An Implementation Process and Factor Model for Information Systems Security Engineering

B.S. Cline

The Children's Hospital of Philadelphia, Pennsylvania, United States
e-mail: clineb@email.chop.edu

Abstract

The link between security engineering and systems engineering exists at the earliest stage of systems development, and, as a whole, there is sufficient evidence to suggest the discipline of security engineering is sufficiently mature to support its implementation. However, there is little in the literature on the practical application of security engineering and even less empirical work grounded in adoption theory. In contrast, the body of knowledge on quality programs is quite extensive and includes general literature on quality models as well as adoption studies of their implementation. Specific factors related to quality implementations are also well documented and generally well understood. This survey study clearly substantiates a connection between these quality factors and security engineering, provides the opportunity for further research on causal models, and supports the application of lessons learned from quality program efforts to the implementation of a security engineering methodology in support of system acquisition and development.

Keywords

Factor Model, Information Systems, Quality, Security Engineering

1. Introduction

Information systems security engineering (ISSE) is a specialized form of systems engineering (Hansche, 2006) that addresses the identification of security requirements and their successful translation into information technology (IT) and information systems (IS) design and development. Its use in various forms has been advocated for quite some time (for example, see Davis, 2004), and the rationale is quite simple. As with any change incorporated late in the system development life cycle (SDLC), 'bolting on' security functionality as an "after thought" (Peters & Schleipfer, 2004, p. 1) can be expensive and adversely affect system functionality and usability.

> "In fact, if ISSE is properly utilized from the beginning of a systems engineering process, ISSE may provide additional benefits such as identifying and mitigating system risk in regards to cost, schedule and performance earlier on and thus further enhance a system's ability to remain on target (Frederick, 2002). … In order to build [information assurance (IA)] into today's systems, the current, most systematic and cost effective method is ISSE." (Davis, 2004, pp. 15-16)

Yet experience has shown that security is often the "sacrificial lamb" (Lim & Carastan, 2004, p. 1221) when project managers seek to trade scope, cost, and schedule despite increasing security and privacy concerns in multiple industries (Deloitte, Touche, & Tohmatsu, 2006). This assessment is also consistent with the literature (Cline, 2008) and suggests problems continue to exist with the practical implementation of ISSE despite a large body of literature on various ISSE methods, processes, and tools. Unfortunately, there appears to be a relative dearth of information on the implementation of ISSE in support of IT/IS development and acquisition and even less empirical work grounded in adoption theory.

In contrast, the body of knowledge on quality programs is quite extensive and includes formal literature on quality models as well as adoption studies specific to their implementation. Various factors related to the implementation of quality programs are also well documented, and a *prima fascia* connection between quality and ISSE methodologies based on the non-functional nature of their requirements (Chung, Nixon, & Yu, 1995; Mylopoulos, Chung, & Nixon, 1992) has already been established in the literature (Cline, 2008). The same may be said for quality and ISSE implementations based on their classification as an organizational innovation (Ahire & Ravichandran, 2001; Veryard, 1987).

2. Methodology

The research methodology was derived from literature on organizational innovation adoption as it relates to post-adoption (decision) implementation and leverages quality implementation survey research conducted by Sebastianelli and Tamimi (2003). This particular study focused on the later part of a two-stage organizational implementation model (Gallivan, 2001) in which the secondary adoption process is affected by three specific constructs: managerial intervention, subjective norms, and facilitating conditions. Managerial intervention describes those actions taken by management to encourage assimilation of an innovation (Leonard-Barton & Deschamps, 1988), subjective norms are "beliefs about the expectations of relevant others regarding their own secondary adoption behaviour, [and] … facilitating conditions is a broad category that captures other factors that can make implementation more- or less-likely to occur" (Gallivan, 2001). Specific factors are subsequently identified and assigned to each of these intermediate constructs to form a complete process and factor model.

Although the factors identified in Sebastianelli and Tamimi (2003) were derived from an exploratory factor analysis, the results—while perhaps statistically optimal—were at times incongruent when individual survey items are viewed in context. As a result, the five factors proposed in this study are slightly modified based on an analysis of quality factors from several prior studies as reviewed by Hill (2006). This approach is similar to the model-generating approach used in confirmatory factor analysis, which "occurs when an initial model does not fit the data and is modified by the researcher" (Kline, 2005, p. 11), and is consistent with the cumulative research tradition espoused by Grover (1997) among others.

The modified factors are organizational culture, leadership, planning, resources, and training (Cline, 2008). Culture is defined as "a set of shared assumptions, values, and behaviours that characterize the functioning of an organization" (Schwalbe, 2006, p. Glossary 8). Leadership is defined as the actions of an individual, usually in a formal position of authority in an organization, "who focuses on long-term goals and big-picture objectives, while inspiring people to reach those goals" (Schwalbe, 2006, p. Glossary 6). Planning is defined as the activities and processes used to devise and maintain a workable scheme to ensure organizational needs are met (Schwalbe, 2006, p. Glossary 8). Resources are defined as "skilled human resources (specific disciplines either individually or in crews or teams), equipment, services, supplies, commodities, materiel, budgets, or funds" (PMI, 2004, p. 372) but not the management of personnel as defined by leadership. And training is defined as "the level of learning required to adequately perform the responsibilities designated … and accomplish the mission" (DAU, 2005, p. B170) and includes education, training and awareness. The complete process and factor model, adapted from Gallivan (2001), is provided in Figure 1.

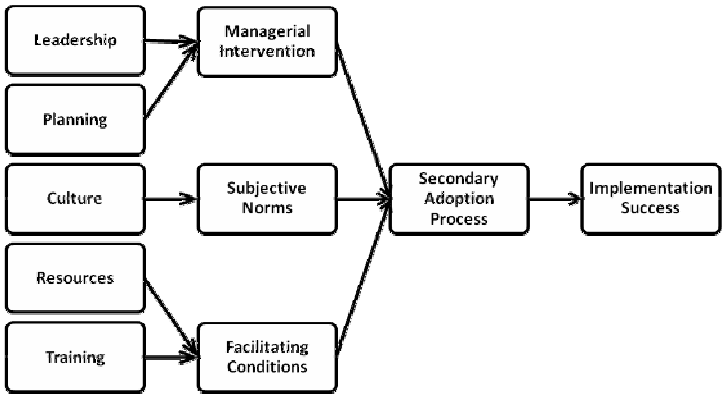

Figure 1: Implementation process and factor model

As with the five factors described, ISSE implementation success is measured concurrently using the same semantic differential scale. The five factors are treated as independent variables and implementation success is treated as the single dependent variable in the study.

The theoretical study population consists of all military, government civilian, and civilian contractor personnel supporting IT/IS acquisition on behalf of a DoD acquisition agency; however, the survey population was restricted to an estimated 100-150 engineering and acquisition professionals (as defined in the theoretical study population) supporting multiple IT/IS acquisition projects and programs under the direction of a single portfolio manager in a specific agency. And while differences between service agencies likely exist, the number and magnitude of these differences are mitigated by extensive regulation of DoD acquisition processes and procedures by public law and Federal and DoD directives, regulations, instructions and related guidance. Thus the sample used for the research is a purposive sample of a "typical instance" (Shadish, Cook, & Campbell, 2002, p. 375) or instantiation of the

theoretical study population as DoD acquisition agencies represent a relatively homogeneous population compared to other agencies with similar missions (amongst each other) but alternatively undergo little or no regulation.

Although the size of the sample population adequately supports correlational/ predictive analysis (Lapin, 1983), it is likely insufficient for statistical modelling of causal explanation. Even in randomized experiments, causal models "are more complex than the simple … models often used to test explanations, and the individual parts of the model may be tested with somewhat less [statistical] power … unless sample size is increased" (Shadish et al., 2002, p. 409). The uncertainties added by use of a non-experimental design certainly exacerbate this problem (Leedy & Ormond, 2005), and assertions of causal relationships are necessarily deferred to future research.

3. Data Collection

Data related to the dependent and independent variables were collected on participant perceptions of relevant survey items using a five-point Likert scale indicating level of agreement. Table 1 provides the modified language for the 30 survey items on the final instrument, which respondents accessed via a Web-based service provider. Note the last item specifically addresses the respondent's perception of the relative success of ISSE implementation in their organization.

Use of this format was necessary due to replication of the Sebastianelli and Tamimi (2003) study. However, unlike the prior study, survey item loadings were determined *a priori* based on each factor's operationalised definition and additional survey items were added where needed to provide a more balanced overall design (five items per factor). Additional modifications were made to support contextual relevance to the implementation of ISSE in a DoD IS/IT acquisition environment. And while it is understood that modifications to a survey instrument may cause problems with internal and external validity, this type of inductive approach is "strongly" (Spector, p. 13) recommended over the deductive approach taken by Sebastianelli and Tamimi (2003), as "almost any group of correlated items is bound to result in factors that can be given meaning" (Spector, pp. 13-14). External validity of the instrument is supported by the theoretical framework and internal validity is supported through pre-test of the survey instrument using a convenience sample of 15 acquisition and engineering professionals.

Out of the 70 respondents who accessed the survey, 51 completed the instrument for a response rate of 34% to 51% given the estimated survey population. The returns are consistent with the findings of a study by Fraze, Hardin, Brashears, Haygood, and Smith (2003) on email- and Web-based survey response rates (averaging 27% and 43%, respectively) and a more recent study by Archer (2008) on Web-based needs assessments (averaging 40%).

#	Survey Item
1	Systems engineering plans do NOT include security engineering goals. (P1)
2	Security engineering best practices of other organizations are benchmarked. (P2)
3	There are excess layers of management. (L1)
4	Security engineering is treated as a separate initiative. (L2)
5	System security is NOT everyone's business. (C1)
6	Personnel are trained in techniques used to identify security problems. (T1)
7	There is NO joint security planning with systems developers and integrators. (P3)
8	System security is effectively measured. (P4)
9	Security requirements are defined by the users of the system. (C2)
10	Personnel are NOT trained in group discussion and communication techniques. (T2)
11	Security planning is often vague. (P5)
12	Information Assurance Strategies are driven by users of the system. (C3)
13	Personnel are empowered to address security issues. (L3)
14	There are adequate resources to effectively implement security. (R1)
15	Cross-functional teams are NOT employed to address system security. (R2)
16	Personnel and/or teams are recognized for achievements in improving security. (C4)
17	Personnel are trained in security engineering skills. (T3)
18	Top leadership is visibly and explicitly committed to acquiring secure systems. (L4)
19	Security efforts rarely meet expectations in terms of desired results. (D1)
20	Management's performance assessments are linked to achieving security goals. (L5)
21	System security is addressed throughout the system development life cycle. (D2)
22	Time constraints prohibit implementing effective security. (R3)
23	Personnel are resistant to change. (C5)
24	The high costs of implementing security outweigh the benefits. (D3)
25	System testing always reveals problems with security. (D4)
26	Security engineers are readily available to support your programs/systems. (R4)
27	System security requirements are adequately addressed in acquisition training. (T4)
28	There is NOT enough funding available to address system security. (R5)
29	Personnel are NOT trained in the acquisition of secure systems. (T5)
30	Security engineering has been successfully implemented in my organization. (D5)

Table 1: Survey items with wording modified to support the ISSE constructs

4. Results

When each survey item was evaluated individually, inter-item correlations were typically less than .500. Correlation analysis yielded a Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy of .753 and Bartlett's test of sphericity with a $\chi 2$ value of 742.457 and 300 degrees of freedom (df), which is significant at $p < 0.001$. KMO for the factor item averages was 0.892, and Bartlett's test of sphericity had a χ^2 value of 215.297, which is significant at $p < .001$ with $df = 10$. Skewness and kurtosis of the factor items were also reduced by taking their averages.

Internal consistency of the factor items in this research compare favourably when loaded against the factors specified in Sebastianelli and Tamimi (2003), although culture appears problematic in both studies. A simple factor item analysis, which eliminates survey items loading poorly on each of the factors in the proposed model, provides further improvement as seen in Table 2 (significant where indicated by an asterisk at $p < .001$). Note the use of factor analysis techniques for this purpose is

supported by the meritorious (close to marvellous) value of the KMO measure of sampling adequacy (.892) (Norušis, 2006).

Proposed	Factor Items	Cronbach's α
Tnew: Training	T1, T3, T4, T5	.778*
Pnew: Planning	P2, P3, P4, P5	.730*
Lnew: Leadership	L3, L4, L5	.706*
Rnew: Resources	R1, R2, R3, R4, R5	.721*
Cnew: Culture	C2, C3	.603

Table 2: Optimized reliability estimates for the proposed ISSE factor model

All factors except culture now have values greater than .70; however, the value for culture is better than indicated in the original study and considered acceptable for exploratory research (Nunnally, 1978). The reason for the consistency likely lies in the focus of both items on customer alignment. However, C3 may be confounding the planning and culture factors as indicated by a simple factor item analysis, which loads C3 against two components at .611 and -.578, respectively. While the reason is not as clear, C2 also loads relatively well against the same two components at .678 and -.462, respectively. Regardless, both component loadings seem to support the factor's lack of statistical significance, which is also noted in Table 2. As a result, the author selected a single survey item, 'System security is NOT everyone's business' (C1), to represent an optimized measure for culture (Cnew). Note a new dependent variable, Dnew, is also computed from a factor analysis of the five items (D1 thru D5) loading under Davg. All items load significantly under Davg for a Cronbach's α of .694, and optimization yields Dnew equal to the average of the best loading items—D2 and D5—with an associated Cronbach's α of .834 significant at a p-value of 0.009.

Table 3 provides the results of the simple regression analysis for all factor models. Factors are significant at a p-value of .10. Adjusted R^2 values are significant at a p-value of less than .05. The regression approach used was step-wise for all factors using an entrance criterion of .10.

DV	Original Factors	R^2 / adjR^2	Proposed Factors	R^2 / adjR^2	Optimized Factors	R^2 / adjR^2
D1	F2	.428/.417	Pavg	.449/.438	Pnew, Rnew	.402/.336
D2	F2	.559/.550	Pavg	.527/.515	Pnew, Cnew, Lnew	.595/.569
D3	F3	.287/.273	Lavg	.225/.209	Rnew	.120/.102
D4	F3	.186/.169	Tavg	.210/.194	Cnew, Tnew	.299/.248
D5	F2	.458/.447	Ravg, Tavg	.500/.479	Tnew, Pnew	.528/.509
Davg	F2, F3	.757/.747	Pavg, Lavg	.734/.723	Tnew, Cnew, Rnew, Pnew	.769/.749
Dnew	F2	.587/.578	Pavg, Ravg	.589/.572	Pnew, Tnew	.617/.601

Table 3: Explanatory power estimates by factor model

In general, the proposed factor item model with all factors loading performed on par with the original model for both number of significant factors and total explanatory power (R^2). The table also shows the optimized factor loadings generally perform

better for variability explained and provide for a larger number of significant factors for all versions of the dependent variable except D3.

Note the computation of averages was an essential component of the comparative analysis for all factor models and provided additional support for the reliability and validity of the survey instrument (Spector, 1992). Averaging retains all relevant information collected in the survey, helps mitigate the effects of random error that would otherwise be unaddressed, and—unlike scores in a summated scale—can be directly related to the original measurement scale. Table 4 provides the results for regression-based tests of the relationship between the optimized factors and ISSE implementation against Dnew.

Factor	F	DF	Sig.	Adj. R2	S.E. Est.	Durbin Watson
Cnew	22.154	50	.000	.297	.96160	2.009
Lnew	38.295	50	.000	.427	.86816	1.782
Pnew	57.242	50	.000	.529	.78695	1.699
Rnew	50.781	50	.000	.499	.81203	1.878
Tnew	54.306	50	.000	.516	.79805	1.601

Table 4: Relationship between optimized ISSE factors and ISSE implementation

Average scores for each factor appear to be linearly associated with the dependent variable. Variability explained is considered adequate for all factors, and the Durbin-Watson values indicate little if any correlation of the residuals (Norušis, 2006).

5. Discussion

Changes made to support the proposed ISSE implementation model appear to have had little effect on the performance of the survey instrument or on the utility of the underlying constructs put forth by Sebastianelli and Tamimi (2003). Reliability estimates for items loaded against the original quality factors are generally consistent with the Sebastianelli and Tamimi (2003) study, and reliability for all proposed factor item loadings supporting ISSE implementation is considered adequate. And although significance of the culture item loadings could not be demonstrated, overall reliability of the proposed factors is also considered adequate.

The high degree of positive correlation between all factors and ISSE implementation supports a general claim of concurrent validity (Spector, 1992) but could also indicate problems with divergent validity. However, this particular threat is believed small since the factors are unlikely to be confounded conceptually. Rationale includes their operationalisation and the prevalence with which they appear in the adoption and quality literatures. Thus multicollinearity of the factors is believed to be the result of the complex nature of their interrelationships.

Regression analysis used to compare the explanatory power of the original, proposed and optimized factors indicate they explain similar amounts of variability; however, more of the optimized factors tended to be significant. Regression also supports the

principle claim put forward by this research: five factors recognized as significant barriers to the implementation of quality programs—culture, leadership, planning, resources and training—are also relevant to the ISSE implementation problem.

5.1. Implications for Future Research

This study provides a survey instrument that may be further refined and validated in future studies and which researchers may use to assess ISSE implementation factors. Opportunities for future research include confirmatory studies of the current findings using other DoD acquisition agencies or additional exploratory studies using commercial organizations, e.g., within industries such as health care or manufacturing, if appropriate changes are made to the instrument to remove DoD-centric terms and concepts. Further investigation of the culture construct, factor interrelationships, and causal or predictive models provide additional opportunities.

5.2. Implications for Practitioners and Policy Makers

Practitioners may apply lessons learned from prior quality program efforts in their organizations—or the efforts of others—to the ISSE implementation problem. General examples specific to each of the five implementation factors include the following:

- *Culture*: Stress the importance of ISSE through policy; provide penalties for non-compliance with the policy and enforce the penalties; include rewards for the development of systems that meet stated security requirements.

- *Strategy/planning*: Incorporate ISSE into systems engineering plans, procedures, standards and guidance; fully integrate ISSE in all engineering design reviews and project or program milestone reviews.

- *Leadership/management*: Ensure leadership understands their information security compliance requirements and the penalties for non-compliance.

- *Resources*: Assign dedicated security engineers to all IS/IT acquisition efforts and provide the tools needed for ISSE, e.g., access to relevant government and commercial documentation and standards, current literature and research, and vulnerability and risk assessment and management tools

- *Training*: Provide ISSE awareness training to systems engineers and project managers and ensure security engineers are properly trained and certified.

More importantly, policy makers must understand the decision to adopt ISSE is a necessary but insufficient condition for its successful implementation. Just as "quality is not free" (Krishnan, Kriebel, Kekre, & Mukhopadhyay, 2000, p. 754) in the sense there must be an upfront investment to realize the benefits of quality, neither is ISSE. It is imperative that policy makers understand the commitment needed to successfully implement ISSE, plan for the implementation just as they

have for quality programs, and ensure policy addresses implementation requirements, e.g., resources and training, in addition to the implementation itself.

6. Conclusion

Formal literature specific to the implementation of ISSE is virtually non-existent. But while the literature on the adoption and assimilation of technological and organizational innovation addresses similar implementations and generally supports the applicability of quality program implementation factors to the ISSE problem, the applicability of these quality factors to ISSE—while certainly reasonable—had not been specifically addressed. This study is the first to formally examine these factors and substantiate the connection between the implementation of ISSE and quality management programs like TQM. Analysis of the data clearly supports the assertion that culture, leadership, planning, resources and training—factors that are grounded in theory and strictly defined—are related to the successful implementation of ISSE in support of the acquisition of secure IS/IT.

Ultimately, the successful implementation of ISSE—like quality—requires a fundamental change in the way organisations acquire IS/IT (Chin & Pun, 2002). Management support for the formal incorporation of ISSE in engineering plans and the assignment of trained security engineers may not guarantee success, but it will certainly go a long way toward helping managers (1) provide targeted application of scarce resources (dollars and personnel), (2) facilitate the proper engineering and implementation of technical security controls, (3) reduce overall risk to project scope, cost and schedule, and (4) address the most critical IS/IT security compliance issues affecting their projects.

7. References

Ahire, S., & Ravichandran, T. (2001). An innovation diffusion model of TQM implementation. *IEEE Transactions on Engineering Management, 48*(4), 445-464.

Archer, T. (2008). Response rates to expect from Web-based surveys and what to do about it. *Journal of Extension, 46*(3).

Chin, K.-S., & Pun, K.-F. (2002). A proposed framework for implementing TQM in Chinese organizations. *The International Journal of Quality & Reliability Management, 19*(3), 272-294.

Chung, L., Nixon, B. A., & Yu, E. (1995, March 27-29). Using non-functional requirements to systematically support change. In *Proceedings of the 2nd International Symposium on Requirements Engineering (RE'97)* (pp. 132-139). York, United Kingdom: IEEE Press.

Cline, B. (2008, June 15-19). *Factors related to the implementation of ISSE: A quality perspective.* Paper presented at the 18th Annual International Symposium (IS'08), Utrecht, NL.

Davis, J. F. (2004). Information systems security engineering: A critical component of the systems engineering lifecycle. *Ada Letters, XXIV*(4), 13-18.

Defense Acquisition University. (2005). *Glossary of Defense Acquisition Acronyms & Terms*. Fort Belvoir, VA: Defense Acquisition University Press.

Deloitte, Touche, & Tohmatsu. (2006). *2006 Global Security Survey*. London: Author.

Fraze, S., Hardin, K., Brashears, T., Haygood, J., & Smith, J. (2003). The effects of delivery mode upon survey response rate and perceived attitudes of Texas agri-science teachers. In *Proceedings of the National Agricultural Education Research Conference*. Las Vegas, NV.

Frederick, C. (Ed.). (2002). *Information Assurance Technical Framework, Version 3.1*. Fort Meade, MD: National Security Agency.

Gallivan, M. J. (2001). Organizational adoption and assimilation of complex technological innovations: Development and application of a new framework. *ACM SIGMIS Database, 32*(3), 51-85.

Grover, V. (1997). An extension of the Tri-core model of information systems innovation: Strategic and technical moderators. *European Journal of Information Systems, 6*(4), 232-242.

Hansche, S. (2006). *Official (ISC)2 guide to the CISSP-ISSEP CBK*. Boca Raton, FL: Auerbach Publications.

Hill, D. A. (2006). *What makes TQM work: A study of obstacles and potential outcomes of TQM in the southeast region (Draft)*. Unpublished Dissertation, Capella University, Minneapolis, MN.

Kline, R. (2005). *Principles and practice of structural equation modeling* (2nd ed.). New York: Guildford Press.

Krishnan, M., Kriebel, C., Kekre, S., & Mukhopadhyay, T. (2000). An empirical analysis of productivity and quality in software products. *Management Science, 46*(6), 745-759.

Lapin, L. (1983). *Probability and statistics for modern engineering*. Belmont, CA: Brooks/Cole Publishing.

Leedy, P. D., & Ormond, J. E. (2005). *Practical research: Planning and design* (8th ed.). Upper Saddle River, NJ: Pearson Education.

Leonard-Barton, D., & Deschamps, I. (1988). Managerial influence in the implementation of new technology. *Management Science, 34*(10), 1252-1265.

Lim, I., & Carastan, I. V. (2004). System development security methodology. In H. F. Tipton & M. Krause (Eds.), *Information security management handbook* (5th ed., pp. 1221-1234). Boca Raton, FL: Auerbach Publications.

Mylopoulos, J., Chung, L., & Nixon, B. (1992). Representing and using non-functional requirements: A process-oriented approach. *IEEE Transactions on Software Engineering, 18*(6), 483-497.

Norušis, M. (2006). *SPSS 15.0 statistical procedures companion*. Upper Saddle River, NJ: Prentice Hall.

Nunnally, J. C. (1978). *Psychometric theory* (2nd ed.). New York: McGraw-Hill.

Peters, R. L., & Schleipfer, C. M. (2004). *Information assurance forethought versus afterthought*. Paper presented at the Interservice/Industry Training, Simulation & Education Conference (I/ITSEC) 2004. Retrieved February 6, 2007, from http://ntsa.metapress.com/media/n49kynvhupdh2ag4rye0/contributions/x/k/e/m/xkembq4fghr6348w.pdf.

Program Management Institute. (2004). *A guide to the project management body of knowledge* (3rd ed.). Newtown Square, Pennsylvania: Author.

Schwalbe, K. (2006). *Information technology project management*. Boston, MA: Thompson Education.

Sebastianelli, & Tamimi. (2003). Understanding the obstacles to TQM success. *The Quality Management Journal, 10*(3), 45-56.

Shadish, W. R., Cook, T. D., & Campbell, D. T. (2002). *Experimental and quasi-experimental designs for generalized causal inference*. Boston: Houghton Mifflin Company.

Spector, P. E. (1992). *Summated rating scale construction: An introduction*. Newbury Park, CA: Sage Publications.

Veryard, R. (1987). Implementing a methodology. *Information and Software Technology, 29*(9), 469-474.