



P1074 Revision Workgroup
Software Engineering Standards
Committee (SESC)
IEEE Computer Society

Information Security Assurance Team

IEEE P1074 Revision Workgroup

Justification for Elevating the priority and visibility of Security Activities in the Revised P1074 Standard

Version 1.06

Information Security Assurance Team
Bar Biszick, Lead
Tom Starai
(Ed Colbert)

3/24/2005

Table of Contents

Table of Contents 1

Revision History 1

Summary Conclusions 2

Background 3

 Definitions 3

 Scope 3

 Assumptions: 3

Supporting Factors 4

 Compelling New Risk factors: How things have changed since 1997 4

 Current Trends: 6

 Security References in Standards 8

 Engineering Context & Perception 12

Conclusions 13

Recommendation: 14

 Approve Phase 2 determine & document specific security activities 14

 Identified Benefits of Adopting Recommendations 14

 Risks and Mitigation 14

 Potential Alternatives & Supplemental Approaches 16

 Guidance: Next Steps (Chair) 16

 Appendix A: References in ISO/IEC Standards 16

 Appendix B: References in IEEE/EIA 12207 and related standards 18

Revision History

Name	Date	Reason For Changes	Ver./Rev.
Bar Biszick	10/20/02	Initial Draft	1.00
Bar Biszick	10/26/02	Title Change	1.01
Bar Biszick	11/18/02	Revised Task Assignments	1.02
Bar Biszick	11/27/02	Initial Draft for Revision (incomplete)	1.03
Bar Biszick	11/27/02	Completion Initial Draft for Review (with change tracking)	1.04
Bar Biszick	11/27/02	Completed Initial Draft for Review (no change tracking)	1.05
Bar Biszick-Lockwood	3/24/05	Corrected date of Sarbanes-Oxley Act	1.06

Summary Conclusions

- 1) This document presents the business case for elevating Information Security Assurance activities in the revised IEEE P1074-1997 standard, based on compelling business need and the required harmonization with IEEE/IEC 12207
- 2) Evidence suggests that greater emphasis on Security Assurance activities in the standard is warranted. Without additions to the current standard, the revised P1074-1997 will not harmonize with IEEE/IEC 12207 and related standards, will not reflect current business practices, and therefore will not meet the needs of the intended users.
- 3) The following conclusions are supported:
- 4) The addition of complex new technologies, combined with a lack of adequately skilled labor has conspired to create an environment that attracts criminal elements.
- 5) National security, global economic stability and personal privacy are at risk.
- 6) Information security assurance has become a government, business and personal imperative.
- 7) Significant progress has been achieved in engineering practices to secure information at the lower levels of the OSI (physical, datalink, network and transport levels). A similar effort is needed to provide greater emphasis on securing information for the higher layers of the OSI reference model (application, presentation and session levels).
- 8) Cooperative efforts in the global public and private sectors have significantly raised awareness on this topic, and have resulted in international standards for system evaluation and management, but these lack specific guidance in the area of risk assessment and engineering practice within the software development life cycle.
- 9) Harmonization with IEEE/IEC 12207 and related standards will require the addition of specific security activities in the P1074 Life Cycle standard. However, additional enhancements may be required to achieve optimal contemporary relevance and usefulness.
- 10) P1074 is clearly deficient in characterizing the contemporary perception, nature and priority of security activities in the Life Cycle.
- 11) IEEE's policy position on Information Assurance reflects the radical increase in constituent professional awareness and interest in regarding information security assurance as an engineering imperative.
- 12) The prevailing perception among engineering practitioners is that information security assurance activities remain un-standardized in current practice, and that such activities should be mandatory, rather than optional, in the Software Development Life Cycle.

Background

Definitions

For the purposes of this document:

Information Assurance (IA) and **Information Security Assurance (ISA)** will be used interchangeably. Information Assurance (IA) is favored by the U.S. Government, military and professional standards organizations. However, "Information Security" has gained popularity and is most often used in industry.

"**IA or ISA activities**" are defined as all preventive, detective, corrective, deterrent, recovery and compensating activities included in a Software Life Cycle that either directly or indirectly protects the confidentiality and integrity of data within a system, and insures its authenticity and availability.

hacker: An unauthorized individual who attempts to circumvent or bypass the security mechanisms of an information system or network to obtain access to data or to control resources.

malware: software created by unauthorized individuals meant to disrupt business, or replicate, modify or damage data or system programs within the system security perimeter.

trade space: The range of flexibility available to balance the selection of technologies and non-technical solutions against cost and risk.

Scope

This document includes the following:

- 1) The factors behind current trends and business practices that compels the proposed changes to the standard.
- 2) How Information Security Assurance activities are currently represented in IEEE P1074, other IEEE standards and in other relevant international standards.
- 3) The results of an informal survey of IT Life Cycle professionals that evaluates current practice and the perception of Information Security Assurance activities in the Life Cycle.
- 4) The IEEE position and constituent perception of security activities within the engineering practice.

This document does not address:

- Inquiry into engineering practices and perceptions outside the U.S.
- Presenting this recommendation for approval to the IEEE P1074 Revision Workgroup (Chair's responsibility)
- Detailing what specific additions or changes would be made to the standard. (Phase 2 ISA team deliverable targeted for Jan.15th, 2003.)

Assumptions:

- Information Security Assurance is not a passing trend. Evidence indicates that attention on information security is likely to increase over time.
- Additions beyond harmonization with ISO standards can be made as part of the revision effort.
- Users of the revised standard expect it to reasonably reflect current practice.

- Users of the standard expect it to represent activities in a manner consistent with the perception of their nature and priority within the Life Cycle.

Supporting Factors

Compelling New Risk factors: How things have changed since 1997

New information security risks have been brought about by the rapid evolution of the internet over the past six years. The following section summarizes the key factors responsible for this growth and describes why building secure systems is essential to 21st century business, and is exponentially more difficult than it was in 1997.

1. Web enabled technology rapidly proliferated in part due to Y2k, significantly increased technology complexity.ⁱ

Since 1997 there has been an explosion of interest in doing business on the web. This was spurred, in part, by the public and investor perception of successful companies like Amazon.com and Expedia that appeared to prove a viable business model. It was also encouraged by the fact that many companies were forced to upgrade--or else trade out entirely--their legacy systems in order to meet required business standards set by the Federal Government for Y2k compliance. When doing so, they chose platforms and technology that would position them to extend their businesses to this new advertising and transaction medium. By the end of 2000, web presence was considered essential to business in the new millennium, and businesses around the globe were fast-tracking e-commerce initiatives, often circumventing good engineering and risk analysis practices to meet market deadlines.ⁱⁱ

2. Many OO & Web developers are unschooled, unskilled in good programming practice.

HTML is the coding language of the web. It is easy to learn, and requires nothing more than a text application to render complex design and text to a browser. There were few barriers to entry for hobbyists with the time to experiment. Businesses anxious to debut a web presence hired coders that were neither schooled nor skilled in project participation or responsible coding practice. Web developers were added to teams already top heavy with "cowboy" coders that had been picked up to accelerate the programming process using interpreted object oriented languages such as Microsoft's Visual Basic. Many self-taught hobbyists became highly paid programmers and were elevated to team leadership positions, despite the fact that they had little or no knowledge of structured programming methodology. When the dot com bubble burst in early 2000 and internet business sites began to fold, poor quality design and programming was noted as partially to blame. Without attention to fundamental engineering principles, companies failed to deliver adequate quality services.ⁱⁱⁱ

3. Many managers are unable to judge software security risk, and therefore reticent to fund preventive measures.

IA is provided in systems by employing vulnerability/risk mitigation in system design, coding and administrative practices to protect the physical system and its data both in transit and at rest. The multiple dimensions involved in ascertaining cost, risk and available solutions at each level of the OSI that would optimally satisfy security need is extremely difficult. Most managers were trained to make risk decisions in world where the physical borders between their business and the outside world were clearly defined and defensible. The diversity and complexity of technology that enables the internet--and its uses, shortcomings and interdependencies--continues to grow at so breathtaking a pace as to make it nearly incomprehensible to the average senior business

manager. Frameworks have been created to better characterize and address the trade space for the IA problem to guide management appropriate assessments.^{iv} Many texts on this subject have been published.^v Strategies are provided for a layered approach that responds specifically to risk management within a technology trade space, but knowledge of these approaches is not widespread.^{vi} Even technically oriented managers are having difficulty judging the level of protection needed for their information assets, in large part because companies have not put appropriate attention to data valuation. Managers remain in a poor position to evaluate information risk that would indicate the level of security investment needed, when the dollar value of their business data is not known.^{vii}

4. Systems Administrators are overworked or lax in applying protective measures

While the chief burden has been placed on software vendors and equipment manufacturers, the public is reticent to sacrifice personal privacy in exchange for automated methods that would tag every public communication. Solutions such as the Government sponsored clipper chip, shot down in the 90s, as well as the new Trustworthy Computing initiative endorsed by Microsoft, Intel and others are subject to heated debate. In the meantime corporate and government systems remain vulnerable, in part because system administrators responsible for monitoring information security are either under-skilled, over-worked, or else reticent to introduce recommended vendor patches to their sensitive environments in a timely manner.^{viii}

5. Radical Change in communications topology significantly increases the likelihood of security breach.

Communication topology changed from a controllable, insular model to a malleable, multi-port design that made protecting information exponentially more difficult. Prior to the introduction of digital communication technology, information was shared via analog media. A company's information security perimeter could be described as the connection points that linked its faxes and telephones to the backbones of public communication utilities. The only information that got out of a company came through a limited number of these physical, controllable connection points, and secure transmission was usually the sole burden of these utilities.

As companies embraced digital technology, they built LAN and WAN networks—clusters of cables purchased or leased, and part of the burden of securing these transmission media shifted to the company. Dumb computer terminals were replaced with powerful PCs which had their own storage and independent processing power. Instead of a centralized information repository, each computer housed some level of corporate business intelligence. The complexity of protecting critical business information increased exponentially, as these interconnected systems were enabled to directly access each other and the outside world. Risk was further increased when these connection points interfaced with partner B2B companies, vendors and consultants—each of whom shared similar interface with other partner (sometimes even competitor) companies. Efforts to guard the “swiss cheese” security perimeter have proven inadequate for protecting against inadvertent sharing of sensitive corporate and private information with other companies or with the outside world. New physical technologies and logical programming capabilities enable even the least powerful computer system on the market to act as a potential portal for access to proprietary business information, and as a hiding place from which to launch “malware” that can cause breach of privacy, business interruption and data destruction.

6. Economic Impacts Severe, Legal Liability Increasing

According to mig2, a U.K company specializing in Digital Risk Management, global losses from malicious incidents may be stabilizing. Still, an estimated \$7 billion dollars is expected to be lost this year, with \$700 million lost during the month of October alone. The last quarter (3rd quarter, 2002) saw 3.8 billion dollars lost worldwide due to viruses and worms, with Bugbear alone inflicting an estimated \$950 million dollars.^{ix}

From a litigation standpoint, companies can be sued for not having adequate information security controls in place, not following security policies they have put in place, or inadvertently acting as the trusted conduit for malware that damages another company's information or disrupts their business.^x Perhaps even more sobering is the Sarbanes-Oxley act of 2002. Addressing Corporate Financial accountability it holds Executive officers accountable (and potentially personally liable) for the quality of internal corporate controls that could affect the reliability of their SEC filings. Security controls are chief among them.^{xi}

7. Criminal hacking has significantly increased

Since the inception of business communication, there have been hackers—people engaged in capturing information from communication media not meant for them. In the past they have done it for sport, market advantage or mercenary profit. But since 9/11 we are now certain that terrorism can be added this list. That a non-friendly foreign power could hack Pentagon systems and change launch codes and missile destination coordinates, that a terrorist could break into a hospital system and change blood types on patients, that a criminal could gain access to a bank computer and transfer all monies to a clandestine account, all gives one serious pause. In the past, the worst that would be expected from a hack was web defacement that might prove embarrassing to a reputable company. Now, lives and livelihoods, as well as business and national security are at stake.

The 7th annual "Computer Crime and Security Survey" [Power, 2002], conducted with the participation of the San Francisco Federal Bureau of Investigation's Computer Intrusion Squad, says "computer crime and other information security breaches continue unabated ... the financial toll is mounting." The FBI reports that criminals have targeted major components of information and economic infrastructure systems. The survey shows losses due to theft of proprietary information totals \$171M as compared with \$20M in 1997. Similarly, the total loss due to financial fraud back then was \$24M as compared to \$116M in 2002.^{xii}

The yearly increase in discreet security incidents reported to the Computer Emergency Response Team (CERT) site has increased an average of 49% each year since 1997. Estimates are expected to be as high as 100,000 incidents by the end of this year as compared with little over 2000 incidents in 1997—an increase of more than 3000%.^{xiii}

Current Trends:

The following section provides an overview of current trends in various areas of the public and private sectors. Whether at the global, national or personal level, the perception is that information security is a high priority issue that must be addressed expeditiously.

Government & Industry

Over the past several years, national governments and global industry have mobilized to meet new information security challenges and embrace new technology advantage. By 1999, U.S. Intelligence was reporting that over 120 nations were engaged in developing both offensive and defensive capabilities for information warfare. Russia called on the U.N. to begin work on a global treaty, and the U.S. agreed to debate relevant issues in open forum.^{xiv}

Numerous initiatives have been mounted to address this challenge by the government, and in partnership with the private sector. Several relatively recent trends are apparent. First, we have entered an information age in which leaders in both government and industry recognize that information superiority is critical to the national interest.^{xv} Critical Infrastructure Protection has

been recognized as a national priority.^{xvi} Legislation has been enacted to better manage information technology as a strategic asset.^{xvii}

Members of major industry have embraced and internalized IA as a business area.^{xviii} Companies including Compaq, HP, IBM, Intel and Microsoft have created the Trusted Computing Platform Alliance that is working to embed security solutions into hardware and operating systems.^{xix} Demand for data privacy access control and protection across diverse vendor platforms and technologies has resulted in the creation of an international system evaluation standard. The *Common Criteria* combined and aligned the U.S. TCSEC standard, the Canadian Standard CTCPEC, and the European standard ITSEC.^{xx} Together with the ISO/IEC 17799 standard for developing security policies and conducting audits, these two sets of recommendations drive Information Security Assurance today. Since 1998, both Government and industry have moved swiftly to adopt these best practice recommendations. The Federal Government's internal standard for system Certification and Accreditation established in 2000, is based in part on the Common Criteria.^{xxi} Several industry leaders have achieved standardized requirements for Information Security Assurance set out in either national or international standards for trusted computing.^{xxii}

Education & Awareness

The federal government began actively partnering with industry to promote information security over the last few years to make information, training, and resources more available.^{xxiii} Academic curricula have been developed and research centers have been established to improve professional skills and raise awareness about cyber-terrorism.^{xxiv} Internationally recognized professional certification programs are now available from several organizations, including the International Information Systems Security Consortium, Inc, the SANS Institute, the Computer Emergency Response Team Coordination Center (CERT/CC), and TruSecure (formerly National Computer Security Association). Certifications are also becoming required for personnel working on government systems.^{xxv}

There was already a healthy market for conferences and forums on security by the late 90s.^{xxvi} Conferences bring together information security and technology professionals from industry, academia, and government to provoke debate, dialog and action on pressing issues, educate the community, encourage interoperability among vendors and promote investments in security products, research and solutions. The agenda has remained the same, but the urgency of the mission has been greatly accelerated, and the content of conferences and forums today tend to be much more hands-on practical than theoretical.^{xxvii} While preventive measures are being stressed at the firewall level, the most rigorous practical work seems to be in the area of reactive methods: breach identification, containment, national coordination and rapid response to intrusion. The Computer Emergency Response Team Coordination Center (CERT/CC) acts as the nexus for information during major Internet security events. It also offers a series of courses on developing in house Computer System Incident Response Teams (CSIRTS) that would act as the organization's on-site rapid response unit and the regional point of contact for the CERT center during a serious Internet event.^{xxviii} Such measures would be far less important if there was confidence that intrusive attacks that make it past the outer perimeter defenses would be thwarted by security measures engineered into critical systems.

Overall efforts fall far short of what is needed. There are thousands of reported intrusions daily. Because industry emphasis is overwhelmingly on security at the corporate perimeter or vendor application level, malicious code that gets past perimeter defenses tends to travel freely from one critical system to another if custom coded applications or integration code is involved. The Security Management Index, an awareness survey sponsored by PentaSafe Technologies and offered by the humanfirewall.org seems to support this.^{xxix} The survey polled more than 800

companies in 27 industries and revealed the severest security deficiencies in security policy, administration and business continuity management, and in software development and maintenance.^{xxx}

Security References in Standards

IEEE P1074 Security References

In the P1074 standard itself, there are only two references to security as an activity. They appear in sections A.1.2.7 Plan Project Management and A.1.3.1 Manage Risks. Neither reference details specific activities that should be undertaken to insure Information Security Assurance during these project phases. More alarmingly, the Guideline for implementation only mentions security once, in the Introductory section as an example of an additional activity that an organization may choose to execute while implementing the standard. That security assurance is considered optional during standard implementation raises suspicion that the standard is deficient against contemporary practice.

P1074 Security References

IEEE Std 1074-1997 (Revision of IEEE Std 1074-1995; Replaces IEEE Std 1074.1-1995) IEEE Standard for Developing Software Life Cycle Processes

A.1.2.7 Plan Project Management

A.1.2.7.1 Input Information

A.1.2.7.2 Description

Project management planning requires the collection and synthesis of a great deal of information into a coherent and organized SPMP based on the SLCP. This Activity shall initially define, and subsequently update, the SPMP using the Input Information. This Activity shall detail the project organization and assign responsibilities. Standards, methodologies, and tools for configuration management, quality, evaluation, training, documentation, and development shall be specified. This Activity shall apportion the project budget and staffing, and define schedules, using the applicable Input Information. It also shall define procedures for scheduling, tracking, and reporting. It shall address considerations such as regulatory approvals, required certifications, user involvement, subcontracting, and security.

A.1.3.1 Manage Risks

A.1.3.1.1 Input Information

A.1.3.1.2 Description

This activity shall iteratively analyze and mitigate business, technical, managerial, economic, safety, schedule, and security risks. Factors that could impair or prevent the accomplishment of project objectives, or could require technical trade-offs for accomplishing the technical objectives of the project or product, shall be identified and analyzed. Technical factors can include such items as real-time performance, safety considerations, security considerations, implementation considerations, usability considerations, testability, and maintainability. Analytical approaches for technical risk assessment can include static and dynamic modeling and simulation, prototyping, independent reviews, and audits. Cost, resource factors, earnings, liabilities, or any other economic measures involved in the project shall be identified and analyzed. The objective of this analysis is to identify potential economic opportunities, losses, and trade-offs. Analytical approaches for economic risk assessment can include financial analysis, such as return on investment and possible incentive and penalty contract clauses. Operational support risk analysis shall determine the probability that the delivered software will meet the users' requirements. Operational support requirements such as interoperability, security, performance.

IEEE Std 1074.1-1995 IEEE Guide for Developing Software Life Cycle Processes

2. General concepts of the Standard

2.2 Compliance

2.2.1 Upward adaptation

The Standard contains a minimum set of Activities needed to be used in developing software systems. Users may find that their selected SLCM, organization, or contracting organization requires additional Activities to be performed. Examples of additional Activities include, but are not limited to, safety, security, or subcontractor.

Potentially Relevant ISO Standards

During the 1980s, the Open Systems Interconnect, a worldwide federation, developed the 7 level OSI model and began working on a set of worldwide protocols to guide vendor development of compatible computer system components. The rapid proliferation of the internet for commercial business purposes drove the need for secure transaction standardization during the 1990s. In 1996 ISO introduced a comprehensive framework aligned with the OSI model to guide security architecture, development and management. Since the turn of year 2000, however, emphasis has shifted dramatically toward preventive measures, including standards for Intrusion Detection systems, selection of security safeguards, protection profiling, trusted third party authentication services, digital signature schemes, and increased encryption security through secure hashing functions.

The only ISO Life Cycle standard that specifically references security as a topical area is [ISO/IEC 21827:2002](#) Information technology -- **Systems Security Engineering -- Capability Maturity Model (SSE-CMM®)** However, [IEC 17799:2000](#) Information technology -- **Code of practice for information security management**, a management rather than engineering standard, may also provide useful guidance.

The ISA team does not have visibility to these standards at this time. Both should be consulted to provide guidance for the elevation of security activities in the P1074 Life Cycle standard. See [Appendix A](#)

Harmonization with IEEE/IEC 12207 Standard

The topic of security is referenced 17 times in IEEE/EIA 12207.0-1996 "Software life cycle processes," 6 times in IEEE/EIA 12207.1-1997 "Life cycle data," 5 times in Guidance sections and Annexes of IEEE/EIA 12207.2-1997 "Implementation considerations," and 3 times in ISO/IEC JTC1/SC7 F.3 "Organizational life cycle processes." These numbers, as compared with the scant two references found in P1074 and its Guidelines, clearly show that far greater emphasis was placed on information security in the 12207 standard than in P1074.

12207 includes a simple definition of security that covers the mandatory areas of information confidentiality, integrity and availability. References in the Acquisition, Organizational Life Cycle Process and B4.Tailoring... sections can be considered comparable to those in P1074 in that security is regarded as a Project Risk to be evaluated and managed. However, the vast majority of references peppered throughout the 12207 standard characterize security instead as a requirement—in fact, a "critical" requirement. This indicates a significant difference between the standards—not just in volume of references but in fundamental perception of the topic. Designating security as a component of requirements embeds it within a normalized, mandatory, structured life cycle activity—rather than relegating it to a project area that is often overlooked or ignored. Designating security as a "critical" requirement significantly elevates its relative importance in the 12207 standard, and this is clearly reflected by its placement, wording and positioning throughout the standard.

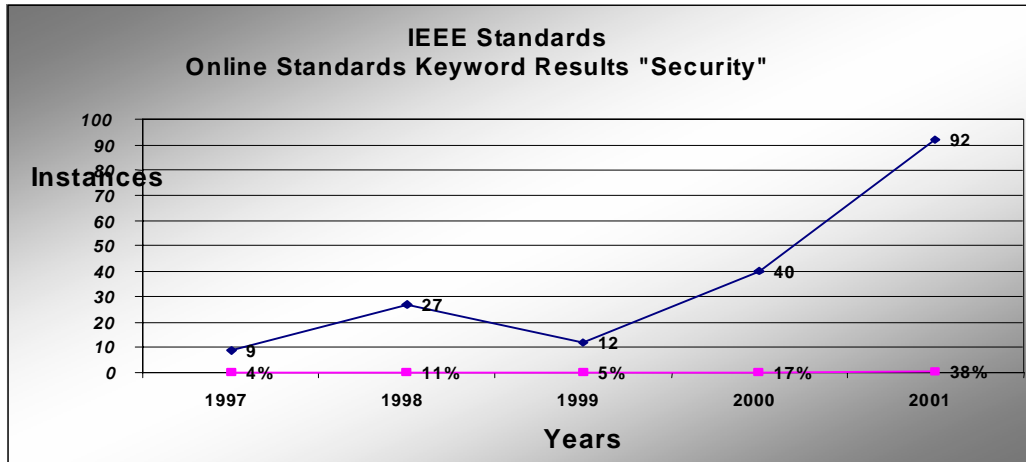
References to security in 12207 are scattered throughout the life cycle, and many include specifics as to the nature of security as a requirement within these processes. During the Planning Process, the potential need for separate security plans is cited and security policies are expected to include "rules for need-to-know and access-to-information at each project

organizational level." The topic obtains a dedicated listing (5.3.4.1e) as part of the Software Requirements Analysis activity and this reference specifically recommends planning for protection against malicious attacks. Security is regarded as a "criticality" factor for prioritization during the Maintenance phase, and as a target for audit and control as part of the Configuration Management, Document Management and Release Management processes. Special emphasis is given to security in the Verification processes—Requirements, Design and Code—where it obtains a dedicated listing as one of only four recommended criteria: "The (requirements, design, code) implements safety, security, and other critical requirements correctly as shown by suitably rigorous methods." For the Acquisition activity, defining safety and security is only one of four Guidance recommendations, and the user is reminded to also include "what the system must not do." "Ability to provide required safety, security and privacy protection," is second only to "provide required capabilities and meet required constraints," in a list of 18 candidate criteria used in evaluating reusable software products (Annex F), Safety, security and privacy concerns are specifically cited for critical requirement reviews (G.3.11). Where problem reporting is concerned, security is the very first of five criteria listed for determining priority handling of reported issues—even superceding the "accomplishment of an essential capability and no work-around-solution."

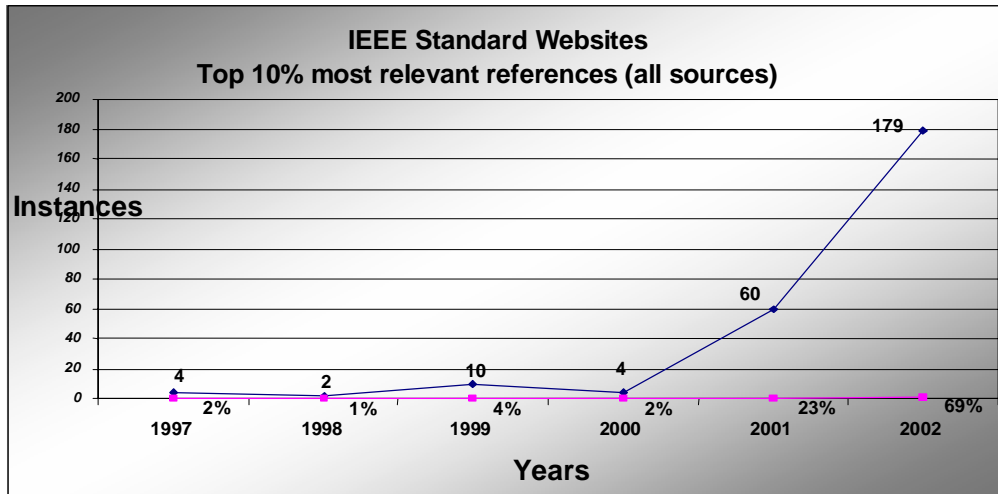
The Life Cycle Data 6.2.6 System Requirements Specification section offers the best model for updating P1074. Of the 23 items listed as important to such a document, Safety, security and privacy protection requirements are listed as sixth, immediately following "Business, organizational and user requirements," and before "Human-factors engineering (ergonomics) requirements." In other words, before any attention is placed on design of any customer facing component, such as a GUI interface, safety, information security and customer data privacy should be thoroughly explored and documented.

Engineering Context & Perception IEEE Standards, Policy & Constituency Perception

The IEEE-USA has taken a policy position that reflects its leadership position, supports government and industry initiatives, and reflects changing practices and perceptions of its constituency.^{xxxix} Since 1997, the number of standards that reference security as a topical area has increased 34%.^{xxxix}



More importantly, a sample of the society's overall activities reveals a very significant increase in attention to the topic of security—especially over the last two years.^{xxxix}



While some of this may be reaction to the increase in cyber-terrorism attacks, the majority centers around the industry drive toward wireless communications. This new, easily exploitable medium requires confirmation of an international standard that assures interoperability as well as transmission security. Therefore, standards focus has been on the lower layers of the OSI, on the physical, datalink, network and lower layers of the transport levels.

In contrast, relatively little has been done to provide comparable guidance at the application, presentation or session levels. IEEE offers 28 standards as part of its subscription package for Software Engineering. Only half make any mention at all of security.^{xxxix} If the level of detail

provided in these is comparable to that which appears in P1074, then the IEEE Engineering standards are severely lacking of guidance in this area, and they are clearly out of step with contemporary concerns. If the assumption was that security could be handled by purely cryptographic measures, or by invasive physical means such as the Clipper Chip, these approaches have been proven inadequate to the task.^{xxxv}

IEEE members currently working on the 8.02.x wireless communications standards are engaged in rigorous debate over the issue of security. There is wide disagreement over the extent to which it should be addressed relative to the wireless standard. Some members believe it represents project scope creep—that it does not belong in the lower levels as addressed by 802.x and therefore should be deferred to groups working on standards that address the levels above them. In the absence of being able to identify those recipient groups, others continue to point out the seriousness of the issue, and the shortcomings of trying to address security at the lower levels without considering security end to end for their system.^{xxxvi}

Compartmentalizing security by level is proving highly problematic for the 802.x team. They are seeking—but not finding—workgroups to provide guidance on security standards at the higher levels. What appears to be needed is a comprehensive approach to security—one that addresses the system comprehensively and at every level during design. This would enable building in not only the necessary safeguards to protect sensitive data, but also the flexibility that will be needed to enhance security in response to changing threats.

With P1074, we have a unique opportunity to introduce the notion of comprehensive security planning, using the system life cycle as the framework.

Professional Survey:

A small sampling of professionals representing a wide variety of job types and industries were polled about how information security perception and practices at their jobs have changed over the past two years. While the sample is too small to be considered conclusive, some broad generalizations are probably valid:

Most respondents:

- reported increased organizational attention to information security.
- reported rework on projects within the last two years due to security problems that they believe probably could have been avoided during development.
- rarely see threat modeling or penetration testing done on projects.
- regard information security assurance as a system requirement (rather than a project risk)
- believe information security assurance should be a mandatory, rather than optional, activity in the life cycle.

About half of respondents noted that security assurance activities were being addressed earlier and more thoroughly in the life cycle and that the responsible party was a security specialist.^{xxxvii}

Conclusions

Efforts that do not treat security as an integral part of systems engineering and architecture fail to provide security. It no longer makes any business sense to spend any money, apply any resources and proceed with any Software Development project unless corporate assets and private customer data will be sufficiently secure.

Software development standards that remain silent on this subject will have less value and will, therefore, be less marketable. It is clear from the available body of knowledge that IA must be integrated into development processes and activities throughout the life cycle. Clarification of IEEE P1074 normative activities to include specific security activities in the Life Cycle is indicated.

IEEE P1074 is arguably in the best position--relative to other standards--to provide guidance on this topic in a way that ensures Information Assurance is sufficiently addressed by incorporating security activities into the development process. The ISA team believes that we cannot afford to miss this important opportunity.

Recommendation:

Approve Phase 2 determine & document specific security activities

To be optimally beneficial, Information Security Assurance should permeate every phase of a System Life Cycle. The confidentiality, integrity, authenticity and availability of information is assured through the use of Physical, Logical, Operational and Administrative controls.

Therefore, to address the Logical deficiencies identified in the foregoing, the ISA team respectfully requests endorsement from the Chair and approval of the recommendation from the P1074 Workgroup at large by December 15. This will enable the ISA Team to begin Phase 2 exploration of the specific security activities that must be added the standard in order to harmonize with IEEE/IEC 12207 etc., to identify what additional activities may be required, and to determine how best to represent these additions within the revised P1074 standard to achieve the proposed deadline of January 15, 2003.

Requirements

- Approval by Dec. 15 to meet proposed delivery date of Jan. 15.
- Access to identified standards cited as potentially relevant.

Identified Benefits of Adopting Recommendations

Timeliness: Adoption of Recommendations would address a pressing government/business concern, and an identified deficiency in engineering standards.

Appropriateness: Recommendations fall within the scope of the P1074 Workgroup charter, align with IEEE/IEC 12207 harmonization efforts, and support current IEEE policy and constituency perception.

Impact: Adopting Recommendations to reflect the contemporary priority of security in this seminal Life Cycle standard, is likely to influence the appropriate elevation of security as a topical area in other downstream standards when they are revised.

Risks and Mitigation

These changes and additions to the revised P1074 standard could be met with resistance from a number of communities. This section lists identified risks and suggests mitigation strategies to effectively market these changes. These strategies would be used to overcome resistance by groups and organizations with which the Life Cycle standard must align.

Software Engineering Community

- **RISK:** Software Project engineers may resist adoption, seeing it as a Project Risk or Infrastructure concern and therefore beyond their scope of responsibility.
- **MITIGATION:** Stress that end to end system security cannot be addressed in the absence of adequate security guidance at all levels of the OSI and through all phases of the system life cycle. Use SMI Index and other research results to support indication of deficiency at the software engineering level.

System Support and Maintenance Community

- **RISK:** System Administrators and Communications/Network Infrastructure management may argue that Information security should be exclusively directed and controlled by its community.
- **MITIGATION:** Provide evidence how deficiencies in the engineering process typically complicates their jobs and increases the quantity of their daily work.

P1074 Standards Process Architect Community

- **RISK:** Users may be uninformed, and therefore resist building in recommended security activities they are unfamiliar with, especially those that pose significant changes to traditional methodology or that represent significant cost.
- **MITIGATION:** The standard must stress the contemporary importance of information security to their business, cite government directives and industry trends, and convince them that they are in a leadership position to effect necessary changes to business process that will assure the protection of their customer's privacy, their organization's assets and continuity, and protect their executive leadership from personal liability.

Project Management Community

- **RISK:** Project Managers may continue to regard information security assurance as a Project Risk rather than a system requirement and resist the addition of security activities that cause project delays or increase project costs.
- **MITIGATION:** Inform them of the Sarbanes-Oxley act which holds companies and their Executives liable for internal controls, and remind them that they are ultimately responsible for assuring that appropriate controls are built into their systems to protect against such legal liability.

IEEE Standards Community

- **RISK:** The IEEE organization may regard the organization's recent proliferation of standards that address information security in various engineering areas as adequate proof that the organization is being responsive to contemporary need.
- **MITIGATION:** Point out that adoption of the recommendations for P1074 and other framework level standards can provide clarity around its policy initiative by supporting those standards that address the problem piecemeal with guidance on the problem at the methodology framework (life cycle) level. Clarifying where and what kinds of security activities should reside may also assist groups like the 802.x workgroups to determine whether addressing security activities at the higher levels of the OSI is in or out of scope for their projects.

Potential Alternatives & Supplemental Approaches

Elevating Information Security activities in the IEEE P1074 standard seems to be a highly efficient way to quickly and deeply penetrate the engineering community to effect necessary change. It will adjust the perception of the relative priority of activities in the Life Cycle to reflect contemporary concerns. The ISA Team can think of no other alternatives or approaches that would yield as swift or comparable result. Specifying security activities within this seminal life cycle standard is likely to have a positive influence on the creation and revision of other engineering standards and is likely to effect a swift and positive change in engineering methodology that addresses urgent government and industry concerns.

Acceptance of these recommendations might be enhanced by endorsements from other IEEE Workgroup leaders.

Guidance: Next Steps (Chair)

1. Chair endorse Recommendation and call for Vote by Dec. 15.
2. If possible, arrange access to related standards: [ISO/IEC 21827:2002](#); IEC [IEC 17799:2000](#);

Appendix A: References in ISO/IEC Standards

A search on keyword "security" returns 98 standards that broadly cover the different levels of the Open Systems Interconnect framework.^{xxxviii} Several concern security at the lower levels such as standards for integrated circuits, data interchange, and connection modes. However, the bulk of them address security at layers 5 and 7—Session and Application protocols. They include entity authentication and PIN management, securing SQL queries, key and digital signatures management; encryption algorithms and hash functions. Some are specific to the telecommunications and finance industries, such as [ISO 10202-x](#), a series of 8 standards that trace the life cycle of a financial transaction card..

The foundation for the ISO position on information security assurance can be found in the seminal standards for the Open Systems Interconnection model:

Open Systems Interconnection

--Basic Reference

- [ISO 7498-2:1989](#) -- Part 2: **Security Architecture**

-- Security frameworks for open systems

- [ISO/IEC 10181-1:1996](#) : **Overview**
- [ISO/IEC 10181-2:1996](#) : **Authentication framework**
- [ISO/IEC 10181-3:1996](#) : **Access control framework**
- [ISO/IEC 10181-4:1997](#) : **Non-repudiation framework**
- [ISO/IEC 10181-5:1996](#) : **Confidentiality framework**
- [ISO/IEC 10181-6:1996](#) : **Integrity framework**
- [ISO/IEC 10181-7:1996](#) : **Security audit and alarms framework**

--Upper Layers Security Model

- [ISO/IEC 10745:1995](#) (this standard provides a basis for the development of application-independent services and protocols, but is limited to specifying the security aspects of communication in the upper layers of OSI)

The following standards are more specific to Security Engineering. For instance, the ISO/IEC 11586-x series provides guidance on building security service components:

--Generic upper layers security

- [ISO/IEC 11586-1:1996](#) : **Overview, models and notation**
- [ISO/IEC 11586-2:1996](#) : **Security Exchange Service Element (SESE) service definition**
- [ISO/IEC 11586-3:1996](#) : **Security Exchange Service Element (SESE) protocol specification**
- [ISO/IEC 11586-4:1996](#) : **Protecting transfer syntax specification**
- [ISO/IEC 11586-5:1997](#) : **Security Exchange Service Element (SESE) Protocol Implementation Conformance Statement (PICS) proforma**

-- Security techniques

- [ISO/IEC 15816:2002](#) -- **Security information objects for access control**
- [ISO/IEC TR 15947:2002](#) -- **IT intrusion detection framework**
-

-- Handling of computer-based technical information

- [ISO 11442-1:1993](#) -- **Part 1: Security requirements**
(addresses security during installation and operations, including physical system security and documentation.)

Series ISO/IEC TR 13335-x address security management

-- Guidelines for the management of IT Security

- [ISO/IEC TR 13335-1:1996](#) **Part 1: Concepts and models for IT Security**
- [ISO/IEC TR 13335-2:1997](#) **Part 2: Managing and planning IT Security**
- [ISO/IEC TR 13335-3:1998](#) **Part 3: Techniques for the management of IT Security**
- [ISO/IEC TR 13335-4:2000](#) **Part 4: Selection of safeguards**
- [ISO/IEC TR 13335-5:2001](#) **Part 5: Management guidance on network security**

Series ISO/IEC 15408-x addresses criteria for security evaluation

-- Evaluation criteria for IT security

- [ISO/IEC 15408-1:1999](#) Part 1: Introduction and general model
- [ISO/IEC 15408-2:1999](#) Part 2: Security functional requirements
- [ISO/IEC 15408-3:1999](#) Part 3: Security assurance requirements

Of special interest are [IEC 17799:2000](#) Information technology -- Code of practice for information security management and [ISO/IEC 21827:2002](#) Information technology -- Systems Security Engineering -- Capability Maturity Model (SSE-CMM®), the latter of which is the only ISO standard designated as specific to Systems Security Engineering.

Appendix B: References in IEEE/EIA 12207 and related standards

IEEE/EIA 12207.0-1996
IEEE/EIA Standard
Industry Implementation of
International Standard
ISO/IEC 12207:1995
(ISO/IEC 12207) Standard for Information
Technology—
Software life cycle processes
March 1998

3 Definitions

3.25 Security: The protection of information and data so that unauthorized persons or systems cannot read or modify them and authorized persons or systems are not denied access to them.

B.4 Tailoring and application considerations

The paragraphs in this clause outline broad tailoring and application considerations for key project characteristics. Neither the considerations nor the characteristics are exhaustive and represent only current thinking. Figure B.1 provides an example of the application of this International Standard.

Organizational policies. Determine which organizational policies are relevant and applicable, such as on computer languages, safety and security, hardware reserve requirements, and risk management. The clauses of this International Standard related to the organizational policies should be kept.

ISO/IEC 12207 : 1995
(ISO/IEC 12207) Standard for Information
Technology—
Software life cycle processes—
Implementation considerations
April 1998

5 Primary life cycle processes

5.1 Acquisition process

5.1.1 Initiation

5.1.1.2 The acquirer will define and analyze the system requirements. The system requirements should include business, organizational and user as well as safety, security, and other criticality requirements along with related design, testing, and compliance standards and procedures.

GUIDANCE:

1—The system requirements should be written at an appropriate level, based on the level of knowledge about the operational concept and the system to be acquired. The system requirements evolve as knowledge is gained by all parties involved. Many methods are available for use in defining system requirements (e.g., concept exploration, prototyping).

2—Definition of system safety and security requirements should also include what the system must not do.

3—In systems containing software with safety requirements, it may be appropriate to apply IEEE Std 1228. RTCA DO-178B may also be a useful reference.

4—In systems containing software with high reliability requirements, it may be appropriate to apply IEEE Std 982.1 to formulate quantifiable reliability requirements.

5.2 Supply process

5.2.4 Planning

5.2.4.5 The supplier shall develop and document project management plan(s) based upon the planning requirements and options selected in 5.2.4.4. Items to be considered in the plan include but are not limited to the following:

- a) Project organizational structure and authority and responsibility of each organizational unit, including external organizations;
- b) Engineering environment (for development, operation, or maintenance, as applicable), including test environment, library, equipment, facilities, standards, procedures, and tools;
- c) Work breakdown structure of the life cycle processes and activities, including the software products, software services and non-deliverable items, to be performed together with budgets, staffing, physical resources, software size, and schedules associated with the tasks;
- d) Management of the quality characteristics of the software products or services. Separate plans for quality may be developed.
- e) Management of the safety, security, and other critical requirements of the software products or services. Separate plans for safety and security may be developed.
- f) Subcontractor management, including subcontractor selection and involvement between the subcontractor and the acquirer, if any;
- g) Quality assurance (see 6.3);
- h) Verification (see 6.4) and validation (see 6.5); including the approach for interfacing with the verification and validation agent, if specified;
- i) Acquirer involvement; that is, by such means as joint reviews (see 6.6), audits (see 6.7), informal meetings, reporting, modification and change; implementation, approval, acceptance, and access to facilities;
- j) User involvement; by such means as requirements setting exercises, prototype demonstrations and evaluations;
- k) Risk management; that is management of the areas of the project that involve potential technical, cost, and schedule risks;
- l) Security policy; that is, the rules for need-to-know and access-to-information at each project organization level;
- m) Approval required by such means as regulations, required certifications, proprietary, usage, ownership, warranty and licensing rights;
- n) Means for scheduling, tracking, and reporting;
- o) Training of personnel (see 7.4)

5.3 Development process

5.3.1 Process implementation

5.3.1.4 The developer shall develop plans for conducting the activities of the development process. The plans should include specific standards, methods, tools, actions, and responsibility associated with the development and qualification of all requirements including safety and security. If necessary, separate plans may be developed. These plans shall be documented and executed.

GUIDANCE:

- 1—The developer may reference, rather than include, specific standards, methods, tools, practices, and computer programming languages in the plans for conducting the activities.
- 2—Planning for development describes the approach (methods/procedures/tools) to applicable activities and tasks of the development process, covers all applicable clauses regarding development, identifies applicable risks/uncertainties regarding those activities and tasks, and describes plans for dealing with the risks/uncertainties.
- 3—Software development planning should be based on the software life cycle model (see 5.3.1.1).

4—Plans to be included may be project management plans and/or software development plans.

5.3.2 System requirements analysis. This activity consists of the following tasks, which the developer shall perform or support as required by the contract:

5.3.2.1 The specific intended use of the system to be developed shall be analyzed to specify system requirements. The system requirements specification shall describe: functions and capabilities of the system; business, organizational and user requirements; safety, security, human-factors engineering (ergonomics), interface, operations, and maintenance requirements; design constraints and qualification requirements. The system requirements specification shall be documented.

GUIDANCE:

1—To fully understand what is required of the intended product, the system requirements analysis activity should include elicitation from the user community.

2—If a system consists of subsystems, the activities in 5.3.2 - System requirements analysis, should be performed iteratively with the activities in 5.3.3 - System architectural design, to define system requirements, design the system and identify subsystems, define the requirements for those subsystems, design the subsystems and identify their components, and so on.

3—Each requirement should be stated in such a way that an objective test can be defined for it.

4—The developer should analyze acquisition requirements concerning computer hardware resource utilization (e.g., maximum allowable use of processor capacity, memory capacity, input/output device capacity, auxiliary storage device capacity, communications/network equipment capacity). If there are no acquisition requirements concerning computer hardware resource utilization, or they are very general, the developer should establish appropriate utilization requirements as part of the system requirements activity. Establishing utilization requirements should be an activity iterated with design activities.

5—The definition of system safety and security requirements should also include what the system must not do.

5.3.4 Software requirements analysis. For each software item (or software configuration item, if identified), this activity consists of the following tasks:

5.3.4.1 The developer shall establish and document software requirements, including the quality characteristics specifications, described below. Guidance for specifying quality characteristics may be found in ISO/IEC 9126.

a) Functional and capability specifications, including performance, physical characteristics, and environmental conditions under which the software item is to perform;

b) Interfaces external to the software item;

c) Qualification requirements;

d) Safety specifications, including those related to methods of operation and maintenance, environmental influences, and personnel injury;

e) Security specifications, including those related to compromise of sensitive information;

f) Human-factors engineering (ergonomics), including those related to manual operations, human-equipment interactions, constraints on personnel, and areas needing concentrated human attention, that are sensitive to human errors and training;

g) Data definition and database requirements;

h) Installation and acceptance requirements of the delivered software product at the operation and maintenance site(s);

i) User documentation;

j) User operation and execution requirements;

k) User maintenance requirements.

GUIDANCE:

1—ISO/IEC 9126 identifies six quality characteristics to be included: functionality, reliability, usability, efficiency, maintainability, and portability.

2—All items, 5.3.4.1 a) through 5.3.4.1 k), should be stated in such a way that objective criteria may be defined for them.

3—Guidance regarding software safety plans may be found in IEEE Std 1228.

5.5 Maintenance process

5.5.2 Problem and modification analysis. This activity consists of the following tasks:

5.5.2.1 The maintainer shall analyze the problem report or modification request for its impact on the organization, the existing system, and the interfacing systems for the following:

- a) Type; for example, corrective, improvement, preventive, or adaptive to new environment;
- b) Scope; for example, size of modification, cost involved, time to modify;
- c) Criticality; for example, impact on performance, safety, or security.

6 Supporting processes

6.1 Documentation process

6.1.2 Design and development. This activity consists of the following tasks:

6.1.2.1 Each identified document shall be designed in accordance with applicable documentation standards for format, content description, page numbering, figure/table placement, proprietary/security marking, packaging, and other presentation items.

GUIDANCE:

Documentation should also include or reference conventions needed to understand requirements, design, code, test, or other information. See IEEE/EIA 12207.0 H.5 for further guidance on the presentation form of life cycle data. Additional guidance on documentation of life cycle data may be found in IEEE/EIA 12207.1

6.1.3 Production. This activity consists of the following tasks:

6.1.3.1 The documents shall be produced and provided in accordance with the plan. Production and distribution

of documents may use paper, electronic, or other media. Master materials shall be stored in accordance with

requirements for record retention, security, maintenance, and backup.

6.2 Configuration management process

6.2.3 Configuration control. This activity consists of the following task:

6.2.3.1 The following shall be performed: identification and recording of change requests; analysis and evaluation of the changes; approval or disapproval of the request; and implementation, verification, and release of the modified software item. An audit trail shall exist, whereby each modification, the reason for the modification, and authorization of the modification can be traced. Control and audit of all accesses to the controlled software items that handle safety or security critical functions shall be performed.

GUIDANCE:

1—The principal focus of the requirements in this clause are those items, products, or entities directly associated with the software for the project, i.e., the planning and engineering information in computer files, electronic media, and documents describing the software, and the computer files and electronic media containing the software itself. While other items, products, or entities, such as reports or documents associated with the management and evaluation of those products, are to be controlled at some level, it is not the intention of IEEE/EIA 12207.0 to require all such items, products, or entities to be managed with the same degree of rigor.

2—Configuration control procedures should cover the levels of control through which each identified item, product, or entity is required to pass (for example, author control, project-level control, acquirer control); the persons or groups with the authority to authorize and make changes at each level; and the steps to be followed to request authorization for changes, process change requests, track changes, distribute changes, and preserve past versions. Changes that affect an

item, product, or entity already under acquirer control should be proposed to the acquirer in accordance with contractually established forms and procedures, if any.

6.2.6 Release management and delivery. This activity consists of the following task:

6.2.6.1 The release and delivery of software products and documentation shall be formally controlled. Master copies of code and documentation shall be maintained for the life of the software product. The code and documentation that contain safety or security critical functions shall be handled, stored, packaged, and delivered in accordance with the policies of the organizations involved.

GUIDANCE:

The release management and delivery requirements apply to the party that releases the software product.

6.4 Verification process

6.4.2 Verification

6.4.2.3 Requirements verification. The requirements shall be verified considering the criteria listed below:

- a) The system requirements are consistent, feasible, and testable.
- b) The system requirements have been appropriately allocated to hardware items, software items, and manual operations according to design criteria.
- c) The software requirements are consistent, feasible, testable, and accurately reflect system requirements.
- d) The software requirements related to safety, security, and criticality are correct as shown by suitably rigorous methods.

6.4.2.4 Design verification. The design shall be verified considering the criteria listed below:

- a) The design is correct and consistent with and traceable to requirements.
- b) The design implements proper sequence of events, inputs, outputs, interfaces, logic flow, allocation of timing and sizing budgets, and error definition, isolation, and recovery.
- c) Selected design can be derived from requirements.
- d) The design implements safety, security, and other critical requirements correctly as shown by suitably rigorous methods.

6.4.2.5 Code verification. The code shall be verified considering the criteria listed below:

- a) The code is traceable to design and requirements, testable, correct, and compliant with requirements and coding standards.
- b) The code implements proper event sequence, consistent interfaces, correct data and control flow, completeness, appropriate allocation timing and sizing budgets, and error definition, isolation, and recovery.
- c) Selected code can be derived from design or requirements.
- d) The code implements safety, security, and other critical requirements correctly as shown by suitably rigorous methods.

7 Organizational life cycle processes

7.2 Infrastructure process

7.2.2 Establishment of the infrastructure. This activity consists of the following tasks:

7.2.2.1 The configuration of the infrastructure should be planned and documented. Functionality, performance, safety, security, availability, space requirements, equipment, costs, and time constraints should be considered.

Annex F

(informative)

Use of reusable software products

F.1 Scope

This annex provides guidance on the incorporation of reusable software products.

F.2 Evaluating reusable software products

Examples of candidate criteria that may be used in evaluating reusable software products include, but are not limited to

- a) Ability to provide required capabilities and meet required constraints;
- b) Ability to provide required safety, security, and privacy protection;
- c) Reliability/maturity, as evidenced by established track record;
- d) Testability;
- e) Interoperability with other system and system-external elements;
- f) Distribution issues, including
 - 1) Restrictions on copying/distributing the software or documentation;
 - 2) License or other fees applicable to each copy.
- g) Maintainability, including
 - 1) Likelihood the software product will need to be changed;
 - 2) Feasibility of accomplishing that change;
 - 3) Availability and quality of documentation and source files;
 - 4) Likelihood that the current version will continue to be maintained by the producer;
 - 5) Impact on the system if the current version is not maintained;
 - 6) The acquirer's usage and ownership rights to the software product;
 - 7) Warranties available.
- h) Short-term and long-term cost impacts of using the software product;
- i) Technical, cost, and schedule risks and trade-offs in using the software product.

G.3 Candidate reviews

G.3.9 Software usability reviews

These reviews are held to resolve open issues regarding one or more of the following:

- a) The readiness of the software for installation at user sites;
- b) Status of training, including "training software products," if applicable;
- c) The user and operator manuals;
- c) The software version descriptions;
- e) The status of installation preparations and activities.

G.3.10 Software maintenance reviews

These reviews are held to resolve open issues regarding one or more of the following:

- a) The readiness of the software for transition to the maintenance organization;
- b) The software product specifications;
- c) The software maintenance manuals;
- d) The software version descriptions;
- e) The status of transition preparations and activities, including transition of the software engineering environment, if applicable.

G.3.11 Critical requirement reviews

These reviews are held to resolve open issues regarding the handling of critical requirements, such as those for safety, security, and privacy protection

Annex J

(informative)

Category and priority classifications for problem reporting

J.1 Scope

IEEE Std 1044 may be useful in developing classifications for problem reporting.

J.2 Classification by category

The developer should assign each problem in software products to one or more of the categories in figure J.1.

Category Applies to problems in

- a. Plans One of the plans developed for the project
- b. Concept The operational concept
- c. Requirements The system or software requirements
- d. Design The design of the system or software
- e. Code The software code
- f. Database/data file A database or data file
- g. Test information Test plans, test descriptions, or test reports
- h. Manuals The user, operator, or maintenance manuals
- i. Other Other software products

Figure J.1—Categories to be used for classifying problems in software products

J.3 Classification by priority

The developer should assign each problem in software products or activities to one of the priorities in figure J.2.

Priority Applies if a problem could

- 1 a) Prevent the accomplishment of an essential capability
b) Jeopardize safety, security, or other requirement designated “critical”
- 2 a) Adversely affect the accomplishment of an essential capability and no work-around solution is known
b) Adversely affect technical, cost, or schedule risks to the project or to life cycle support of the system, and no work-around solution is known
- 3 a) Adversely affect the accomplishment of an essential capability but a work-around solution is known
b) Adversely affect technical, cost, or schedule risks to the project or to life cycle support of the system, but a work-around solution is known
- 4 a) Result in user/operator inconvenience or annoyance but does not affect a required operational or mission-essential capability
b) Result in inconvenience or annoyance for development or maintenance personnel but does not prevent the accomplishment of the responsibilities of those personnel
- 5 Any other effect

(ISO/IEC 12207) Standard for Information Technology— Software life cycle processes— Life cycle data April 1998

6 Specific information item content guidelines

6.5 Development process plan

6.5.3 Content: The development process plan should include

- a) Generic plan information (see 5.2 of this guide) for the following activities:
 - 1) Development process implementation;
 - 2) System requirements analysis;
 - 3) System architectural design;
 - 4) Software requirements analysis;
 - 5) Software architectural design
 - 6) Software detailed design;

- 7) Software coding and testing;
- 8) Software integration;
- 9) Software qualification testing;
- 10) System integration;
- 11) System qualification testing;
- 12) Software installation;
- 13) Software acceptance support.

b) Specific standards, methods, tools, actions, reuse strategy, and responsibility associated with the development and qualification of all requirements, including safety and security.

6.11 Project management plan

6.11.3 Content: The project management plan should include

- a) Generic plan information (see 5.2 of this guide) for managing the project;
- b) Project organizational structure showing authority and responsibility of each organizational unit, including external organizations;
- c) Engineering environment (for development, operation or maintenance, as applicable), including test environment, library, equipment, facilities, standards, procedures, and tools; © IEEE
- d) Work breakdown structure of the life cycle processes and activities, including the software products, software services and nondeliverable items to be performed, budgets, staffing, physical resources, software size, and schedules associated with the tasks;
- e) Management of the quality characteristics of the software products or services (Separate plans for quality may be developed.);
- f) Management of safety, security, privacy, and other critical requirements of the software products or services (Separate plans for safety and security may be developed.);
- g) Subcontractor management, including subcontractor selection and involvement between the subcontractor and the acquirer, if any;
- h) Quality assurance;
- i) Verification and validation, including the approach for interfacing with the verification and validation agent, if specified;
- j) Acquirer involvement (i.e., joint reviews, audits, informal meetings, reporting, modification and change, implementation, approval, acceptance, access to facilities);
- k) User involvement (i.e., requirements setting exercises, prototype demonstrations and evaluations);
- l) Risk management (i.e., the management of the areas of the project that involve technical, cost, and schedule risks);
- m) Security policy (i.e., the rules for need-to-know and access-to-information at each project organizational level);
- n) Approval required by such means as regulations, required certifications, proprietary, usage, ownership, warranty and licensing rights;
- o) Means for scheduling, tracking, and reporting;
- p) Training of personnel;
- q) Software life cycle model;
- r) Configuration management.

6.22 Software requirements description

6.22.3 Content: The software requirements description should include

- a) Generic description information (see 5.1 of this guide);
- b) System identification and overview;
- c) Functionality of the software item, including
 - 1) Performance requirements;
 - 2) Physical characteristics;
 - 3) Environmental conditions.

- d) Requirements for interfaces external to software item;
- e) Qualification requirements;
- f) Safety specifications, including those related to methods of operation and maintenance, environmental influences, and personnel injury;
- g) **Security** and privacy specifications, including those related to compromise of sensitive information;
- h) Human-factors engineering (ergonomics) requirements, including those for
 - 1) Manual operations;
 - 2) Human-equipment interactions;
 - 3) Constraints on personnel;
 - 4) Areas that need concentrated human attention and are sensitive to human errors and training.
- i) Data definition and database requirements, including installation-dependent data for adaptation needs;
- j) Installation and acceptance requirements of the delivered software product at the operation site(s);
- k) Installation and acceptance requirements of the delivered software product at the maintenance site(s);
- l) User documentation requirements;
- m) User operation and execution requirements;
- n) User maintenance requirements;
- o) Software quality characteristics;
- p) Design and implementation constraints;
- q) Computer resource requirements;
- r) Packaging requirements;
- s) Precedence and criticality of requirements;
- t) Requirements traceability;
- u) Rationale

6.26 System requirements specification

6.26.3 Content: The system requirements specification should include

- a) Generic specification information (see 5.7 of this guide);
- b) System identification and overview;
- c) Required states and modes;
- d) Requirements for the functions and performance of the system;
- e) Business, organizational, and user requirements;
- f) Safety, **security**, and privacy protection requirements;
- g) Human-factors engineering (ergonomics) requirements;
- h) Operations and maintenance requirements;
- i) System external interface requirements;
- j) System environmental requirements;
- k) Design constraints and qualification requirements;
- l) Computer resource requirements:
 - 1) Computer hardware requirements;
 - 2) Computer hardware resource requirements, including utilization requirements;
 - 3) Computer software requirements;
 - 4) Computer communications requirements.
- m) System quality characteristics;
- n) Internal data requirements;
- o) Installation-dependent data requirements;
- p) Physical requirements;
- q) Personnel, training, and logistics requirements;
- r) Packaging requirements;

s) Precedence and criticality of requirements;

t) Rationale.

NOTE—At the system level, the constraints on computer resources listed in item l) should be specified consistent with the degree of risk identified. The details of the resource requirements may be listed in supporting documents (e.g., system architecture and requirements allocation description, software requirements description, software architecture description).

ISO/IEC JTC1/ SC7

F.3 Organizational Life Cycle Processes

Date: 2001-07-08

ISO/IEC 12207:1995/FDAM

ISO/IEC JTC1/ SC7/ WG7/N0473

Secretariat: Standards Council of Canada

Information technology — Software life cycle processes

F.3.2 Infrastructure Process

Purpose:

The purpose of the *Infrastructure process* is to maintain a stable and reliable infrastructure that is needed to support the performance of any other process. The infrastructure may include hardware, software, methods, tools, techniques, standards, and facilities for development, operation, or maintenance.

Outcomes:

As a result of successful implementation of the *Infrastructure process*:

1. an infrastructure is established that is consistent with and supportive of the applicable process procedures, standards, tools and techniques;
2. the infrastructure will meet all requirements for functionality, performance, safety, security, availability, space, equipment, cost, time and data integrity.

Annex H (informative)

ISO/IEC TR 15504-2, PDAM1, Reference Model Extensions For the ISO/IEC 12207:1995 Acquisition Process

H.1.4 Technical Requirements

Purpose:

The purpose of the *Technical Requirements process* is to establish the technical requirements of the acquisition.

This involves the elicitation of functional and non-functional requirements that consider the deployment lifecycle of the products so as to establish a technical requirement baseline.

Outcomes:

As a result of successful implementation of the process:

1. the technical requirements, including environment effect evaluation, safety and security requirements where appropriate, will be defined and developed to match the needs and expectations of the users;
2. the current and evolving acquisition needs will be gathered and defined;
3. the requirements and potential solutions will be communicated to all affected groups;
4. a mechanism will be established to incorporate changed or new requirements into the established baseline;
5. a mechanism for identifying and managing the impact of changing technology to the technical requirements will be defined;

6. the requirements will include compliance with relevant standards, including environment effect evaluation, safety and **security** standards where appropriate.

i Some companies swapped out legacy technology for Web enabled technology to meet Y2k compliance. Others used funds earmarked for Y2k problems on new technology when serious problems did not materialize. [U.S. Fourth Quarter Computer Sales](#), Gartner Dataquest, Note Number: SRQS-US-MS-0101, March 26, 2001

ii [E-business: Not If, but when.mht](#), TechRepublic, April 12, 2000.

iii [Dot.com To Dot.bomb](#), BBC News: In-Depth Review, Dec. 15, 2000

iv [CSRC NIST Framework](#): The CSD umbrella framework addresses five major areas: [Cryptographic Standards and Applications](#), [Security Testing](#), [Security Research / Emerging Technologies](#), [Security Management and Guidance](#), [Outreach, Awareness and Education](#); Interoperability assessment framework: [Levels of Information System Interoperability \(LISI\) LISI Narrative.doc](#); Policy & Guidance frameworks: [Information Assurance Support Environment Policy & Guidance \(U.S. Gov/military\)](#); Hardware/op system framework: [Trusted Computing Platform Alliance Specification Document](#); Security Assessment framework: [Security Knowledge in Practice, Lawrence Rogers and Julia Allen. Crosstalk Nov 2002](#); The Network Rating Methodology: a Framework for Assessing Network Security, Sept. 11, 1997 [Network Security Rating Framework \(U.S. Navy\)](#).

v See [Intro To Security Risk Analysis](#); [Security Risk Assessment: How & Why](#); [Security Risk Analysis: The COBRA Approach](#)

vi See US Navy Defense in Depth: [Security For Network-Centric Warfare \(U.S. DoD\)](#), presents an overview of the layered strategy which addresses 4 concentric zones of protection. [How Intrusion Detection Systems Fit Into the Strategy](#), for instance, addresses a strategy for a detective control applied at Zone 4, the outermost network layer; [Security For Network-Centric Warfare \(U.S. DoD\)](#); Defense in Depth is part of a comprehensive security strategy that addresses all aspects of IA at levels of the OSI: [IATF Framework v3.1](#)

vii [IT Will Make Big Security Purchases](#), Enterprise Systems Newsletter, 101 Communications, Nov. 4, 2002.

viii [Study-System Admins Slow To Zap Bugs](#), CNET News, Nov. 19, 2002

ix [Economic Damage From Digital Risk Stabilising](#), mi2g, Oct. 22, 2002

x [Eli Lilly Privacy Case](#), Computerworld, July 25, 2002; Also, B2B communications are cited by Mike Rasmussen (GiGA Information Group) as perhaps the most difficult area for security. Most companies are prohibited from providing full disclosure on their network architecture design and external communications interfaces with partnering companies. Thus, it is highly conceivable that—whether authorized or unauthorized, an individual obtaining access to the network of one company, could conceivably use it as a conduit to access any other company network legitimately interfacing with the conduit company. This leaves company's at risk to market espionage by competitors or to trickle through malware attacks, regardless of how robust its own security strategy may be.

xi [Sarbanes-Oxley Act for Corporate Accountability](#), HR.3763 Sec. 404 requires Management Assessment of internal controls—including those controls that protect financial accounts from unauthorized access and tampering.

xii See: [Computer Crime Security Survey 2002](#), Power, R. (2002). Computer Security Issues & Trends. Vol. III, No. 1 (Spring), Computer Security Institute, <http://www.gocsi.com>.

xiii [CERT Incident Statistics, 1988-2002](#), Computer Emergency Response Team, Carnegie Mellon Institute, Nov. 25, 2002.

xiv See: "[Computer Security Journal Focuses on Information Warfare](#)", Computer Security Institute, January 20, 1999.

xv "Information Superiority is essential to our capability to meet the challenges of the 21st Century. It is a key enabler of Joint Vision 2010 and its four fundamental operational concepts of dominant maneuver, precision engagement, full dimensional protection and focused logistics – because each demands obtaining, processing, distributing and protecting accurate information in a timely manner while preventing our adversaries from doing so. Without achieving Information Superiority we will, very simply, not be able to achieve the goals established in Joint Vision 2010." Statement of The Honorable John J.Hamre, Deputy Secretary of Defense, 106th Congress. [Statement of The Honorable John J.Hamre, Deputy Secretary of Defense, 106th Congress](#) ;See also: [NISC](#)

xvi Regarding information protection, the FBI formed the infrastructure protection center and the national intellectual property rights coordination center. See: [FBI](#) and The Committee on National Security Systems references at [NTISSC](#).

Under Executive Order (E.O.) 13231 of October 16, 2001, Critical Infrastructure Protection in the Information Age, the President has re-designated the National Security Telecommunications and Information Systems Security Committee (NSTISSC) as the Committee on National Security Systems (CNSS); The acquisition policy (National Information Assurance Acquisition Policy, dated January 2000) and the C&A process (NSTISSI no. 1000 – National Information Assurance Certification and Accreditation Process, April 2000) were both updated; See also: GAO

xvii Clinger-Cohen Act at [CIT](#)

xviii [Northrop-Grumman](#)

xix [Trusted Computing Platform Alliance](#)

xx International Standard 15408, Common Criteria, Version 2.0, May 1998. See: <http://www.commoncriteria.org/cc/cc.html>;

xxi The Federal Government referenced Common Criteria in the making of its internal standard NSTISSI no. 1000 – National Information Assurance Certification and Accreditation Process, April 2000. See [NSTISSI 1000](#).

xxii Some institutions offer system certification services, such as [IRIA at Dartmouth](#). Industry leaders have worked to achieve national and international standards certification to provide confidence to consumers and businesses as the trustworthiness of their products. Examples include:

- Windows NT 4.0 was deemed C2 compliant on 02 December, 1999, as a result of an extensive survey performed according to the Trusted Computer Systems Evaluation Criteria (TCSEC)
- ORACLE 8i attained EAL 4 according to the Common Criteria
- Microsoft and Cisco are participating in the DoD MURI on Understanding Mobile Code.
- [Government Affiliated Research Institutes](#)
- From SUN Microsystems: [SUN](#)

xxiii See [CSRS](#), [NIAP](#) and [Defense Software Collaborators](#), [CSRC Projects Section](#)

xxiv At West Point, NPGS offer IA studies; See also [Iowa State University IA Program](#) and [CERIAS at Purdue](#).

xxv [CISSP Certification](#); This certification is offered by the International Information Systems Security Consortium, Inc., and is administered throughout the U.S. by the Information Systems Security Association [ISSA](#). The certification has been publicly recognized by the FTC. [GIAC Certification](#) is an offering of the highly respected SANS institute which offers courses throughout the use [SANS Training](#); The US Military requires Information Assurance training and certification for all personnel using DoD computer systems. [Military Required IA Certification](#); Tru Secure offers the TruSecure ICISA Certified Security Associate (TICSA) [TICSA Certification](#). CERT's training and education program offers licensing in its Octave Method for security evaluation, recommending follow up with its set of best practices. [CERT Training](#)

xxvi 20th National Information Systems Security Conference, 7-10 Oct 1997: [CSRC Conference Agenda](#)

xxvii Third Annual Information Assurance Workshop 17-19 June 2002, United States Military Academy, West Point, New York. See [IEEE Computer Society](#); also E-Gov sponsored conference on Information Assurance, September 2002: [E-Gov](#); See also Information Assurance Technical Framework Forum at [IATF](#)

xxviii See: [CSIRTS Training](#)

xxix See [humanfirewall.org](#);

xxx [SMI Results](#) courtesy Kimber Spradlin, PentaSafe Security Technologies, Inc., Nov. 2002.

xxxi [IEEE Position Statement](#) -Approved by the IEEE-USA Board of Directors, 20 June 2002; See also: [IEEE Computer Society Task Force on Information Assurance](#). The IEEE CIMC standard, Certificate Issuing Managing Components Family of Protection Profiles (CIMC), was vetted in the IEEE-SA.

xxxii A search of the IEEE Online Standards on keyword "security" returned 249 standards with references. Year 2002 is not counted, as it yields incomplete data for a partial year. Resource data can be found at: [IEEE Trends in Security Standards. Policy and Perception](#)

xxxiii A search of the IEEE Standards Websites for all references to security reveals 2534 references ranging from entries in discussion threads, society announcements, white papers and reports, press releases as well as standards. The top 10% sample--those deemed most relevant by the search engine (ranging from 42% to 55%)--suggests that between January 1, 1997 and Nov. 15, 2002 there has been a 67% increase in attention on the subject of security—46% of which has taken place within the last two years.

xxxiv See [IEEE Engineering Standards that Reference Security](#)

xxxv The clipper chip was an NSA designed tamperproof chip proposed to be embedded in every computer system. Its purpose was to tag and identify every communication session as well as encrypt data for transmission. It was introduced in 1993, but was abandoned in the late 90s due to the public outcry concerning government invasion of privacy. Palladium, another such invasive chip solution, and is at the heart of the Trustworthy Computing initiative endorsed by Microsoft and Intel, and currently is being met with the same public pressure as the clipper chip, for the same reasons. DES, the standard cryptographic algorithm effective since 1977 was thought to be extremely difficult to exploit. However, it was broken in 1998 after only three days of processing. It still remains the worldwide standard until localization issues can be overcome. See Harris, Shon, CISSP Certification “All In One” Study Guide, pp. 510-511, 525-526; <http://www.microsoft.com/PressPass/features/2002/jul02/0724palladiumwp.asp> <http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html>

xxxvi For insight into the difficult struggle of where/how much security should be applied at particular levels of the OSI, see <http://grouper.ieee.org/groups/802/3/efm/public/email/msg01898.html>; <http://grouper.ieee.org/groups/802/17/email/msg01534.html>; <http://grouper.ieee.org/groups/802/3/efm/public/email/msg01899.html>; <http://www.ieee802.org/3/efm/public/nov02/sec>; <http://grouper.ieee.org/groups/802/17/email/msg01539.html>; <http://grouper.ieee.org/groups/802/17/email/msg01531.html>

xxxvii [ISA Survey Results](#), 19 data points. (BBiszick, updated Dec. 12, 2002)

xxxviii See [ISO Security Search Results \(1-50\)](#) and [ISO Security Search Results \(51-98\)](#)