ISI ISG Proposal

WW
29 March 2011

From: **ISG ISI (Information Security Indicators) Founding members**

To: **ETSI Director General, ETSI Board**

Subject: **ISG ISI (Information Security Indicators) initial Terms of Reference proposal**

1 Decision/action requested

The Director-General is requested to approve the creation, Terms of Reference,
and Membership Agreement for an ISG on Information Security Indicators;
and to appoint Mr. Gerard GAUDIN (G^{2}C) as Convenor for the first meeting.

2 References

ToRs clause 9.3.9	Responsibilities of the Director-General "…taking decisions on the creation or cessation of Industry Specification Groups, approving their terms of reference and reviewing their progress and work programmes…".
TWP clause 3	Operation of Industry Specification Groups

3 Rationale and Vision

A brief review of the Information Security Indicators field

With the current level of maturity of Information Security (IS), the focus in companies is applied more and more on security assurance and residual risk knowledge and treatment. This concern can be highlighted by the following two main issues:

- Are the organization’s practices compliant with its security policy or ISMS (Information Security Management System) and with what level of enforcement?
- Are existing security measures and tools effective?

These two issues can be dealt with in a harmonized and common way by relying on a global **reference framework** whose goal is to build a model based on several key features:

- Even emphasis on security incidents and vulnerabilities/non-conformities,
- Event-centric approach (consistent with the growing need for continuous monitoring and checking),
- Clear correspondence with ISO27002 points of control.

This reference framework is an event model which can lead to **accounting** through the selection of relevant and meaningful items, typically in the area of external or internal threats or of users’ deviant behaviours. The reference framework is an across the board one (all industry sectors), but can be refined for a specific sector or organization. Accounting makes it possible to derive **state of the art** figures, so long that the selected items lead to reasonably similar results depending on industries or organizations. Therefore, the key issue is to define a full set of measurements (typically 70 to 100), shared by the profession on a wide scale (at least European) through standardization. Moreover, this set of measurements must offer a relevant coverage, in order to give management a reasonable level of confidence as regards the continuous assessment of an organization’s security posture.

Standardization on this matter is essential because such a set of measurements has to be proven by sharing of experience and has to be widely published in order to stimulate sharing of figures within the IS profession. Such a trend could eventually lead to the emergence of widely recognized and reliable state-of-the-art statistics, and organizations could benefit greatly from them to assess themselves and benchmark the level of assurance and effectiveness of their security measures.

An urgent need

ETSI seems to be the relevant body to launch a **standardization** initiative on this matter, given its ICT and low time-to-market orientation. The urgency to move ahead is why the Club R2GS association (initiated by G²C) has been created in France by the end of 2008 with the purpose of building up hands-on reference frameworks in the new SIEM (Security Information and Event Management) and cyber defence field; this one concerns globally the Check and the Act of the well-known PDCA model in a continuous approach. This association, which gathers roughly 30 big companies and organizations from various industry sectors has produced 3 reference documents which are already used by many members (some on a world-wide scale). One of this document describes 74 IS Indicators (linked with the upper level ISO 27002 standard), which could be a basis for an ETSI standardization group.

The need for standardization in the SIEM field (exclusively product and engineering driven to the detriment of process implementation outside the US) has reached today a critical level that has led to a high rate of failures (3 to 4 times the usual rate in IT system projects). This concerns especially security event models, indicators and metrics, forensics practices and reference frameworks for reaction plans.

This situation is particularly harmful to organizations at a time when cyber attacks (crime or state-sponsored) are more and more aggressive, and when powerful detection and reaction means and processes are therefore urgently required. Special industry sectors targeted in particular **suffer huge loss** of intellectual property (for example, the ones with advanced R&D) and of reputation (for example e-commerce with publicized private data breaches).

Existing relating trends

Some fundamental trends have surfaced through several initiatives launched recently that may shed light on the increasing need for reliable figures. It is said that information security is one of the few management disciplines that has yet to submit itself to real analytic scrutiny, which includes notably the "hard data" IS needs today (similar for example to those regarding physical security such as fire or burglary). The above-mentioned initiatives are the following (major ones):

- US Computer Security Institute (CSI) annual survey carried out for 5 years, based on its own event model and a set of 100 polled organizations, and leading to 50 key figures regarding security incidents (malice, carelessness, breakdowns and accidents),
- Verizon data breach investigations 2009 and 2010 reports, based on 4 years of forensic research and more than 500 cases, which can be considered as narrower surveys but probably more dependable than the previous one,
- The European BUGYO Beyond project, whose aim is to build a global continuous security assurance methodology and framework based on a service oriented modelling of communication infrastructure, in order to share security assurance information between Telco entities and organizations,
- The Think-Trust recommendations (interim) report funded by the European Commission's 7th Framework ICT Programme, dated 01/06/2010, mentions 10 research & development challenges, including Management and Governance which specifies in particular (page 16/22) "Continuity of security relationships within these dynamic environments must also be appropriately managed", elsewhere requiring "A framework for consistent expression and interpretation of security policies" (page 16/22), which is something very similar and very close to the framework described in the introduction,
- The US CAG (Consensus Audit Guidelines) initiative, which has defined a set of 20 critical controls which are a perfect, risk-based subset of the NIST 800-53 Priority One controls, and that measure security effectiveness. The goal is to help organizations test their security compliance. This initiative is considered to be a breakthrough insofar as it enables to enter a new era of continuous checking with a very efficient set of controls against external attacks.

Those initiatives or projects are aimed at providing guides to practically implement and use the notions of security assurance, trust and dependability, and to help managers take the appropriate decisions and steps regarding security investments.

But all these initiatives **still lack** either sharing among the profession or detailed indicators (as the ones presented above). The future to build is to reconcile and bridge the gap between initiatives such as the CAG one and the one presented here.

Possible impacts

The various results stemming from the availability of a new standard may be the following:

- Basis for an across the board indicators framework to be published at least at the European level in all industry sectors (which could complement the US S-CAP standard initiative, which deals in particular with naming and categorizing vulnerabilities and nonconformities),
- Basis for establishment of a global European state of the art, with the possible build up of a centralized database (on the same model as US large databases, such as the Identity Theft Resource Center and DataLossDB),
- Basis for a full set of metrics to evaluate the quality and actual effectiveness of protection equipment.

4 Terms of Reference for ETSI ISG on Information Security Indicators [TWP D.3, Part Aa)]

4.1 Scope

The Information Security Indicators ISG ("ISG ISI") will develop ETSI Group Specifications for Information Security Indicators. The activities carried out within ETSI ISG ISI aim to:

- Summarize the existing results on similar activities related to measurement and metrics,
- Develop and build up a full set of Information Security Indicators (with the goal to become an ETSI Group Specification), that will be the basis for further state-of-the-art figures,
- Select the relevant Priority One Indicators (with a detailed description in compliance with the ISO 27004 standard),
- Develop an underlying Security Event Classification Model (with the goal to become an ETSI Group Specification), linked and consistent with the set of IS Indicators,
- Disseminate the results outside the ETSI community,
- Define a possible implementation of a subset of Indicators, with definition of the relevant monitoring tools and/or methods (with the goal to become an ETSI Group Specification).
- Encourage the innovation and pragmatism in inviting for contributions from the circles of both users companies and providers, towards developing common reference draft,

4.2 Membership

Membership in ISG ISI is restricted in accordance with Clause 3.4 of the ETSI Technical Working Procedures to ETSI members and applicants for membership, who have signed the ISG agreement.

Observers and non-members of ETSI may not become members of the ISG but may participate in the ISG according to the rules as described in the ISG Participant Agreement. Participation of non-members of ETSI is subject to acceptance of the ISG Participant Agreement, and payment of a per-meeting participation fee as described in the ISG Participant Agreement.

Electronic access to ISG documents (if provided) is removed from Participants if they fail to participate in, or register and pay for participation in any ISI ISG meeting for 6 months, or in two successive meetings of the ISG if they are separated by more than 6 months. This access is restored when they resume participation in the ISG. An ISG Participant Agreement may be terminated if the Participant fails to participate in an ISG meeting during a 12 months period.

4.3 Dues

Dues for membership and operation are fixed on an annual basis by the members of ISG ISI, based on the costs the members anticipate to incur.

For the initial year of operation of the ISG, no costs are anticipated therefore there are no membership fees for the initial year.

Observers and non-members of ETSI are required to pay a per-meeting participation fee as described in the ISG Participant Agreement. This per-meeting fee is set initially at €100 (excluding taxes) per person per meeting day. These fees may be modified by a decision of the members of the ISG.

4.4 Duties and Rights of Members

Members have the duty to constructively cooperate on the development of ISG Group Specifications. Members have the right to cast their vote on the approval of a specification when necessary, and in other instances when decisions by the members are required. Members have the right to appeal directly to the ETSI Board to challenge a Chairman's decision.

Voting is on a one-member one-vote basis, and voting rights are dependent on regular participation in the ISG: members are required to have participated in at least one of the three meetings preceding any vote in order to have the right to vote.

4.5 Term of office of chairman, vice-chairmen and working group chairmen

The chairman, vice-chairmen and working group chairmen of ISG ISI are appointed for a period of 2 years. After each period they may be re-appointed.

4.6 Preparation of Group Specifications

Group specifications are prepared within the ISG or within specific working groups. Working groups are chaired by working group chairmen, who are appointed according to the rules of operation of the ISG. All draft specifications must be approved by the ISG members using the decision making process detailed in the rules of operation of the ISG. If a specification is prepared in a working group and fails to be approved by the members, it is referred back to the working group.

4.7 Convening an ISG meeting

The rules for convening meetings follow the same principles as those laid down in Clause 1.5 of the ETSI Technical Working Procedures, with the deviations detailed in Annex 5 of the ISG ISI Agreement for ETSI Members.

In particular, invitations to ISG ISI meetings shall be disseminated at least 30 days before each meeting.

The first meeting of a new Industry Specification Group will be announced in a Collective Letter, with at least 30 days notice, by the ETSI Secretariat.

Further, the draft agenda shall be disseminated by the responsible Chairman to all on the Industry Specification Group membership list at least 21 days before a meeting.

5 ETSI field of interest [TWP D.3, Part Ab)]

See § 3 “Rationale and vision” (An urgent need + possible impacts).

6 Why any overlapping or complementary elements (with reference to existing work or Terms of Reference of any existing Technical Committee or Project) is regarded as desirable [TWP D.3, Part Ac)]

There is no overlap of any sort with the existing Technical Committees or Projects or ISGs.

7 Time plan [TWP D.3, Part Ad)]

The ISG is expected to remain open for at least 2 years. It may remain in activity for longer, or it may be absorbed into formal standardization in an ETSI Technical Body.

8 Chairmanship [TWP D.3, Part Ae)]

Mr. Gérard Gaudin of G²C (ETSI Applicant Member) has accepted to stand as convenor for the first meetings and has expressed willingness for the candidacy for Chairman of the ISG.

9 Resource requirements [TWP D.3, Part Af)]

No resource requirements, beyond the "basic administrative support" provided by the ETSI Secretariat to ISGs, have been identified. Further resource requirements may be identified from time to time by the ISG members, who will decide on the funding arrangements as required.

10 ETSI Secretariat resources [TWP D.3, Part Ag)]

"Basic administrative support" will be provided by the ETSI Secretariat, e.g.:

- Info/meeting/document handling area on the ETSI Portal.
- e-mail lists provision, depending on the number of ISG members
- Entry of the Work Items into the WPM database (provided by ESP).
- Processing/publication of ETSI Deliverables (providing they have respected the ETSI Drafting Rules).
- Meetings and premises organization
- A support officer will be allocated to provide guidance and assistance to the ISG.

Support for meetings will be provided when the meeting is held at the ETSI Headquarters, e.g.:

- Meeting rooms in ETSI premises.
- Meeting support for invitations, badges, etc in ETSI premises.
- Tea/coffee in ETSI premises.

Meetings held outside of the ETSI Headquarters shall be supported by the hosting member organization.

11 ISG membership agreement [TWP D.3, Part Ah)]

See Annex of this document.

12 ETSI full and/or associate members having declared their willingness to provide resources [TWP D.3, Part Ba)]

The following ETSI members have indicated that they are willing to support the ISG (at least four required):

Bouygues Telecom
CASSIDIAN (Until 17 September 2010 it was known as EADS Defence & Security)
G²C
Institut Telecom
Alcatel-Lucent

The following non-members of ETSI have also expressed an interest in participating in the work of the ISG:

BNP Paribas
CEIS
Groupe La Poste (The French Post Office)
Caprioli & Associés

13 Planned deliverables and their delivery dates shall be identified [TWP D.3, Part Bb)]

At the point of writing this proposal, 3 main Group Specification deliverables have been planned:

- A full set of Information Security Indicators, to be delivered 15 months after the beginning of the ISG,
- A Security Event Classification Model, consistent with the previous standard, to be delivered 6 to 9 months later,
- A possible implementation of a subset of indicators, with definition of the relevant monitoring tools and/or methods, to be delivered 4 months later.

14 Internal organization [TWP D.3, Part Bc)]

No internal organization or Working Groups have yet been identified. This will depend on the results of the initial work of the ISG.

15 Any committee/project-external ETSI resources required (i.e. outside those provided by the Industry Specification Group participants) shall be specified [TWP D.3, Part Bd)]

A Special Task Force may be required in order to collect existing statistical figures available for some key indicators. The ISG members will be obliged to find their own source of funding for this activity, if it is considered necessary.

16 Maintenance arrangements for deliverables shall be specified [TWP D.3, Part Be)]

The maintenance of any Group Specification will be assured by the ISG. At the end of the work the ISG shall define the follow-on responsibility for any required maintenance.

17 The relationship with ETSI Technical Organisation shall be specified (i.e. list the interfaces between the ISG and ETSI TBs) [TWP D.3, Part Bf)]

The ISG has no need to use existing ETSIDeliverables, given the positioning of security matters.