). It gets its international currency through the IT Governance Institute. Its development can be related to the work of the Treadway commission, so it may be considered to have originated in the same general period as the other two models. (1992).

COBIT is meant to serve as a comprehensive guideline for constructing secure IT processes. It does this by specifying a standard set of control functions. These are embodied within a control framework. There are four process domains that govern this framework: (1) Planning and organization, (2) Acquisition and implementation, (3) Delivery and Support and (4) Monitoring. This is then further elaborated by means 34 high-level *Control Objectives*, one for each of the IT processes that are represented within these four domains. To aid in that process, COBIT provides 318 detailed control objectives, which have been individually referenced to each of the high-level control functions. The detailed control objectives are contained in another (lengthy) element of the COBIT documentation set and are not used in this comparison because they populate a more precise stratum of detail than the control objectives of the other standards.

5. A Mapping Comparison

Given the background provided in the prior section, the aim of this article is to present a detailed comparison of the principles embodied in these three models for the purpose of identifying commonalities that might serve as a basis for harmonization of a single standard for information security. As a first step in this process Figure One lays out the high-level control objectives of all three standards side-by-side. There has been some minor editing of this table for readability but fundamentally what is displayed are the (conceptually similar) security principles em-

bodied in each of these models. Items have been placed in the same row where their intent is equivalent. Shading indicates unique principles, or items that do not have an exact equivalent in the other standards.

Figure 1: High Level Control Objectives

GASSP	IS 17799	COBIT
Information Security Policy	Security Policy	Communicate Direction
Accountability Infrastructure	Security Infrastructure	Define the IT Organization
Catalogue Information Assets	Asset Control	Information Architecture
Personnel Security	Personnel Security	Manage Human Resources
Physical & Environmental Security	Physical Security	Manage Facilities
Network/Infrastructure Security	Communication Management	Manage Operations
Access Control	Access Control	Ensure Systems Security
Lifecycle Security Management	Systems Development	Manage the Configuration
Continuity Planning/Assurance	Continuity Management	Ensure Continuous Service
Regulatory/Contractual Compliance	Compliance	Compliance
Risk Assessment/Management		Assess Risks
Education and Awareness		Educate and Train Users
Application/System Security		Manage Performance/Capacity
Ethical Practices		Manage the IT Investment
		Manage Projects
		Manage Quality
		Identify Automated Solutions
		Acquire Application Software
		Install and Accredite Systems
		Manage Changes
		Define Manage Service Levels
		Manage Third-Party Services
		Strategic IT Plan
		Identify and Allocate Costs
		Technological Direction
		Assist and Advise Customers
		Manage Problems and Incidents
		Manage Data
		Technology Infrastructure
		Develop Security Procedures
		Monitor the Processes
		Assess Control Adequacy
		Obtain Independent Assurance
		Provide for Independent Audit

Even though there are a different number of high-level control objectives it is easy to identify a set of common factors by simply looking at the principles side-by-side. Based on this comparison it is possible to see that the following ten issues are shared

1. Security Policy
2. Security Infrastructure
3. Asset Identification
4. Personnel Security
5. Physical Security
6. Access Control
7. Operational Process/Network Security
8. Lifecycle Development Process Security
9. Business Continuity
10. Regulatory Compliance

Three other common control objectives can be added to the list even though there is no explicit statement in one of the models at this level. Specifically, in the case of 17799, which involves the fewest high-level control objectives, there is an obligation to consider the lower level objectives. Once that has been done there is unequivocal support for the shared nature of these final three items.

1. Risk Assessment (which is explicit in COBIT and GASSP and central to the 7799:2 guideline of 17799)
2. Application/System Security (which is explicit in COBIT and GASSP and implicitly embodied as a lower level control objective under the Access Control and Systems Development control objectives of 17799)
3. Education and Awareness (which is also explicit in COBIT and GASSP and embodied as a lower level control objective under the Security Infrastructure and Personnel control objectives in 17799)

Finally in the case of COBIT, because it is more of an accounting control framework than an explicit security standard the 34 high level objectives it embodies are inevitably going to introduce some detailed factors not shared by the rest. However, there is explicit evidence that these thirteen items are embodied by concept in all of these models. And as a consequence it might be safe to say that there is considerable overlap between them.

Moreover, the point of this article is not to advocate a new framework, in fact that would be exactly counter to its goals. Our only aim is to demonstrate the commonality between these three very important models, two of which almost perfectly mirror each other, and to suggest that the responsible agencies could help practitioners out by harmonizing a single agreed on definition of what constitutes the information security body of knowledge out of this similarity.


Getting a single agreed on approach is particularly important to two very different groups, practitioners and educators. It is true for IT workers because information protection is not a trivial or easy to put into practice discipline. And without a common definition of the fundamental building blocks it is almost impossible to be assured that you are undertaking due diligence. In the case of educators the problem is more a matter of deciding what to teach. The current situation has a number of true believers in higher education who adhere to a certain model as if it were the one solution, which is patently not true. With a single common definition of the body of knowledge educators could begin to train people under a unified concept. This clarification would make the current programs in security education much more effective, because they could advocate a commonly recognized and authoritative set of principles rather than the current situation, which requires them to present a range of approaches and caveats.

6. Conclusion

The conclusion to this is to some extent embodied in the prior section. We believe that the current state of affairs is particularly dysfunctional because of the confusion created by the presence of too many “authoritative” models. Because of the complex issues that must be addressed in securing a large organization, it is probably inevitable that countries and major industries will continue to go the route of communicating expert best practice advice in

the form of a favorite standard. If that is the case the worst possible situation for global commerce, particularly for something as borderless as IT, is the prospect of having a number of potentially controlling definitions.

Moreover, this is presently the emerging trend since, for example, as a result of the impacts of the “slammer” virus the Government of the UK has put in motion a requirement that all industrial sectors MUST have a BS 7799 (e.g., ISO 17799) compliance certificate. And since the United States is the home of two other initiatives, one known as “the Common Criteria” as well as GASSP (under the auspices of the National Performance Review Task Force) and information security is a pressing priority of the Strategy to Secure Cyberspace, of the National Infrastructure Taskforce, it is likely that one of those models will be adopted. And if this were to be the case companies who operate in these two countries would have to install and comply with two entirely DIFFERENT security system standards. That is not to mention the fact that there are already strict compliance requirements based around the National Security Telecommunications and Information Systems Security Standards (NSTISSI), which control interaction with Federal Government agencies such as NSA.

So there is some pressing importance in coming to agreement on a single expert model of best practice that satisfies both the operational and the political concerns that surround this issue. We believe that we have made the case that people are essentially all saying the same thing. The issue is for them to agree on and publish a single definitive model that can provide effective guidance to practitioners. ISO pretty much did that with the definitive ISO 12207 Standard (adopted in the US as IEEE 12207.1 and by the military as MIL-STD 498), which after fifteen years of study and discussion provided an unequivocal definition of the software lifecycle. This framework has been an immeasurable asset to managers in IT organizations because it has created a common concept of IT operation. However, given the stakes in global security, the requirement for a single standard for software lifecycle process is nothing compared to the need for a common understanding of how to define and implement effective information protection solutions. Given the fact that authoritative understanding has been achieved in one area of the discipline, we believe that it is possible to do it in another more important one. Furthermore we believe that the diverse players are very close to each other in their concepts. All that is required is a globally accepted statement of that, which is the point of our article. 

References

1. “7799 Standards Can Enhance Your Organization's Information Security Program”, Business/Technology Editors, *InfoWorld*, 10, 2001
2. Ashton, Gerry, “Cleaning up your Security Act for Inspection”, *Computer Weekly* Jan 18, 2001
3. British Standards Institution, BSI 7799:2, 1999
4. CEN/CENELEC, *Internal Regulations, Part 2, Common Rules for Standardization Work*
5. Critical Infrastructure Taskforce, *National Strategy to Secure Cyberspace* (Draft), Department of Homeland Security, September 18, 2002
6. Department of Trade and Industry, *Information Security Breaches Survey*, Great Britain, 2001
7. Dorofee A.J., JA Walker, RC Williams, “Risk Management in Practice”, *Crosstalk*, Volume 10 #4, April 1997
8. Goodwin, William “UK's security code of practice becomes worldwide standard”, *Computer Weekly*, Jan 25, 2001
9. Information Systems Audit and Control Association (ISACA), “Framework”, *COBIT* (third edition)
10. Internet Business News, *CSI Survey*, FBI/Computer Security Institute, April 8, 2002
11. Moad, Jeff, “The Answer to Security Riddle”, *e-world*, May 20, 2002
12. Simons, Mike, “NHS takes unpopular BS 7799”, *Computer Weekly*, Jan 18, 2001
13. Swanson, Marianne, “Security Self Assessment Guide for Information Technology Systems”, National Institute of Standards and Technology NIST 800-26, November 2001
14. United Kingdom Accreditation Service (UKAS), *UKAS Directory of Accredited Inspection Bodies*

Notes