

# Information Security Standards: A Closer Look

By Vicente Aceituno Canal

## An International Article Brought to you from Spain

Standards avoid redundant research and knowledge management costs while narrowing the number of choices you have to make. It is very difficult to imagine how trade was undertaken before the introduction of the International System of Units, when basic units, sometimes with the same name, had different values from region to region.

Standards are just like any other agreement; some are broadly accepted, others are hardly applied at all. The success of a standard can be measured by the size and fidelity of the user base. Standards are normally of voluntary use, unlike laws, but the pressure to adopt a standard can be very high, like some standards that must be met to gain government contracts, or when a standard becomes a de facto industry standard.

There are a good many bodies, organizations and institutions that publish standards, constituted at national, transnational and international levels. Standards bodies normally cooperate trying to reduce overlaps between their interest areas, or distributing their responsibilities by regions. Standards set by these bodies are considered de iure standards, like ISO9001, while standards set by market forces are considered de facto standards, like JavaScript.

The main standardization bodies for information systems and security are:

### International Organizations

- ▼ IEC International Electrotechnical Commission.
- ▼ ISO International Organization for Standardization.
- ▼ ITU International Telecommunication Union.

### Volunteer Organizations

- ▼ IETF Internet Engineering Task Force.

### Private Industry Consortia

- ▼ OASIS Organization for the Advancement of Structured Information Standards.
- ▼ W3C World Wide Web Consortium.

### Professional Organizations

- ▼ IEEE Institute of Electrical and Electronics Engineers.
- ▼ ISSA Information Systems Security Association.
- ▼ ISACA Information Systems Audit and Control Association

### Private Research Institutes

- ▼ Software Engineering Institute.
- ▼ ISECOM

A national organization, the British Standards Institute is notable for being the leader in ISO quality and information security management standards.

## Standards Lifecycle

The lifecycle of a standard starts with the user base. Several organizations or companies might jump to the opportunity and might try to set a standard, creating a temporary standards inflation. These standards will be open or proprietary. Open standards are cheaper to implement and more likely to succeed, but the incentives to create a proprietary standard are high, as there are royalties to be made from those willing to enter or remain in the market after the proprietary standard becomes the most successful.

The competition between standards for user base can become fierce, leading to three or less surviving standards if users are lucky, as a multiplicity of standards have high costs in terms of interoperability. Sometimes there are partial victories, with different winners for different markets or regions, which happened in the VHS/Betamax wars. There are many reasons for this initial standards proliferation, like gaining a bigger market share, or because the proposed standards are perceived as not suitable for the market.

In any phase of the lifecycle of the standard, some intentional and unintentional incompatibilities might arise between implementations of the standard. Unintentional incompatibilities can arise from ambiguities in the standard specification, or simple poor implementation of the standard. Intentional incompatibilities can arise from proprietary extensions of the standard, or embrace and extend tactics that try to negate the advantages of standardization. The later tactic is used sometimes when a standard can menace the markets of a powerful and established player.

If the standard gets old enough, it can be improved upon and reach a high level of maturity, holding a sizeable chunk of the user base and covering well the needs of most users, leaving small room for incompatibilities or even getting some desirable features of the less successful or even failed standards.

Finally, when new developments undermine the user base, the standard will drift into obsolescence, with users flocking to upgrade to the new technology. When only one standard prevails in a certain area (standard monoculture), obsolescence can create a bad situation for new standards, as

they have to retain backwards compatibility if they are to gain market share. This can be costly or restrict the possibilities of the new technology.

Andrew Tanenbaum famously quipped that "The good thing about standards is that there are so many to choose from." This is one of several situations that could be called standard inflation, standard monoculture and standard starvation.

Standards inflation is the situation when more than two or three standards achieve relative success in terms of user base. This leads to interoperability costs that damage all the players, industry and users. Electrical plugs, for example, suffer standard inflation, as there are dozens of plugs that are very country specific. This is one of the reasons that killed the effective market influence of PKI, as almost every PKI advantage was negated by the wildly different ways it was implemented and the disparate ways of managing PKI infrastructures. Standards inflation can effectively prevent any standard to become the standard, as the user base might not find any advantage, like economy of scale of skills availability by using a particular standard over the others. This kind of situation can only be solved by broad agreements between the standard publishers, like the situation that gave birth to UML from the ashes of Booch, OMT, OOSE and Class-Relation modeling.

Standards monoculture is the situation when there is only one standard that takes virtually all the user base. This leads to a powerful network effect, as every user of the standard can interoperate with everyone else, increasing the value of using the standard. In this situation, improvements can only be brought forward incurring in the cost of backwards compatibility. The interlocking of two monoculture standards, Microsoft operating systems and x86 processors, led to a situation of slow development in the personal computing arena, as it was impossible for competing technologies to overcome this link. Computers makers were not willing to pay for operating systems, as they had to pay fees to MS even if they didn't install an MS operating system, and users couldn't use MS operating systems on non-x86 processors. If there had been suitable alternatives of operating systems and processors, other standards would have had emerged, making desktop computing evolution much faster.

Standards starvation is the situation when no organization undertakes the development and publication of a standard for the market need. In this situation, only de facto standards are available, which can be covered by patents and licenses and can lock many small players out of the market.

## Information Security Standards

The most successful information security standards are technical, especially those related to cryptography. The following areas of standardization can be considered as well covered and more or less successfully:

1. Certificate and Certificate Revocation Lists Management—PKIX / X.509 and matching RFCs.
2. Symmetric Encryption Algorithms—DES, AES, RC2, IDEA.
3. Asymmetric Encryption Algorithms—PKCS, Diffie-Hellman.
4. Time Stamping—TSP.
5. One-Way Hash Functions—SHA-x, MD5.
6. Digital Signature Algorithms—PKCS, DSA, MAC, HMAC.
7. Pseudo Random Number Generation—X9.82.
8. Intellectual Property Protection—FairPlay™, Microsoft® DRM.
9. Environment Hardening—CIS, NSA.
10. Secure Channel Formats—SSL, TLS, IPSEC, Ipv6, s versions of major

Internet Protocols.

11. Software Development Lifecycle Control—SSE-CMM, OWASP, SPSMM
12. Formats—S/MIME, XML, PKCS formats, OpenPGP.
13. Application Programming Interfaces—RFC2078 GSS-API, WSS.
14. Directories—LDAP, X.500, DNSSEC.
15. Authentication—SAML, Sender ID, Kerberos, RADIUS.
16. Authorization—RFC 2904 AAA Authorization Framework.
17. Deletion Standards—Gutmann, DoD 5220.22.
18. Time Keeping Standards—SNTP.
19. Products—ISO15408 Common Criteria, Trusted Platform Module (TPM), Trusted Network Connect (TNC) .
20. Management
  - a. 800-14 GAASP by National Institute of Standards and Technology.
  - b. Standard of Good Practice for Information Security from ISF.
  - c. SysTrust by AICPA.
  - d. ISO 17799 based on BS 7799 of the British Standards Institute.
  - e. ISO/IEC TR 13335-4 by ISO/IEC Joint Technical Committee 1.
  - f. Cobit by ISACA.
  - g. IT Baseline Protection by BSI
21. Risk Management
  - a. Magerit by Ministerio de Administraciones Públicas (Spain).
  - b. OCTAVE by Software Engineering Institute.
22. Alerts Monitoring—SVRRP by Organization for Internet Safety.
23. Handling of Incidents and Near-Incidents—ISO18044.
24. Vulnerability Assessment—OSSTMM from ISECOM.

On the other hand, there are many information security areas that are clearly lacking standards:

Technologies lacking standards:

- ▼ Digital Watermarking.
- ▼ Steganography.
- ▼ Logs syntax.

There are very few standards for:

- ▼ Governance.
- ▼ Responsibilities Partition, Segregation, Rotation and Supervision.
- ▼ Background Checks.
- ▼ Security Personnel Training.

There is no standard for the following assessments:


- ▼ Threat Assessment.
- ▼ Business Impact Analysis.
- ▼ ROSI Analysis.

There is no standard for the following management processes:

1. User Registration Management
2. Encryption Management
3. Change Control Management
4. Inventory Management
5. Physical Environment Protection Management
6. Operations Continuity Management
7. Incident Emulation Management

8. Segmentation Management
9. Malware Protection Management
10. Backup Management
11. Redundancy Management
12. Filtering Management
13. Events Detection and Analysis Management
14. Patching Management
15. Security Awareness
16. Classification and Prioritization of Information
17. Identification
18. Forensics

## Conclusion

Whereas having many standards can be a good thing, as it fosters competition, the lack of standards in certain areas are impeding advance of information security. Many businesses are reinventing the wheel over and over again, wasting million of dollars for this reason. User groups and professional organizations are normally in the best position to fill these gaps, as an open standard approach with a fast publishing process could give the maximum return for those involved. 

---

*Vicente Aceituno Canal has 12 years' experience in IT and security consulting. He leads the F.I.S.T information security conferences in Spain ([www.fistconference.org](http://www.fistconference.org)), authored the ISM3 (Information Security Management Maturity Model [www.isecom.org/ism3](http://www.isecom.org/ism3)), published his first book, Information Security, ISBN: 84-933336-7-0 last year, and maintains a Web site on personal computer security ([www.seguridaddelainformacion.com](http://www.seguridaddelainformacion.com)).*