

## University of Dayton eCommons

---

MIS/OM/DS Faculty Publications

Department of Management Information Systems,  
Operations Management, and Decision Sciences

---

3-2015


# Assessing the Emphasis on Information Security in the Systems Analysis and Design Course

William David Salisbury  
*University of Dayton*, [wsalisbury1@udayton.edu](mailto:wsalisbury1@udayton.edu)

Thomas W. Ferratt  
*University of Dayton*, [tferratt1@udayton.edu](mailto:tferratt1@udayton.edu)

Donald E. Wynn  
*University of Dayton*, [dwynn1@udayton.edu](mailto:dwynn1@udayton.edu)

Follow this and additional works at: [https://ecommons.udayton.edu/mis\\_fac\\_pub](https://ecommons.udayton.edu/mis_fac_pub)

 Part of the [Business Administration, Management, and Operations Commons](#), [Databases and Information Systems Commons](#), [Management Information Systems Commons](#), [Management Sciences and Quantitative Methods Commons](#), [Operations and Supply Chain Management Commons](#), and the [Other Computer Sciences Commons](#)

---

### eCommons Citation

Salisbury, William David; Ferratt, Thomas W.; and Wynn, Donald E., "Assessing the Emphasis on Information Security in the Systems Analysis and Design Course" (2015). *MIS/OM/DS Faculty Publications*. 48.  
[https://ecommons.udayton.edu/mis\\_fac\\_pub/48](https://ecommons.udayton.edu/mis_fac_pub/48)

This Article is brought to you for free and open access by the Department of Management Information Systems, Operations Management, and Decision Sciences at eCommons. It has been accepted for inclusion in MIS/OM/DS Faculty Publications by an authorized administrator of eCommons. For more information, please contact [frice1@udayton.edu](mailto:frice1@udayton.edu), [mschlangen1@udayton.edu](mailto:mschlangen1@udayton.edu).

# Communications of the Association for Information Systems



## Issues and Opinions: Assessing the Emphasis on Information Security in the Systems Analysis and Design Course

W. David Salisbury

*MIS, OM & Decision Sciences Department, University of Dayton*  
*salisbury@udayton.edu*

Thomas W. Ferratt

*MIS, OM & Decision Sciences Department, University of Dayton*

Donald Wynn, Jr.

*MIS, OM & Decision Sciences Department, University of Dayton*

---

### Abstract:

Due to several recent highly publicized information breaches, information security has gained a higher profile. Hence, it is reasonable to expect that information security would receive an equally significant emphasis in the education of future systems professionals. A variety of security standards that various entities (e.g., NIST, COSO, ISACA-COBIT, ISO) have put forth emphasize the importance of information security from the very beginning of the system development lifecycle (SDLC) to avoid significant redesign in later phases. To determine the emphasis on security in typical systems analysis and design (SA&D) courses, we examine (1) to what extent security is emphasized in the core SA&D courses and (2) at what phase in the SDLC do most SA&D courses begin to emphasize security. In order to address these questions, we reviewed SA&D textbooks currently on the market to identify how extensively they cover security-related issues. Given the fairly high awareness of information security in practice, we expected to see an equally high emphasis on such matters in the textbooks. However, our review suggests that this is not the case, which suggests a gap in our preparation. To address this gap, we offer a proposal for modifying a portion of the SA&D curricula.

**Keywords:** Systems Analysis And Design, Security, Information Risk, Pedagogy.

Volume 36, Article 18, pp. 337-356, March 2015

The manuscript was received 12/02/2014 and was with the authors 2 months for 4 revisions.

### I. INTRODUCTION

Businesses, governments, and other institutions serve their respective constituencies today in an age of ever-increasing global connectivity and integration, which is facilitated by the information infrastructure that the Internet provides. Open standards and protocols enable easy communication among enterprises of all stripes, including those governmental organizations that oversee commerce activities (Salisbury, Miller & Turner, 2011). With the advent of big data and cloud-based computing, organizations are increasing their online presence, and data volumes continues to grow rapidly.

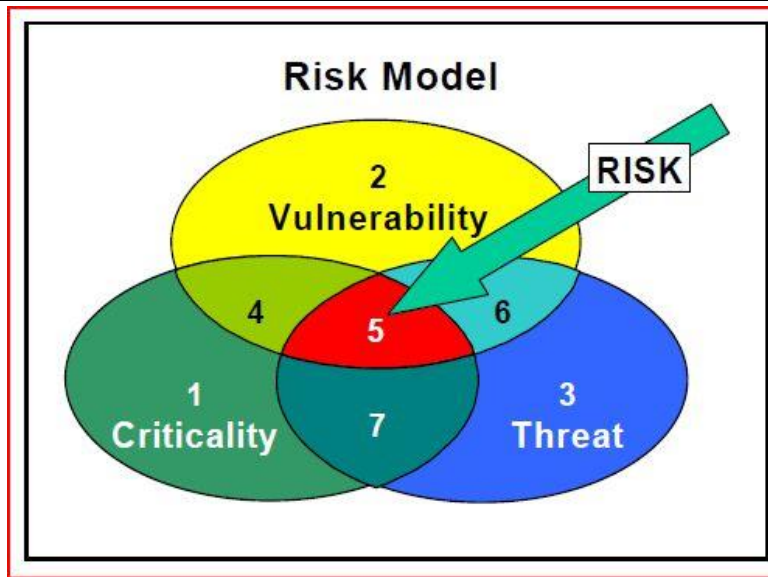
In this environment, scarcely a week can pass without news of a security breach occurring that exposes sensitive information of a significant number of individuals (cf. Privacy Rights Clearinghouse, 2013). Such breaches allow non-authorized individuals to alter data or render a given system unavailable to its legitimate users. In late 2013, it was revealed that Target suffered a breach that exposed sensitive information from customers (cf. Eversley & Hjelmgard, 2013). The troubled 2014 roll-out of the Healthcare.gov site has also featured significant gaps in the website's security posture (Whitney, 2014). Outcomes such as these are increasingly likely in a world where more and more valuable information resources are placed in systems that have any number of identifiable vulnerabilities in an environment replete with threat agents that are increasing exponentially in terms of their motivation, sophistication, and willingness to attack. The seriousness of these issues was made clear by the massive Sony breach of 2014, which involved the release of significant amounts of personally identifiable information (e.g., actors' and employees' social security numbers) and intellectual property (e.g., complete movies, scripts) (cf. The Economist, 2014). As such, it seems reasonable that firms are increasingly paying attention to information security; in fact, a variety of major U.S. firms (e.g., John Deere, JP Morgan-Chase, PepsiCo Inc.) have sought chief information security officers (CISO) and other credentialed security personnel (Damouni, 2014).

The intersection of valuable information assets online, vulnerabilities in systems, and threat agents with intent and capability are the components of information risk (Figure 1). As vulnerabilities are discovered and more dangerous threats are identified, information assets' exposure to risk naturally increases (U.S. Department of Defense, 2000; cf. Dutta & McCrohan, 2002). We should clarify that what we describe here is not "risk" as is often viewed in the system development literature (which focuses on the risk of failures in the development effort), but risk to the information assets for which systems are developed in the first place. This is an important distinction because at least one European organization suggests that appropriate risk management principles are not effectively applied when the topic turns to cyber-risks (Graham, 2013). Given the current threat environment, it should not be surprising that the risk to data and systems has become increasingly visible.

One plausible explanation for why these sorts of breaches are becoming near universal is that systems development practices and methodologies may not yet have caught up with the realities inherent in systems that are connected globally and always on, always connected, and always available. This situation is analogous to problems that occurred when information systems did not have appropriate validity checks specified in their requirements and, subsequently, were built into implemented systems. For example, consider the occurrence of unreasonably high bills or account balances as in the case of an extraordinary water bill for \$4,704.88 (Neumann, 1995) or a phenomenal checking account balance of \$924,844,208.32 (Neumann, 1996). Systems development practices are more likely to avoid these errors today. It is now common to include validity checks, such as reasonableness and range tests, when specifying requirements, whereas such controls were not necessarily specified when manual systems were first converted to computer-based systems. We suggest that similar attention should be applied to concerns regarding the security of organizational information, and that, at this writing, it appears this is often not the case.

A variety of organizations have promulgated security standards for organizations (see Table 1 for a sample). This said, at the heart of any discussion regarding information security stands the importance of three basic requirements: confidentiality (i.e., only those with appropriate privileges should see restricted information), integrity (only those with appropriate privileges should be able to modify restricted information) and availability (all individuals with appropriate privilege should have ready access to restricted information) (National Institute of Standards and Technology, 2004a; cf. ISACA, 2012). These requirements are often referred to as the CIA triad (cf. Perrin, 2008). Other perspectives on security exist: for example, consider access control via identification, authentication, and authorization (Zviran & Erlich 2006), or authentication, authorization, and accounting (cf. de Laat, Gross, Gommans, Vollbrecht, & Spence, 2000). CIA is an over-arching perspective that includes these as a means of achieving the

three basic information security requirements. Given the broad focus and widespread recognition of CIA, we use the NIST standards with CIA as a basis for our discussion that follows.



Legend for numbered segments of risk model.

- 1 – Critical assets (information, systems, programs, people, equipment or facilities) for which there is no known vulnerability and no known threat exposure.
- 2 – Vulnerabilities in systems, programs, people, equipment or facilities that are not associated with critical assets and for which there is no known threat exposure.
- 3 – Threat environment for which there is no known threat to critical assets or access to vulnerabilities (or vulnerability information).
- 4 – Critical assets for which there are known vulnerabilities, but no known threat exposure.
- 5 – Critical assets for which there are known vulnerabilities and threat exposure.
- 6 – Threat has acquired specific knowledge and/or capability to exploit a vulnerability although not a critical asset vulnerability.
- 7 – Critical asset for which there are no known vulnerabilities, but there is exposure to a specific threat.

**Figure 1. Risk Viewed as the Intersection of Threats, Vulnerabilities, and Valuable Information Assets**

Hence, one way to assess the validity of our explanation described above for the prevalence of security breaches would be to investigate the extent to which systems professionals' education prepares them to address the CIA of data and systems. A growing consensus in the security field suggests that security planning should be a prime consideration even in the earliest phases of system development (cf., National Institute of Standards and Technology, 2004b), which the system development lifecycle (SDLC) represents. Systems analysis and design courses are central to IS curricula, and the IS 2010.6 standard for systems analysis and design suggests developers should "incorporate principles leading to high levels of security...from the beginning of the systems development process" (Topi et al., 2010, p. 51). Thus, it's relevant to assess the extent to which this is true in courses where systems professionals learn what to do during the SDLC, particularly the early stages. Typically, relevant courses in MIS curricula for developing system professionals are systems analysis and design courses.

**Table 1: Sampling of Organizations with Some Emphasis on Information Security Risk Management**

Standard	Sponsoring organization	Organizational website
COBIT	ISACA	isaca.org
NIST	U.S. Federal Government	csrc.nist.gov
COSO	Treadway Commission	coso.org
ISO/IEC	International Standards Organization	iso.org
ITIL	Information Technology Infrastructure Library	itil.org
FERMA*	Federation of European Risk Management Associations	ferma.eu

Note: FERMA as an organization is focused on risk more broadly, of which cyber risk is one part.

In this paper, we examine the extent to which information security is included in the teaching of university systems analysis and design courses. More specifically, we review relevant artifacts to develop an initial answer to our question: that is, we closely examined the textbooks most commonly used to teach systems analysis and design (SA&D) courses. We do not assert that MIS faculty use only these sources; however, we do assert that examining the content of widely adopted SA&D texts enables an initial assessment of the emphasis on information security in typical SA&D courses. Because the various security standards generally cover the same ground, we first outline one of these standards with widely available (free and online) prescriptions relevant to the system development lifecycle and compare its precepts with the material on security in several well-known systems analysis and design texts. The results should assist in understanding the extent to which information security is or is not included in the texts, and, by extension, what is actually emphasized when security-relevant material in systems analysis and design texts is taught. Additionally, we also examine at what point in the SDLC is security introduced in current systems analysis and design texts.

To preview our findings, our results suggest that the material on security included in SA&D textbooks is somewhat limited and focuses typically on the SDLC's later stages. Indeed, one could strongly suggest that this material is, as it stands, inadequate to address the concerns raised in either the security standards or in practice. We conclude by discussing our findings and offering suggestions for how this situation might be remedied.

## II. STANDARD WE CHOSE FOR REVIEW

We began by reviewing one of the commonly known standards for information security (at least in the US): the National Institute of Standards and Technology (NIST) special publications 800 series of documents, which describe security policies, procedures, and guidelines. The 800 series was established in 1990 to provide a separate identity for IT security publications (National Institute of Standards and Technology, 2007) and covers topics such as cloud computing (800-145 and 800-146), risk management (800-37), mobile phones and PDA security (800-124) and clearing storage media of sensitive information (800-88). We point out that, while NIST standards were developed by and for the U.S. Federal Government, they are quite consistent with other standards covering similar topics (e.g., ISACA, 2012; Committee of Sponsoring Organizations, 1992; Cartledge et al., 2007) and are often applied in the private sector. Further, security certification regimes (e.g., International Information Systems Security Certification Consortium (ISC<sup>2</sup>)), often draw from these standards in setting certification examinations, and there is significant isomorphism in the relevant standards (e.g., COBIT and NIST both emphasize CIA; indeed, CIA is part of the COBIT definition of information security; cf. ISACA, 2012).

We found the most relevant NIST standards for our particular exercise include NIST 800-37 Revision 1 (*Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*), NIST 800-39 (*Managing Information Security Risk: Organization, Mission and Information System View*) (National Institute of Standards and Technology, 2011), NIST 800-30 (*Guide for Conducting Risk Assessments*) (National Institute of Standards and Technology, 2012), and NIST 800-64 Revision 2 (*Security Considerations in the System Development Life Cycle*) (National Institute of Standards and Technology, 2008c), so we use these for our assessment.

Taken together, the standards we review here provide guidelines for applying an integrated framework for risk management when developing information systems in organizations. This includes security categorization, security control selection, implementation, assessment, and monitoring. The underlying emphasis of the NIST standards is on managing information system security risks in a manner consistent with a given organization's mission, business objectives, and overall risk strategy, which is accomplished by ensuring necessary security controls are integrated into enterprise architecture and SDLC processes to encourage the use of appropriate risk-management strategies (National Institute of Standards and Technology, 2010).

Importantly, the NIST risk-management framework assumes that information technology and information assets are among organizations' most valuable assets. Of significance to a comprehensive security program is the notion of return on security investment (ROSI) (cf., Mehan & Krush, 2009). To ensure that ROSI is achieved (i.e., that the most valuable assets receive the highest level of protection) and that inappropriately large sums are not spent on protecting assets whose value does not justify the expense, it is critical that organizations correctly appraise the value of various information assets they need to protect. Organizations own critical assets they need to protect; should those assets be breached, the organizations will suffer accordingly. Further, organizations operate in a space where there are known threat agents with some degree of sophistication, motivation, and resources that they could use to attack defenses surrounding these critical information assets. Finally, organizations have a wide range of possible vulnerabilities (e.g., unpatched systems, etc.) that may be present in their systems.

Estimating risk begins with characterizing a system, which involves documenting such things as its purpose, scope, functions, boundaries, and information processed (Howard, 2013). Characterizing can be a fairly involved exercise, depending on the complexity of the system and the nature of the information being processed. However, similar assessments are done routinely as part of the SDLC, wherein the project scope, feasibility, operating environment, description of the proposed system (including types of information to be processed, and available inputs to, and required outputs from, the system) and other managerial issues are initially assessed (cf., Hoffer, George, & Valacich, 2014). When an organization understands the value of its information assets, it has access to the basic information required to begin categorizing the information system it needs; that is, it can assess what impact a breach in confidentiality, integrity, and/or availability of organizational information would have, which it can express in terms of its mission, reputation, and/or finances. The organization can then assess its assets' values, threats, and vulnerabilities (and, as a consequence, risk) as described in NIST 800-64.

Obviously, assessing risk means first weighing the value of the information to be processed and the impact that would result from a breach. Information in a system can be mapped to various information types processed as described in NIST 800-60 (National Institute of Standards and Technology, 2008a; 2008b) (which is in the initiation phase of the SDLC). Table 2 summarizes the security objectives of confidentiality, integrity, and availability, and the potential impacts if these were breached; with this in hand, one can evaluate the importance of, and therefore appropriate level of controls for, one's information assets.

**Table 2: Security Objectives and Impact Definitions from FIPS 199 (National Institute of Standards and Technology, 2004a)**

Security objective	Potential impact		
	Low	Moderate	High
<b>Confidentiality</b> Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have a <b>limited</b> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a <b>serious</b> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a <b>severe or catastrophic</b> adverse effect on organizational operations, organizational assets, or individuals.
<b>Integrity</b> Guarding against improper information modification or destruction, which includes ensuring information non-repudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a <b>limited</b> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a <b>serious</b> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a <b>severe or catastrophic</b> adverse effect on organizational operations, organizational assets, or individuals.
<b>Availability</b> Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a <b>limited</b> adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a <b>serious</b> adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a <b>severe or catastrophic</b> adverse effect on organizational operations, organizational assets, or individuals.

The assessed security impact categories (low, moderate, high) have implications for system development and acquisition. Once an organization knows that valuable information is in play, it can review threats and vulnerabilities to better understand the risk level, for which NIST 800-30 (*Guide for Conducting Risk Assessments*) is useful. Conducting a risk assessment involves identifying threats (sources and events), vulnerabilities and predisposing conditions (e.g., constraints on information handling, technology requirements, environmental concerns), likelihood of occurrence, and likely impact (see Table 2).

From reviewing various NIST publications, we developed three key understandings, which are consistent with other security standards (e.g., those in Table 1). First, security should be a key part of the SDLC from the point of system initiation because adding security controls later in the SDLC (after the system architecture is fairly complete) in the form of patches would be expensive, perhaps prohibitively so (cf. Boehm, 1981). Second, specifically identifying goals for information confidentiality, integrity, and availability early on during the SDLC is important. From these goals, one can derive appropriate controls to implement an acceptable level of security in a cost-effective manner. Third, information systems should be categorized in the initiation phase (cf., National Institute of Standards and Technology, 2004a, 2004b) of the SDLC (Table 3). This means assessing the impact (e.g., a low, moderate, or high) in terms of disrupted operations, financial losses, or loss of life that a breach of confidentiality, integrity, or availability would have were it to occur (see Table 2). The system is then designed and built/bought with this security categorization in mind while security controls are selected and built into the system in later phases. In other words, attention to information security needs to be an integral element of the SDLC from the earliest phases so that it is incorporated into every aspect of information system development, which is consistent with the IS 2010.6 for SA&D courses.

One can assert that a focus on security early in the SDLC is particularly appropriate for systems that will be functioning while attached to the Internet, which is to say the vast majority of new systems being built. While the Internet is a tremendous resource for facilitating organizations and individuals to connect, the design of its architecture has significant limitations that create serious concerns regarding security. To wit:

*While the Internet represents a robust global information system, one needs to recall that it was originally devised with an emphasis on availability (i.e., the network and relevant information should be available to those with legitimate need). Confidentiality (i.e., that a given store of data should only be seen by those with legitimate authority or privilege to do so) and integrity (i.e., data should be changeable only by those with legitimate authority to do so) were not emphasized in the design of the Internet. When the network was exclusively the domain of government, this may have been acceptable. However, with the opening of the infrastructure to the world at large, and given the sensitivity of the data transmitted and criticality of the systems it supports, concerns about these vulnerabilities are now rising to the forefront. Further, the openness of the architecture itself creates vulnerabilities that may lead to denial of availability (e.g., through DDOS attack). When these vulnerabilities come into contact with those who may not share the same beliefs about "appropriate" use and who may have reason to do harm, these concerns become even more salient. (Salisbury et al., 2011, p. 298)*

With this understanding, we focused on reviewing textbooks, which we discuss in Section 3.

### III. SELECTION AND ASSESSMENT OF TEXTBOOKS

From reviewing three NIST standards documents, we created a rubric to review texts that are commonly used in systems analysis and design classes. The rubric (see Table 4) first identifies the text, followed by some descriptive information (viz., number of chapters and pages). Next, we used the rubric to assess (as surrogates for each textbook's precedence of security) the earliest SDLC phase in which it the textbook indicates that security requirements should be taken up, whether or not the CIA triad is discussed (as a surrogate for emphasis on security), and whether security is seen as a functional or non-functional requirement. We also noted any security standards we found referenced in the texts. We put any insights not readily fitting one of our headings in the comments column.

We generated an initial, short list of texts by consulting faculty who teach the SA&D course at our university. We then contacted authors and publishers to flesh out our list: we asked them for the latest editions of the main textbooks on our list and for the names of any titles we missed. Finally, we submitted an earlier draft of our manuscript to the each textbook's authors for their comments, and presented it at a conference to obtain further feedback. Table 4 lists the books we reviewed, along with what we believed to be relevant security attributes.

**Table 3: IT Security in the SDLC as Described in NIST 800-64 (NIST, 2004c)**

	Initiation	Acquisition / development	Implementation	Operations / maintenance	Disposition
<b>SDLC</b>	<ul style="list-style-type: none"> <li>• Needs determination:                             <ul style="list-style-type: none"> <li>▪ Perception of a need</li> <li>▪ Linkage of need to mission and performance</li> <li>▪ Objectives</li> <li>▪ Assessment of alternatives to capital assets</li> <li>▪ Preparing for investment review and budgeting</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Functional statement of need</li> <li>• Market research</li> <li>• Feasibility study</li> <li>• Requirements analysis</li> <li>• Alternatives analysis</li> <li>• Cost-benefit analysis</li> <li>• Software conversion study</li> <li>• Cost analysis</li> <li>• Risk management* plan</li> <li>• Acquisition planning</li> </ul>	<ul style="list-style-type: none"> <li>• Installation</li> <li>• Inspection</li> <li>• Acceptance testing</li> <li>• Initial user training</li> <li>• Documentation</li> </ul>	<ul style="list-style-type: none"> <li>• Performance measurement</li> <li>• Contract modifications</li> <li>• Operations</li> <li>• Maintenance</li> </ul>	<ul style="list-style-type: none"> <li>• Appropriateness of disposal</li> <li>• Exchange and sale</li> <li>• Internal organization screening</li> <li>• Transfer and donation</li> <li>• Contract closeout</li> </ul>
<b>SECURITY CONSIDERATIONS</b>	<ul style="list-style-type: none"> <li>• Security categorization</li> <li>• Preliminary risk assessment</li> </ul>	<ul style="list-style-type: none"> <li>• Risk assessment</li> <li>• Security functional requirements Analysis</li> <li>• Security assurance requirements Analysis</li> <li>• Cost considerations and reporting</li> <li>• Security planning</li> <li>• Security control development</li> <li>• Developmental security test and evaluation</li> <li>• Other planning components</li> </ul>	<ul style="list-style-type: none"> <li>• Inspection and acceptance</li> <li>• Security control integration</li> <li>• Security certification</li> <li>• Security accreditation</li> </ul>	<ul style="list-style-type: none"> <li>• Configuration management and control</li> <li>• Continuous monitoring</li> </ul>	<ul style="list-style-type: none"> <li>• Information preservation</li> <li>• Media sanitization</li> <li>• Hardware and software disposal</li> </ul>

\* Risk management in this context refers to risk associated with the development and not computer security or system technical risk.

Because there is variance between texts in terms of the number of SDLC phases, we decided to “normalize” all of the textbooks we assessed around the NIST five-phase SDLC framework (see SDLC phase column in Table 4). We list the lifecycle phase each textbook follows, in brackets, by the corresponding NIST phase. We believe that this enables us to make reasonable assertions across the range of texts. While we adopted NIST as an organizing scheme for our brief review, we also reviewed the texts for mention of any of the other security standards or any tenets of information risk management (e.g., information criticality/sensitivity, threat assessment, vulnerability assessment, control assessment). We also reviewed the textbooks’ indices and their detailed tables of contents. Where we found terms that led us to believe it possible that security was being discussed, we reviewed the content on those and adjacent pages.

While we primarily used NIST for our review, for our purposes, we could have adopted any of the fairly well-known standards (e.g., COBIT, COSO, etc.) because each includes various means by which information security risk can be assessed and then mitigated by using of various controls. Our concern is not with *which* standard is being used; it is whether *any* standard is being extensively used in SA&D texts to identify the criticality of information assets and, depending on this assessment, specify appropriate and cost-effective requirements for controls in proposed systems early in the SDLC.



**Table 4: Texts and Assessments**

SDLC phase (text (NIST)) security first indexed in (page)?	CIA triad discussed?	Security standards mentioned	Security control		Other comments
			Functional	Non-functional	
<b>Hoffer, J. A., George, J. F., &amp; Valacich, J. S. (2014). Modern systems analysis and design (7th ed.). Upper Saddle River, NJ: Pearson Prentice Hall. (14 chapters, 526 pages)</b>					
Page 13 in the overview; in terms of SDLC in design/acquisition (acquisition/development) (p. 335).	No	COBIT ITIL Microsoft SDL		X	Introduces Microsoft security development lifecycle in introductory chapter on SA&D environment. Discussion of security in terms of information security (integrity) in the context of the SDLC occurs later in the book with the mention of data integrity. Security also discussed in implementation and testing. COBIT and ITIL noted in discussion of data integrity.
<b>Kendall, K. E., &amp; Kendall, J. E. (2014). Systems analysis and design (9th ed.). Upper Saddle River, N.: Pearson Education. (16 chapters, 518 pages)</b>					
Analysis (acquisition/development) (p. 193).	No	None (ISO mentioned but seems to reference usability standards and the UNICODE character set.)		X	Security focus in the analysis phase is somewhat limited, though the need for secure applications, security in the cloud, BYOD, and security when working with SaaS providers (as examples) are discussed. Authors discuss the importance of something analogous to system categorization as early as page 88. However, they appear to separate security planning from SA&D: they describe security planning as "a project in and of itself and must be managed as such..." (p 88). Security partitioning appears to be the primary focus on security as we might view it. Integrity constraints are discussed with database design. The major discussion of security, including privacy and disaster recovery, is near the end of the book in the context of quality assurance and implementation (chapter 16).
<b>Rosenblatt, H. J. (2014). Systems analysis and design (10th ed.). Boston: Course Technology Cengage Learning. (12 chapters, 668 pages)</b>					
Systems analysis (acquisition/development) (p. 132)	Yes	ISO		X	Security is very briefly defined as early as page 132. CIA triad appears to not be discussed in terms of overall lifecycle, appearing near the end of the text (pages 524-542), in a section on security and risk management (discussed after implementation). ISO mentioned on pages 389 and 451-452.
<b>Dennis, A., Wixom, B. H., &amp; Roth, R. M. (2015). Systems analysis and design (6th ed.). Hoboken, NJ: John Wiley and Sons. (Note: online version reviewed) (14 chapters, 472 pages)</b>					
Requirements determination (acquisition/development) (p. 108)	No	PCI HIPAA ISO		X	The importance of identifying non-functional requirements (security being one of these) is noted fairly early as something that will affect decisions in the design phase. Security controls are discussed on page 249 (chapter 8); PCI, HIPAA and ISO compliance are also discussed in this general area; however, these appear more as something mainly to make operations staff aware of potential risks. Topics such as encryption, certificate authorities, and virus protection are described as well, and appear in the section "Architecture design".
<b>Dennis, A., Haley Wixom, B., &amp; Tegarden, D. (2012). Systems analysis and design with UML version 2.0: An object-oriented approach, 4th ed., Hoboken, NJ: John Wiley and Sons, Inc. (Note: A new edition is anticipated in 2015). 13 chapters, 592 pages)</b>					
Requirements determination (acquisition/development) (p. 113)	No	COBIT HIPAA ISO		X	Relevant legal mandates (e.g., Sarbanes-Oxley) noted as important to consider. ISO 9000 and COBIT noted briefly on page 113; access controls are discussed on page 464, encryption and authentication are described on pages 500 and 501; virus protection on page 503.
<b>Satzinger, J. W., Jackson, R. B., &amp; Burd, S. D. (2015). Systems analysis and design in a changing world (7th ed.). Boston, MA: Course Technology/Cengage Learning. (14 chapters, 484 pages)</b>					
Requirements (acquisition/development) (p. 46)	No			X	CIA not specifically described as such but fairly extensive discussion of security and integrity controls appear in Chapter 6 (Foundations for Systems Design).
<b>Valacich, J. S., George, J. F., &amp; Hoffer, J. A. (2015). Essentials of Systems Analysis &amp; Design (6th ed.). Hoboken, NJ: Pearson Education. (10 chapters, 418 pages)</b>					
Design/acquisition (acquisition/development) (p. 202).	No			X	Relatively short book; security not discussed much; briefly in analysis, and design and again in implementation and testing. Data integrity is discussed, but mainly in terms of input validation and processing controls.
<b>Whitten, J. L., &amp; Bentley, L. D., (2007). Systems analysis and design methods (7th ed.). Boston: McGraw-Hill. (20 chapters, 747 pages)</b>					

**Table 4: Texts and Assessments**

SDLC phase (text (NIST)) security first indexed in (page)?	CIA triad discussed?	Security standards mentioned	Security control		Other comments
			Functional	Non-functional	
20/747 Initiation (initiation) (p. 19)	No			X	Security is briefly discussed (three paragraphs) in the introductory chapter. The focus is on business continuity in the event of breach or disaster and on privacy. It is also noted in the third chapter in a figure listing potential system problems. Data integrity discussed in chapter 14 (database design). Another discussion (six paragraphs near the end of the text) focuses on authentication and authorization in user interface design.

**IV. FINDINGS**

Interestingly, the majority of these SA&D textbooks do not place much emphasis on security. Instead, they often only cursorily mention it, and at least one textbook doesn't introduce it until the acquisition or even the implementation phase, by which time it may be extremely difficult to implement effective security controls without prohibitive cost (cf., Boehm, 1981). Another interesting finding is that only one of the books we reviewed directly mentions the concepts of confidentiality, integrity, and availability, although at least one other made mention of concepts that would have similar meaning.

One text (Valacich et al., 2012) appears to specifically mention security three times, all in the implementation and testing phase (note: implementation as described by NIST), though this text does also discuss data integrity as a concern. This was a fairly common theme among the majority of books. In instances where security was mentioned, it is typically featured toward the middle to latter portion of the SDLC, even in books that do emphasize the importance of security controls:

*Sometimes, the analyst is concerned about events that are important to the system but do not directly concern users or transactions... During analysis, the analyst should temporarily ignore these events...At this stage, the analyst should focus only on the functional requirements. ...Most of these physical system events involve system controls, which are checks or safety procedures put in place to protect the integrity of the system. ...These controls are important to the system, and they will certainly be added to the system during design.* (Satzinger et al., 2015, p. 79)

Another text in our sample singles out the Sarbanes-Oxley Act, COBIT, ISO 9000, and capability maturity model as topics that affect the functional and nonfunctional requirements in the requirements determination portion of the systems analysis process. The textbook states:

*The Sarbanes-Oxley Act, for example, mandates additional functional and nonfunctional requirements. These include additional security concerns (nonfunctional) and specific information requirements that management must now provide (functional). When developing financial information systems, information system developers should be sure to include Sarbanes-Oxley expertise in the development team.* (Dennis et al., 2012, p. 113)

Further, another textbook discusses security as non-functional requirements:

*The IIBA (International Institute of Business Analysts, Guide to Business Analysis Body of Knowledge) defines (nonfunctional requirements) as 'the quality attributes, design, and implementation constraints, and external interfaces which a product must have.' Although the term 'nonfunctional' is not very descriptive, this requirement category includes important behavioral properties that the system must have, such as performance and usability.... Nonfunctional requirements are primarily used in the design phase when decisions are made about the user interface, the hardware and software, and the system's underlying architecture. Many of these requirements will be discovered during conversations with users in the analysis phase, however, and should be recorded as they are discovered.* (Dennis et al., 2012, p. 107)

These particular texts raise issues that at least suggest an emphasis on security fairly early in the SDLC, although this is more toward the notion of seeing security as a non-functional requirement and regulatory compliance (e.g., Sarbanes-Oxley) rather than focusing on a risk management perspective as pertains to information security. In fact,

one text does assess the potential for information risk and impacts on confidentiality, integrity, and availability explicitly, although the primary focus on this was found toward the latter part of the SDLC (cf. Rosenblatt, 2014).

Another item that we noticed when assessing current SA&D textbooks against NIST standards is that disposition of obsolete or uninstalled hardware and software does not appear to be discussed even in passing. This is something that should be at least mentioned in that archival of important data and disposal of hardware have implications for confidentiality and availability. Indeed, Garfinkel and Shelat (2003) demonstrate this in a clear fashion in their study of disk sanitization practices: they obtained disposed-of hard drives from a variety of sources and checked to see whether they still contained readable data, and found that approximately one third of the drives contained confidential information that should have been erased prior to disposal.

## V. DISCUSSION

One of the key points of divergence between the NIST standards we reviewed and the majority of SA&D texts is a lack of emphasis on understanding information risk (see Figure 1), particularly confidentiality, integrity, and availability issues associated with a system early in the SDLC. Put simply, many texts do not see assessing the impact of a breach as an important step early in the SDLC. Further, we found fairly limited discussion of specific end-of-lifecycle activities that may be important to ensure information confidentiality, such as destroying records (although Kendall and Kendall (2014) note media shredding (or media sanitization) (as discussed in NIST 800-88) (National Institute of Standards and Technology, 2014).

Although not found across the board, a couple of newer books discuss information security as we focus on it. For example, Rosenblatt (2014) explicitly discuss CIA. And, in their discussion of the systems development environment, Hoffer, George, and Valacich's (2014) discuss the notion of the Microsoft security development lifecycle, which was not in the previous edition. We applaud their introducing this into the discussion, in particular their emphasis on having "security become part of the development process from the beginning and not suddenly appear at the end of the SDLC". While this is important, note that the presentation of this perspective and methodology appears to focus on developing secure products, which would clearly be a concern for a software developer, rather than developing systems (as one example) for a bank that is looking at threats to the CIA of its own information assets and the potential impacts (e.g., financial, legal, reputational) to that organization in the event of an information breach.

Given limited evidence of the importance of security in SA&D textbooks, one implication of our effort suggests that security needs to be elevated both in emphasis and precedence in the SA&D course. For example, authors and instructors in systems analysis and design courses often categorize requirements into functional (something the system does) and non-functional (something the system is required to have—constraints) (cf. Satzinger et al., 2012). The distinction between functional and non-functional requirements is consistent with an approach to systems development that emphasizes understanding what the system is required to do before designing how it should meet the requirements. The intent of the distinction is not to imply that non-functional requirements are less important or should receive less attention than functional requirements. Our findings indicate, though, that this distinction clearly focuses more attention during requirements analysis on functional requirements, which do not typically include security in textbooks used to teach systems analysis and design.

Although security has traditionally been characterized as a non-functional requirement, some research suggests that security should, in some instances, be viewed as a functional requirement, in particular with respect to inter-organizational systems (cf., Baskerville, Rowe, & Wolff, 2012). Baskerville et al. challenge the assumption that there is necessarily an inverse relationship between security and functionality (in particular in inter-organizational systems that require integration) and identify environmental dynamism as a key moderator of this relationship.

This identification of security as a functional requirement also seems particularly appropriate for systems that require security functions. For especially sensitive types of information (e.g., social security and financial or medical records), we assert that security is, by definition, a functional requirement since security functions must be met before any other functions may be performed. Indeed, certain systems cannot legally operate (i.e., perform any functions) in the absence of security protections for the confidentiality and integrity of personally identifiable information. The impact of a breach of confidentiality, integrity, or availability (assessed in accordance with appropriate security standards) would also seem relevant. In environments in which a breach of one or more of either confidentiality, integrity, or availability would have moderate or high impact, one could assert that the operating environment of an associated information system is "dynamic", to apply the term that Baskerville et al. (2012) use.

We did not collect data indicating whether similar differences in attention occur in practice. As such, we cannot discuss whether the functional vs. non-functional distinction should be re-examined in light of more rapid

development approaches that blur the difference between analysis and design phases; however, other papers could focus on this topic<sup>1</sup>.

Returning to the notion of system risk factors, the interrelated nature of systems and the advent of the Internet may mean that vulnerabilities and threats cannot be readily assessed, which makes risk less definable. One could readily assess the impact of a breach, but may not be able to readily assess the threat environment or perhaps even vulnerabilities. This is even more of a concern due to many-to-many relationships between users and systems. Indeed, the potential for breach of data confidentiality, integrity, and availability involving these systems that have no apparent interrelationship was made clear in a dramatic fashion by the experience of Matt Honan, a technology writer for *Wired* magazine. Mr. Honan's misfortune was caused in part by the fact that he used both Amazon and Apple iCloud services. Information (viz., the last four digits of a credit card number) deemed non-sensitive by Amazon turned out to be values that Apple used as identity verification. By working back and forth between Amazon and Apple, hackers were able to access his iCloud account and assume control of all his Apple digital devices (Honan, 2012).

The issues raised here will become only more relevant with the advent of "bring-your-own-device" (BYOD) initiatives (cf. Office of the President, 2012; Kendall & Kendall, 2014), wherein employees are enabled to use their own smartphones, laptops, and other devices at work. This, of course, implies that entry points into various systems will be necessary, which exposes various systems to a wider range of threats due in no small part to vulnerabilities present in these devices. The use of devices that are portable feature operating systems with updates controlled by third-party telecommunications carriers and that are often taken into non-controlled environments and sometimes lost will create an ongoing challenge for identifying, quantifying, and controlling for risks to information security (Kopytoff, 2012).

More aggressive digitization of various extant systems (e.g., the "smart" utility grid or electronic health records) will also lead to a greater need to assess impact of information breaches and put appropriate controls in place. For example, a report from the U.S. Office of the Inspector General (cited in Clune, 2011) found a lack of IT security controls during audits at Medicare contractors, state Medicaid agencies, and hospitals in several U.S. states. This is troubling given the sensitivity of the information contained in health records. To remedy a breach or vulnerability in these settings after the fact would be quite expensive. For another example, there are growing concerns surrounding the control devices for industrial systems (cf., Larkin, Lopez, Butts, & Grimaila, 2014), which include power-generation facilities. The impact of a breach of integrity or availability in these sorts of systems would be problematic (Salisbury et al., 2011), and the cost of after-the-fact remedies again would be prohibitive. Hence, considering impact in a manner analogous to that suggested by NIST standards during system development would seem appropriate.

These issues noted, there is some movement toward enhancing the emphasis on security throughout the SDLC. The International Information Systems Security Certification Consortium (ISC<sup>2</sup>), a well-known not-for-profit that specializes in information security education and certifications, offers a certified secure software lifecycle professional (CSSLP) certification (cf. National Institute of Standards and Technology, 2008d), which places significant weight on public standards, such as NIST, that emphasize designing systems for security throughout their lifecycle. Other certificates offered by ISC<sup>2</sup> include the *Certified Information Systems Security Professional* (CISSP), one of the more advanced and comprehensive security certifications. Other standards and standards organizations mentioned here feature similar foci.

## VI. CHALLENGES FOR INTEGRATING THESE CONCEPTS INTO SA&D PEDAGOGY

Clearly, we believe that we have identified a disconnect between the importance of information security in practice and its importance in material used to prepare information systems practitioners. Information security is of critical concern in practice and yet core SA&D courses in the MIS field seem to have limited interest in this topic, and, indeed, place little emphasis on information security early in the SDLC.

We do not wish to be overly critical: SA&D courses already have a very full plate, and it is reasonable to assert in this light that our recommendations in Tables 5a and 5b are ambitious, to put it mildly. However, it is not only SA&D courses that are full, but the curriculum of many IS programs. At our university, the MIS major is (along with accounting) generally the fullest in terms of required classes required for completion. We are inclined to believe that our university is not an anomaly in this matter, especially given that the IS 2010 model curriculum (Topi et al., 2010) suggests that the typical AACSB-accredited North American business school would have 24 credit hours in the information systems core and electives. The major at our university currently has 27 credit hours, which includes the

<sup>1</sup> Our thanks to Stephen Burd (co-author of one of the reviewed texts) for raising this issue.

business school core IS course IS 2010.1. Hence, it seems important to take great care before advocating the position that we simply need another course. Students at our university can take an elective on security (with content similar to what is suggested in the IT audit and IT risk management electives from IS 2010), but they can also satisfy their electives (6 credit hours) with other courses.

While we primarily hope to raise awareness about the limited emphasis on information security, we offer some suggestions that may be useful to integrate this content more readily into SA&D courses. With the concerns we have noted, we submit that a possible answer already lies in some of our earlier discussion on these matters.

First, we revisit the SDLC model advocated in NIST 800-64 (National Institute of Standards and Technology, 2008c). As we note earlier, the model proposed in 800-64 advocates a fairly early focus on understanding the security implications with respect to information and data proposed to be processed by an anticipated system. Given that the vast majority of the necessary knowledge about these matters should already be captured as part of system development, it seems to us a relatively straightforward matter to include system characterization, system categorization, and risk assessment as learning content to be adopted from the beginning of the SDLC, which would be consistent with the learning objective from IS 2010.6 that security principles should be incorporated from the beginning of the SDLC. Controls are already covered reasonably well, so the only changes there would be to map the importance of the information assets onto appropriate controls to protect these things.

Second, we believe that information security and risk management should be a focus of SA&D textbooks (and courses) from the beginning of the SDLC. This is consistent both with IS 2010.6 and with good practice as Boehm (1981) describes; leaving something this important to the latter stages of the SDLC invites a lack of necessary emphasis and leaves open the potential for expensive rebuilding of system elements.

At this point, we note that many of the topics we mention here are discussed in the elective IT audit and security and risk management courses from IS 2010 (which refer to ISACA and COBIT); the course we currently offer at our university covers these topics, too. There is coverage of these topics in the data and information management, IS strategy, enterprise systems, and infrastructure courses, too, though we assert that this is limited. However, we believe that security is no longer something that can be seen as a minor component or as elective, and many of the topics currently seen as part of an IT audit course should receive significant attention in courses comprising the IS core. Further, if systems are going to eventually be *audited* given certain standards, it would seem reasonable to suggest that they be *built* with those standards in mind. As such, we propose that incorporating CIA assessment, requirements specification, and design specification into IS curricula be directed at the systems analysis and design course in the 2010 standard IS curriculum (IS2010.6). As the standard curriculum (Topi et al., 2010) specifies, this course is primarily focused on analyzing and documenting business requirements and on converting these requirements into detailed systems requirements and high-level design specifications (e.g., mock-ups of forms, reports, HCI, and other user interface components), not on internal design or system implementation design.

Tables 5a and 5b show course objectives, topics, and proposed security coverage for major SDLC phases emphasized in this course. We use the three SDLC phases from Table 3 related to SA&D courses, except that we split acquisition/development into the two phases (i.e., analysis/functional requirements specification and logical system design). Several IS2010.6 objectives and topics are not based on any specific SDLC phase. Instead, they involve pre-project activities, such as clearly defining problems, opportunities, or mandates that initiate projects and identify opportunities for IT-enabled organizational change. They also cut across SDLC phases such as “manage information systems projects using formal project management methods” and “fundamentals of IS project management in the global context”. Thus, we identify these objectives and topics in Tables 5a and 5b as spanning multiple phases in the SDLC (see footnotes in these tables). We note that the only security-relevant objective that we identify as spanning multiple phases is the following broad statement about both security and user experience: “incorporate principles leading to high levels of security and user experience from the beginning of the systems development process”. Only one topic related to security is included in the topics for IS 2010.6; a sub-topic in analysis and specification of system requirements.

The part of the broadly stated objective related to security is consistent with our proposal; however, IS2010.6 provides limited further guidance. Thus, we provided more specific proposals for security-relevant content (including some elements drawn from NIST 800-64, the NIST pamphlet “Information Security in the SDLC” and other sources) in the appropriate SDLC phase in Tables 5a and 5b. The reader will note that we have also included for consideration NIST 800-64 phases “operations/maintenance” and “sunset (disposition)” as shaded columns. Operations/maintenance is the portion of the lifecycle wherein the system is functioning and performing its intended tasks; it has traditionally been considered as part of the SDLC (e.g., Hoffer, George and Valacich, 2014) and we included it here. Sunset (disposition) refers to the steps whereby the transition occurs from one system to another; while one could assert that this would simply reflect the beginning of the SDLC for a new proposed system, the

SDLC as presented in the SA&D books we reviewed does not appear to offer guidance with respect to the information extant in a current system, but which must be preserved in any new system. We believe this more rightly falls under what NIST refers to as the sunset, (or disposition) phase. This reflects our belief that there should be an introduction, at least at a rudimentary level, to the notion of preserving and protecting organizational information throughout the SLDC, given the importance both of providing accurate information to decision makers without distortion and maintaining the confidentiality of organizational information assets. This perspective arguably appears lacking in current SA&D curricula.



**Table 5a: Learning Objectives**

Table 5a: Learning Objectives					
Initiation	Acquisition / development		Implementation	Operations / maintenance	Sunset (disposition)
	Analysis-functional requirements specification	Logical system design			
<b>IS2010.6 learning objectives</b>					
<ul style="list-style-type: none"> <li>Understand the types of business needs that can be addressed using information technology-based solutions.</li> <li>Initiate, specify, and prioritize information systems projects and to determine various aspects of feasibility of these projects.</li> <li>Clearly define problems, opportunities, or mandates that initiate projects.</li> <li>Incorporate principles leading to high levels of security and user experience from the beginning of the SDLC.</li> </ul>	<ul style="list-style-type: none"> <li>Use at least one specific methodology for analyzing a business situation (a problem or opportunity), modeling it using a formal technique, and specifying requirements for a system that enables a productive change in a way the business is conducted.</li> <li>In the context of the methodologies they learn, write clear and concise business requirements documents, and convert them into technical specifications.</li> <li>Use contemporary CASE tools for the use in process and data modeling.</li> </ul>	<ul style="list-style-type: none"> <li>Articulate various systems acquisition alternatives, including the use of packaged systems (ERP, CRM, SCM, etc.) and outsourced design and development resources.</li> <li>Compare the acquisition alternatives systematically.</li> <li>Design high-level logical system characteristics (user interface design, design of data, and information requirements).</li> </ul>	<ul style="list-style-type: none"> <li>Learn how to implement information systems in organizations using various alternative methods. (Note: this isn't specifically mentioned in the IS 2010.6 learning objectives, but various topics that would seem relevant to this are listed there).</li> </ul>	<p>Operations/maintenance and sunset (disposition) are phases not addressed in IS2010.6 but are suggested by NIST documentation on information security. Maintenance activities are discussed in the IS 2010 elective IT audit course. We found limited if any guidance on system disposition.</p>	
<b>Additional security-relevant learning objectives that NIST 800-64 suggests</b>					
<ul style="list-style-type: none"> <li>Understand potential impacts from breach of confidentiality, integrity or availability of information assets.</li> <li>Learn how to assess risk and perform security categorization.</li> </ul>	<ul style="list-style-type: none"> <li>Document security requirements and convert these into specific security controls based on the value of information assets.</li> </ul>	<ul style="list-style-type: none"> <li>Design procedures for securing information assets.</li> </ul>	<ul style="list-style-type: none"> <li>Learn how to assess IS security controls and ensure that they are part of the ongoing operation of the system.</li> </ul>	<ul style="list-style-type: none"> <li>Learn how to devise and put into place plans for the secure ongoing operation of information systems.</li> </ul>	<ul style="list-style-type: none"> <li>Learn how to develop a systematic procedure for secure system disposal</li> <li>Understand the importance of maintaining information security, and information preservation in system transition</li> </ul>
<p>Note: The following learning objectives are not necessarily associated with any specific SDLC phase and are considered here as such. From IS 2010.6, these are: manage information systems projects using formal project management methods; incorporate principles leading to high levels of security and user experience from the beginning of the SDLC; analyze and articulate ethical, cultural, and legal issues and their feasibilities among alternative solutions; communicate effectively with various organizational stakeholders to collect information using a variety of techniques and to convey proposed solution characteristics to them. Those suggested by NIST 800-64 include: understand the importance of establishing and maintaining information security, and information preservation throughout the SDLC.</p> <p>* NIST phase "acquisition/development" split into two for consistency with the majority of SA&amp;D books.</p>					



**Table 5b: Topics**

Table 5b: Topics					
Initiation	Acquisition / development*		Implementation	Operations / maintenance	Sunset (disposition)
	Analysis-functional requirements specification	Logical system design			
<b>IS2010.6 topics (high-level categories only)</b>					
<ul style="list-style-type: none"> <li>• Identification of opportunities for IT-enabled organizational change.</li> <li>• Analysis of business requirements.</li> <li>• Analysis of project feasibility.</li> <li>• Structuring of IT-based opportunities into projects.</li> <li>• Project specification.</li> <li>• Project prioritization.</li> </ul>	<ul style="list-style-type: none"> <li>• Analysis and specification of system requirements (note: includes “factors affecting security”).</li> <li>• Impact of implementation alternatives on system requirements specification.</li> </ul>		<ul style="list-style-type: none"> <li>• Different approaches to implementing information systems to support business requirements.</li> <li>• Specifying implementation alternatives for a specific system.</li> <li>• Methods for comparing systems implementation approaches.</li> <li>• Organizational implementation of a new information system.</li> </ul>	See comment in Table 5a.	
<b>Additional security-relevant topics that NIST 800-64 suggests</b>					
<ul style="list-style-type: none"> <li>• Develop specific confidentiality, integrity and availability requirements.</li> <li>• IS security categorization.</li> </ul>	<ul style="list-style-type: none"> <li>• Risk assessment</li> <li>• Security planning.</li> <li>• Security functional requirements analysis.</li> <li>• Security assurance requirements analysis.</li> <li>• Impact of security control requirements on system requirements specification.</li> <li>• Cost considerations and reporting for security.</li> </ul>	<ul style="list-style-type: none"> <li>• Risk assessment</li> <li>• Design security controls.</li> <li>• Select initial baseline of security controls, then refine.</li> <li>• Security planning.</li> <li>• Security control development.</li> </ul>	<ul style="list-style-type: none"> <li>• Security control integration.</li> <li>• System &amp; component inspection &amp; acceptance.</li> <li>• Security certification.</li> <li>• Security accreditation.</li> </ul>	<ul style="list-style-type: none"> <li>• Configuration management.</li> <li>• Continuous monitoring.</li> <li>• Security Auditing.</li> <li>• Intrusion detection &amp; monitoring.</li> <li>• Contingency &amp; Continuity plans.</li> </ul>	<ul style="list-style-type: none"> <li>• Transition planning.</li> <li>• Hardware &amp; software component disposal.</li> <li>• Media sanitization.</li> <li>• Information preservation &amp; archiving.</li> </ul>
<p>Note: The following topics are not necessarily associated with any specific SDLC phase and are considered here as such. From IS 2010.6, these are: business process management; fundamentals of IS project management in the global context; using globally distributed communication and collaboration platforms; different approaches to systems analysis and design: structured SDLC, unified process/UML, agile methods. Those that NIST 800-64 suggest include: tools, techniques, and controls to establish and maintain information security; and information preservation throughout the SDLC.</p> <p>* NIST phase “acquisition/development” split into two for consistency with the majority of SA&amp;D books. Therefore, some topics span more than one phase.</p>					

While we focus on the SA&D course, there is probably a larger issue that should be addressed: that is, the treatment of security in MIS curricula. Security is introduced mainly in introductory MIS courses, but, at times, it is lost in later courses due to the understandable need to focus on the technical details of actually getting students to learn things such as process and data modeling, SQL, basic programming control structures, and so on. The IS 2010 model curriculum mandates “significant coverage” for the topic areas of IT security/risk management and IT audit/controls for a single proposed career track, labeled information auditing and compliance specialist. Significant coverage of either topic applies to a limited number of proposed career tracks, not including business analyst or project manager (Topi et al., 2010). Hence, while topics relevant to security do indeed receive some small mention in various model course descriptions, some rethinking may be necessary regarding how to thread security more readily throughout IS curricula, rather than having it reside in a stand-alone course (as is the case currently at our university and likely others) or be featured only as minor additions to the requirements of some courses (e.g., SA&D or databases).



## VII. CONCLUSION

This study is an initial attempt to understand the extent to which information security, which has received increased emphasis in practice in recent years, is emphasized in system development courses. Specifically, we focused on the importance of information security in teaching SA&D courses. As such, our study has some limitations. First, note that we looked at only texts in this study, not course syllabi. This said, textbook publishers go to fairly great lengths by using focus groups, faculty reviewers, and other means to be certain that their texts have content that faculty wish to see included. Hence, the texts may be seen at the least as a reflection (albeit with some distortion) of what faculty want to teach.

Certainly, we re-emphasize that we are not overly critical of existing SA&D texts or their authors. Textbook authors tend to write books that reflect the market and its expressed interests as reflected in adoptions. Further, both textbook authors and faculty often face significant time constraints, which may lead to certain topics being dropped, even important ones. It is understandable that the texts as a group cannot focus heavily on information security given that (a) security has been universally viewed as a non-functional requirement to date, (b) addressing security concerns along with everything else that needs addressed adds complexity to an already full SA&D course agenda, (c) thinking about security requirements as espoused here is fairly recent, and (d) authors and faculty have time and space constraints. With textbooks, as with knowledge, there is evolution in play that will hopefully lead to a greater emphasis on these topics in the future; we hope our effort accelerates an increased and earlier emphasis on information security in the textbooks used to develop systems professionals.

Even though we used NIST standards in presenting our findings, other relevant standards that we referenced earlier are not terribly distinct from NIST standards. All of the standards emphasize the bedrock importance of confidentiality, integrity, and availability. They also have some means by which the importance of information is assessed along with the salience of threats and vulnerabilities (which, along with the value of the information asset, comprise risk). In addition, they emphasize building security controls into information systems commensurate with the value of information assets and the risk to them. Our concern is not that SA&D materials, represented by the texts we reviewed, are not using NIST per se; our concern is that, as our findings suggest, a significant portion are not addressing these issues in any effective manner, which makes it plausible that a majority of faculty delivering SA&D courses are not either.

At this writing, we have not yet researched this topic with those working in industry, although one of the authors found that the primary thesis of this article resonated with attendees when it was presented at a practitioner conference in 2013. Obviously, this paper is a first effort toward getting a better handle on how security is viewed in the system development life cycle, and perhaps in IS curricula writ large.

We also suggest that the issues we raise here may not be limited only to the SA&D courses. It seems reasonable to assess courses in MIS curricula to determine the extent to which courses emphasize the CIA triad. We believe that most courses in IS curricula feature a distinct lack of emphasis on such matters. For instance, how is security included in textbooks and teaching materials in database management coursework? Noted security expert Bruce Schneier (2000) has stated that “security is a process, not a product”, which implies that security should be featured when developing information systems, throughout their life, and that it should be practiced as a matter of routine both in IS departments and the organizations for which we build systems. We are unsure at this point as to whether this is the case.

Note that the vast majority of examples we provide here to illustrate risk are almost solely limited to the threat of malicious agents. Security preparation must necessarily be seen in the context of not only malicious action, but also human error and natural accident. However, for our purposes here, these distinctions are not particularly crucial. Risk comprises the value of the information being processed, vulnerabilities in one’s systems, and the threats that exist to that information. The specific types of controls that should be put in place will change depending on the nature of the threat, but our main point (that greater emphasis and precedence should be placed on information security in the SDLC) does not.

We think that it’s clear that our systems analysis and design courses could benefit from a greater emphasis on information security. Further, to avoid costly rework and/or missed security requirements resulting in system vulnerabilities that may well lead to breaches of confidentiality, integrity, or availability, the security requirements of information systems should be considered earlier and throughout the system development lifecycle, which is consistent with the position advocated by NIST. In addition to assessing development risks during the SDLC, it is important to categorize the impact of information security breaches over a system’s life. Understanding the issues involved in protecting information assets is an important perspective that appears to be lacking in the core MIS curricula for teaching future systems professionals. We suggest that it would be instructive to both textbook authors and faculty to revisit the emphasis placed on information security in teaching systems analysis and design courses.

We present our admittedly ambitious suggestions for such an emphasis in the spirit of engendering further discussion.

We intend our effort here to establish a basis to "call" IS educators to address what we perceive as a gap pertaining to information security as required content in the preparation of future MIS professionals. SA&D courses are arguably essential in information security preparation for IS professionals since students should presumably learn the appropriate foundation to (1) analyze information security requirements for a system and (2) design the system to meet those requirements. Without some such preparation from SA&D courses that use any of the relevant standards noted here (NIST, COBIT, COSO, ISO, ITIL, FERMA), IS professionals are likely missing foundational elements for meeting organizations' information security needs. We believe that our assessment provides persuasive evidence that there is a problem with information security preparation in SA&D courses and call on our colleagues in academia to address this concern.

## ACKNOWLEDGEMENTS

The authors appreciate the kind and constructive feedback provided by authors of the texts we reviewed.

## REFERENCES

*Editor's Note:* The following reference list contains hyperlinks to World Wide Web pages. Readers who have the ability to access the Web directly from their word processor or are reading the paper on the Web, can gain direct access to these linked references. Readers are warned, however, that:

1. These links existed as of the date of publication but are not guaranteed to be working thereafter.
2. The contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.
3. The author(s) of the Web pages, not AIS, is (are) responsible for the accuracy of their content.
4. The author(s) of this article, not AIS, is (are) responsible for the accuracy of the URL and version information.

Baskerville, R., Rowe, F., & Wolff, F. C. (2012). Functionality vs. security in IS: Tradeoff or equilibrium? In V. Sambamurthy, M. H. Huang, & G. Piccoli (Eds.), *Proceedings of the Thirty-Third International Conference on Information Systems* (pp. 588-593).

Boehm, B. W. (1981). *Software engineering economics*. Englewood Cliffs, NJ: Prentice-Hall.

Cartlidge, A., Hanna, A., Rudd, C., Macfarlane, I., Windebank, J., & Rance, S. (2007). *An introductory overview of ITIL V3*. UK: itSMF.

Clune, S. (2011). Report: Push for electronic medical records overlooks security gaps. *PBS*. Retrieved January 29, 2013, from <http://www.pbs.org/newshour/rundown/2011/05/report-push-for-electronic-medical-records-overlooks-security-gaps.html>

Committee of Sponsoring Organizations. (1992). *Internal control-integrated framework*. New York, NY: AICPA.

de Laat, C., Gross, G., Gommans, L., Vollbrecht, J., & Spence, D. (2000). *Generic AAA architecture* (request for comments #2903). Internet Engineering Task Force.

Dennis, A., Wixom, B. H., & Roth, R. M. (2015). *Systems analysis and design* (6<sup>th</sup> ed.). Hoboken, NJ: John Wiley.

Dennis, A., Wixom, B. H., & Tegarden, D. (2012). *Systems analysis and design with UML Version 2.0: An object-oriented approach* (4<sup>th</sup> ed.). Hoboken, NJ: John Wiley.

Damouni, N. (2014). Exclusive: U.S. companies seek cyber experts for top jobs, board seats. *Reuters*. Retrieved from <http://www.reuters.com/article/2014/05/30/us-usa-companies-cybersecurity-exclusive-idUSKBN0EA0BX20140530>

Dutta, A., & McCrohan, L. (2002). Management's role in information security in a cyber economy. *California Management Review*, 45(1), 67-87.

The Economist. (2014). *Horror movie: Hackers shine a harsh light on Sony*.

Eversley, M., & Hjelmgard, K. (2013). Target confirms massive credit-card data breach: Secret Service confirms investigation of potential breach that began around Black Friday. *USA Today*. Retrieved from <http://www.usatoday.com/story/news/nation/2013/12/18/secret-service-target-data-breach/4119337/>

Graham, J. (2013). Many companies do not give sufficient attention to cyber risks—survey. Retrieved from <http://www.ferma.eu/blog/2013/01/many-companies-do-not-give-sufficient-attention-to-cyber-risks-survey/>

- Garfinkel, S. L., & Shelat, A. (2003). Remembrance of data past: A study of disk sanitization practices. *IEEE Security & Privacy*, 1(1), 17-27.
- Hoffer, J. A., George, J. F., & Valacich, J. S. (2014). *Modern systems analysis and design* (7<sup>th</sup> ed.). Upper Saddle River, NJ: Pearson.
- Honan, M. (2012). How Apple and Amazon security flaws led to my epic hacking. *Wired*. Retrieved from <http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/all/>
- Howard, P. (2013). *Official (ISC)<sup>2</sup>® guide to the CAP® CBK®*. Boca Raton, FL: CRC Press.
- ISACA. (2012). *COBIT 5: A business framework for the governance and management of enterprise IT* (5<sup>th</sup> ed.). Rolling Meadows: ISACA. Retrieved from <https://www.isaca.org/COBIT/Pages/Product-Family.aspx>
- Larkin, R. D., Lopez, J., Butts, J. W., & Grimaila, M. R. (2014). Evaluation of security solutions in the SCADA environment. *The Data Base for Advances in Information Systems*, 45(1), 38-53.
- Kendall, K. E., & Kendall, J. E. (2014). *Systems analysis and design* (9<sup>th</sup> ed.). Upper Saddle River, NJ: Pearson.
- Kopytoff, V. (2012). The risks and rewards of personal electronics in the workplace. *BloombergBusinessweek*. Retrieved from <http://www.businessweek.com/articles/2012-10-02/the-risks-and-rewards-of-personal-electronics-in-the-workplace>
- Mehan, J. E., & Krush, W. (2009). *The definitive guide to the C&A transformation*. Cambridgeshire, UK: IT Governance Publishing.
- National Institute of Standards and Technology. (2004a). *Federal information processing standards publication 199: Standards for security categorization of federal information and information systems*. Retrieved from <http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>
- National Institute of Standards and Technology. (2004b). *Information security in the system development life cycle*. Retrieved from [http://csrc.nist.gov/groups/SMA/sdlc/documents/SDLC\\_brochure\\_Aug04.pdf](http://csrc.nist.gov/groups/SMA/sdlc/documents/SDLC_brochure_Aug04.pdf)
- National Institute of Standards and Technology. (2007). *Special publications (800 series)*. Retrieved from <http://csrc.nist.gov/publications/PubsSPs.html>
- National Institute of Standards and Technology. (2008a). *NIST SP 800-60 revision 1: Volume 1: Guide for mapping types of information and information systems to security categories*. Retrieved from [http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60\\_Vol1-Rev1.pdf](http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf)
- National Institute of Standards and Technology. (2008b). *NIST SP 800-60 revision 1: Volume 2: Appendices to guide for mapping types of information and information systems to security categories*. Retrieved from [http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60\\_Vol2-Rev1.pdf](http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol2-Rev1.pdf)
- National Institute of Standards and Technology. (2008c). *NIST SP 800-64 revision 2: Security considerations in the system development life cycle*. Retrieved from <http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf>
- National Institute of Standards and Technology. (2008d). *Information security and privacy advisory board*. Retrieved from [http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2008-12/CSSLP\\_ISPAB-Dec2008\\_LMcNulty.pdf](http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2008-12/CSSLP_ISPAB-Dec2008_LMcNulty.pdf)
- National Institute of Standards and Technology. (2010). *NIST SP 800-37 revision 1: Guide for applying the risk management framework to federal information systems: A security life cycle approach*. Retrieved from <http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf>
- National Institute of Standards and Technology. (2011). *NIST SP 800-39: Managing information security risk: Organization, mission and information system view*. Retrieved from <http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf>
- National Institute of Standards and Technology. (2012). *NIST SP 800-30 revision 1: Guide for conducting risk assessments*. Retrieved from [http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800\\_30\\_r1.pdf](http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf)
- National Institute of Standards and Technology. (2014). *NIST SP 800-88 revision 1: Guidelines for media sanitization*. Retrieved from <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>
- Neumann, P. G. (1995). Risks to the public in computers and related systems. *ACM SIGSOFT Software Engineering Notes*, 20(2), 8-9.
- Neumann, P. G. (1996). Risks to the public in computers and related systems. *ACM SIGSOFT Software Engineering Notes*, 21(5), 13.

- Office of the President. (2012). *Bring your own device: A toolkit to support federal agencies implementing bring your own device (BYOD) programs*. Retrieved from <http://www.whitehouse.gov/digitalgov/bring-your-own-device>
- Perrin, C. (2008). The CIA triad. *TechRepublic*. Retrieved from <http://www.techrepublic.com/blog/security/the-cia-triad/488>
- Privacy Rights Clearinghouse. (2013). *Chronology of data breaches: Security breaches 2005—present*. Retrieved from <http://www.privacyrights.org/data-breach>
- Salisbury, W. D., Miller, D. W., & Turner, J. M. (2011). On contending with unruly neighbors in the global village: Viewing information systems as both weapon and target. *Communications of the AIS*, 28(1), 295-312.
- Satzinger, J. W., Jackson, R. B., & Burd, S. D. (2015). *Systems analysis and design in a changing world* (7<sup>th</sup> ed.). Boston, MA: Course Technology/Cengage Learning.
- Schneier, B. (2000). *The process of security*. Retrieved from <http://www.schneier.com/essay-062.html>
- Rosenblatt, H. J. (2014) *Systems analysis and design* (10<sup>th</sup> ed.). Boston, MA: Course Technology Cengage Learning.
- Topi, H., Valacich, J. S., Wright, R. T., Kaiser, K., Nunamaker, J. F., Jr., Sipior, J. C., & De Vreede, G. J. (2010). IS 2010: Curriculum guidelines for undergraduate degree programs in information systems. *Communications of the AIS*, 26(18), 359-428.
- U.S. Department of Defense. (2000). DoD insider threat mitigation: Final report of the insider threat integrated process team. Retrieved from <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA391380>
- Valacich, J. S., George, J. F., & Hoffer, J. A. (2015). *Essentials of systems analysis & design* (6<sup>th</sup> ed.). Hoboken, NJ: Pearson.
- Whitten, J. L., & Bentley, L. D. (2007). *Systems analysis and design methods* (7<sup>th</sup> ed.). Boston, MA: McGraw-Hill.
- Whitney, L. (2014). HealthCare.gov security—"a breach waiting to happen". *Cnet.com*. Retrieved from [http://news.cnet.com/8301-1009\\_3-57617335-83/healthcare.gov-security-a-breach-waiting-to-happen/](http://news.cnet.com/8301-1009_3-57617335-83/healthcare.gov-security-a-breach-waiting-to-happen/)
- Zviran, M., & Erlich, Z. (2006). Identification and authentication: Technology and implementation issues. *Communications of the AIS*, 17(4), 2-30.

## ABOUT THE AUTHORS

**W. David Salisbury** (PhD, University of Calgary) is an Associate Professor in the School of Business Administration at the University of Dayton. He has investigated information technology influences on small group interaction, managing organizational knowledge, and prices in online markets. More recent work includes describing criminal and terrorist uses of information technologies and information security in the MIS curriculum. Dave's work has been published in *Information Systems Research*, *Small Group Research*, *Information & Management*, *Decision Support Systems*, *Communications of the AIS*, *Group Decision and Negotiation*, *Electronic Markets* and *The Database for Advances in Information Systems*. Dave serves as Co-Editor-in-Chief at *The Database for Advances in Information Systems*, and administers the cybersecurity course sequence at UD.

**Thomas W. Ferratt**, PhD, is the Sherman-Standard Register Endowed Chair in Management Information Systems at the University of Dayton. He teaches the core course in systems analysis and design. His primary research focuses on the management of information systems professionals. He has been on the editorial boards of *Information Systems Research*, *MIS Quarterly*, *Journal of the Association for Information Systems*, and *The Data Base for Advances in Information Systems*. In addition, he has served in leadership roles with the Special Interest Group on Computer Personnel Research (SIGCPR), and subsequent to its merger, the Special Interest Group on Management Information Systems (SIGMIS) of the Association for Computing Machinery (ACM).

**Donald E. Wynn, Jr.**, is an Associate Professor in the School of Business Administration at the University of Dayton. He holds a PhD in Business Administration from the University of Georgia. His research appears in journals such as *MIS Quarterly*, *MIS Quarterly Executive*, *Information Systems Journal*, *Cutter IT Journal*, the *Journal of Organizational and End User Computing*, *Communications of the AIS*, and *Journal of the Academy of Marketing Science*. He has published research articles in a number of areas, including open source software, behavioral information security, electronic health records (EHR) software, technological ecosystems, and research methodologies.

Copyright © 2015 by the Association for Information Systems. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for

profit or commercial advantage and that copies bear this notice and full citation on the first page. Copyright for components of this work owned by others than the Association for Information Systems must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers, or to redistribute to lists requires prior specific permission and/or fee. Request permission to publish from: AIS Administrative Office, P.O. Box 2712 Atlanta, GA, 30301-2712, Attn: Reprints; or via e-mail from [ais@aisnet.org](mailto:ais@aisnet.org).





# Communications of the Association for Information Systems

ISSN: 1529-3181

## EDITOR-IN-CHIEF

Matti Rossi  
Aalto University

## AIS PUBLICATIONS COMMITTEE

Virpi Tuunainen Vice President Publications Aalto University	Matti Rossi Editor, CAIS Aalto University	Suprateek Sarker Editor, JAIS University of Virginia
Robert Zmud AIS Region 1 Representative University of Oklahoma	Phillip Ein-Dor AIS Region 2 Representative Tel-Aviv University	Bernard Tan AIS Region 3 Representative National University of Singapore

## CAIS ADVISORY BOARD

Gordon Davis University of Minnesota	Ken Kraemer University of California at Irvine	M. Lynne Markus Bentley University	Richard Mason Southern Methodist University
Jay Nunamaker University of Arizona	Henk Sol University of Groningen	Ralph Sprague University of Hawaii	Hugh J. Watson University of Georgia

## CAIS SENIOR EDITORS

Steve Alter University of San Francisco	Michel Avital Copenhagen Business School
--------------------------------------------	---------------------------------------------

## CAIS EDITORIAL BOARD

Monica Adya Marquette University	Dinesh Batra Florida International University	Tina Blegind Jensen Copenhagen Business School	Indranil Bose Indian Institute of Management Calcutta
Tilo Böhmann University of Hamburg	Thomas Case Georgia Southern University	Tom Eikebrokk University of Agder	Harvey Enns University of Dayton
Andrew Gemino Simon Fraser University	Matt Germonprez University of Nebraska at Omaha	Mary Granger George Washington University	Douglas Havelka Miami University
Shuk Ying (Susanna) Ho Australian National University	Jonny Holmström Umeå University	Tom Horan Claremont Graduate University	Damien Joseph Nanyang Technological University
K.D. Joshi Washington State University	Michel Kalika University of Paris Dauphine	Karlheinz Kautz Copenhagen Business School	Julie Kendall Rutgers University
Nelson King American University of Beirut	Hope Koch Baylor University	Nancy Lankton Marshall University	Claudia Loebbecke University of Cologne
Paul Benjamin Lowry City University of Hong Kong	Don McCubbrey University of Denver	Fred Niederman St. Louis University	Shan Ling Pan National University of Singapore
Katia Passerini New Jersey Institute of Technology	Jan Recker Queensland University of Technology	Jackie Rees Purdue University	Jeremy Rose Aarhus University
Saonee Sarker Washington State University	Raj Sharman State University of New York at Buffalo	Thompson Teo National University of Singapore	Heikki Topi Bentley University
Arvind Tripathi University of Auckland Business School	Frank Ulbrich Newcastle Business School	Chelley Vician University of St. Thomas	Padmal Vitharana Syracuse University
Fons Wijnhoven University of Twente	Vance Wilson Worcester Polytechnic Institute	Yajiong Xue East Carolina University	Ping Zhang Syracuse University

## DEPARTMENTS

Debate Karlheinz Kautz	History of Information Systems Editor: Ping Zhang	Papers in French Editor: Michel Kalika
Information Systems and Healthcare Editor: Vance Wilson		Information Technology and Systems Editors: Dinesh Batra and Andrew Gemino

## ADMINISTRATIVE

James P. Tinsley AIS Executive Director	Meri Kuikka CAIS Managing Editor Aalto University	Copyediting by Adam LeBrocq, AIS Copyeditor
--------------------------------------------	---------------------------------------------------------	------------------------------------------------

