ETSI GS ISI 001-1 V1.1.1 (2013-04)

Information Security Indicators (ISI); Indicators (INC); Part 1: A full set of operational indicators for organizations to use to benchmark their security posture

Disclaimer

This document has been produced and approved by the Information Security Indicators (ISI) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
DGS/ISI-001-1

Keywords
ICT, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
 http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services: http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Group Specification (GS) has been produced by ETSI Industry Specification Group (ISG) Information Security Indicators (ISI).

The present document is part 1 of a multi-part deliverable covering the Information Security Indicators (ISI); Indicators (INC), as identified below:

Part 1: "A full set of operational indicators for organizations to use to benchmark their security posture";

Part 2: "Guide to select operational indicators based on the full set given in part 1".

The present document is included in a series of 6 ISI 00x specifications. These 6 specifications are the following (see figure 1 summarizing the various concepts involved in event detection and interactions between all specifications):

- The present document addressing (together with its associated guide GS ISI 001-2 [3]) information security indicators, meant to measure application and effectiveness of preventative measures.

- GS ISI 002 [4] addressing the underlying event classification model and the associated taxonomy.

- GS ISI 003 [i.5] addressing the key issue of assessing organization's maturity level regarding overall event detection (technology/process/ people) and to weigh event detection results.

- GS ISI 004 addressing demonstration through examples how to produce indicators and how to detect the related events with various means and methods (with a classification of the main categories of use cases/symptoms).

- GS ISI 005 [i.2] addressing ways to produce security events and to test the effectiveness of existing detection means within organization (for major types of events), which is a more detailed and a more case by case approach than ISI 003 one and which can therefore complement it.

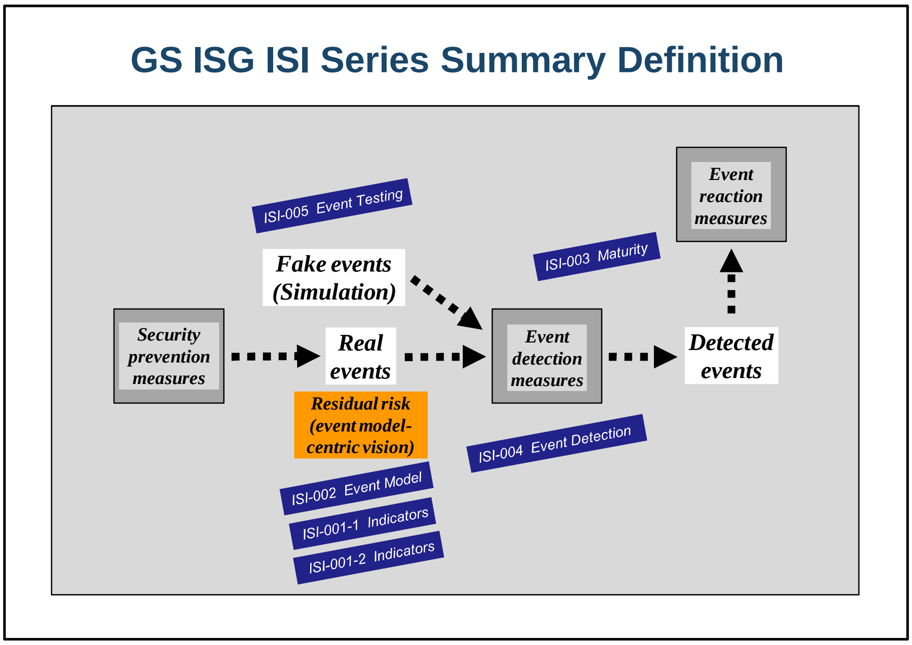

Figure 1: Positioning the 6 GS ISI 00x against the 3 main security measures

Introduction

Over the course of recent years, a general consensus has progressively taken shape within the industry, recognizing that the security benchmarking of IT systems was worthwhile, on an equal footing with what is done in some other areas or disciplines such as quality or management. In other words, it seems possible to perform an objective assessment of the **application and effectiveness** of a security policy or, more generally, of an Information Security Management System (ISMS) and of the **residual risk** (see chart in introduction of GS ISI 002 [4], which highlights the 2 associated types of events - **incidents and vulnerabilities** - and the joint area covered by IT security policy through the concept of usage or implementation drift). Initial confirmation of this shared belief began to be seen worldwide in various sources of highly converging figures, notably the figures from some advanced Cyber Defense and SIEM (Security Information and Event Management) projects in the USA and Europe, through reliable and very refined operational indicators dealing with both incidents and vulnerabilities. This emergence of security **state-of-the-art figures** (proving a trend towards practical outcomes as much as sheer compliance) also made it possible:

- To bring to light the types of indicators that can under no circumstances serve as reference points (in particular, ones that are too risk-oriented and consequently specific to a given industry sector), and to determine the ones that are common to all industry sectors and situated on the right level (see the associated event classification model in GS ISI 002 [4]),

- To map these indicators to the 11 domains of the ISO/IEC 27001/2 standards [6], [2] to assess continuously the application and effectiveness of an existing ISMS (Continuous Checking), to the ISO/IEC 27006 standard on ISMS audit, and to ISO/IEC 27004 [1] that primarily relates to security indicators.

Furthermore, to meet the requirements of governance (need for executive summary) and accuracy (need for clear description), the idea is to tag and organize them according to the underlying event classification model and the associated taxonomy, making it therefore possible to group them based on various criteria (origin, type of action, type of asset impacted, type of impact, etc.) and to build a **pyramidal structure** with different level of more and less aggregated indicators (with high flexibility). Each incident and each vulnerability will be described following a structured language.

The typical list of some **90 indicators** and their **10 to 15 possible derived and consolidated indicators** (as provided in the present GS), generally shared by most advanced Cyber Defense and SIEM projects, is meant as a priority to CISOs, in order to help them assessing and enforcing their company's or organization's IT security governance. Some of them or some aggregates of them may also be used by Operational Risk Managers, CIOs and senior executives by providing them with an **overview of trends, drifts or progress** as regards organization's whole security posture. However, the proposed list of indicators is more or less in wide-spread use, leading to group them into 4 distinct categories, each with different maturity levels:

- Well-known with accidental security incidents (i.e. breakdowns and natural disasters).
- Better and better defined with security incidents of the malicious and unawareness type (external intrusions and attacks, internal deviant behaviours).
- Little developed with impact measurements.
- Very little developed with behavioural, software, configuration and general security vulnerabilities.

A question remaining is **how to use this GS** and select the relevant indicators, which depend on organization's existing ISMS. In this regard, the proposed range of indicators should be considered as a simple but representative ground work, from which a selection can be made by completely relying on the existing ISMS. Proceeding in this manner will lead to a series of unique indicators that are specific to each organization, amongst which a first part will typically consist of specific indicators, with a second part consisting of a sub-set of the list given in the present document. The main characteristic of the former will be "effective ISMS implementation", while that of the latter will be more "operational". As such, the structuring side of the ISMS will clarify and validate the choice of a given indicator from the proposed ground work.

A second aspect to consider in the use of the present GS is the dispersal or not of the proposed state-of-the-art figures, a state that can be directly associated with their greater or lesser "universal" reference quality (which in some extreme cases can go so far as production impossibility). As such, the summary table proposed in clause 5.7 brings to light the indicators with high convergence, which it is therefore possible to rely on with full trust in order to carry out benchmarking within one's organization or one's company.

These considerations together with mapping with various reference frameworks and contexts are addressed in a separate **Guide** called **GS ISI 001-2 [**3**]**. Another completely different use of indicators, which is worth mentioning here, is also being dealt with in this Guide; it consists of applying them to the field of **security product certification** (with ISO 15408).

It should be finally mentioned that the present GS rests partly on a work carried out by Club R2GS (see annex D), a French association created during 2008, specializing in Cyber Defence and Security Information and Event Management (SIEM). This association brings together a large number of representatives from many of the bigger French institutions (mainly users) concentrating on those that are the most advanced in the Cyber Defence and SIEM field. The present document (and associated GS ISI 001-2 [3]), as well as all other GS ISI 00x, is therefore **based on sound experience**, this community of users having adopted and used the set of indicators and the related event classification model sometimes for more than 3 years and sometimes on a world-wide scale. Moreover, it should be added that a survey amongst the members proved the existence of a large core of indicators shared by most of them (30 %). This core mainly overlaps the set of indicators mentioned as Priority 1 in clause 5.7 (Recap of state-of-the-art figures), thus strengthening their level of dependability.

1 Scope

The present document provides a full set of information security indicators (based on already existing results and hands-on user experience), covering both security incidents and vulnerabilities. These one become nonconformities when they violate organization's security policy. The present document is meant to aid CISOs and IT security managers in their effort to evaluate and benchmark accurately their organization's security posture. GS ISI 001-2 [3] gives precise instructions on how to use the present document and select indicators.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

[1] ISO/IEC 27004:2009: "Information technology -- Security techniques -- Information security management - Measurement".

[2] ISO/IEC 27002:2005: "Information technology -- Security techniques -- Code of practice for information security management".

[3] ETSI GS ISI 001-2: "Information Security Indicators (ISI); Indicators (INC); Part 2: Guide to select operational indicators based on the full set given in part 1".

[4] ETSI GS ISI 002: "Information Security Indicators (ISI); Event Model; Part 2: A security event classification model and taxonomy".

[5] SANS Consensus Audit Guidelines V4.0: "20 Critical Security Controls for Effective Cyber Defense".

NOTE: See http://www.sans.org/critical-security-controls/ for an up-to-date version.

[6] ISO/IEC 27001:2005: "Information technology -- Security techniques -- Information security management systems -- Requirements".

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the organization with regard to a particular subject area.

[i.1] NIST SP 800-55 Rev. 1 (July 2009): "Performance Measurement Guide for Information Security".

[i.2] ETSI GS ISI 005: "Information Security Indicators (ISI); Event Testing; Part 5: Event Testing".

[i.3] NIST SP 800-126 Rev. 2 (Sept. 2011): "The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2".

[i.4] NIST SP 800-53 Rev. 3 (August 2009): "Recommended Security Controls for Federal Information Systems and Organizations".