ETSI GS ISI 001-2 V1.1.2 (2015-06)

Information Security Indicators (ISI); Indicators (INC); Part 2: Guide to select operational indicators based on the full set given in part 1

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
RGS/ISI-001-2ed2

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

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (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:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Contents

List of figures

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 2 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 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 base list of indicators described in ETSI GS ISI 001-1 [5]) information security indicators, which are meant to measure application and effectiveness of preventative measures.
- ETSI GS ISI 002 [9] addressing the underlying event classification model and the associated taxonomy.
- ETSI GS ISI 003 [i.12] addressing the key issue of assessing organization's maturity level regarding overall event detection (technology/process/ people) and to weigh event detection results.
- ETSI GS ISI 004 [i.13] 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).
- ETSI GS ISI 005 [i.14] 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 the ETSI GS ISI 003 [i.12] and which can therefore complement it.

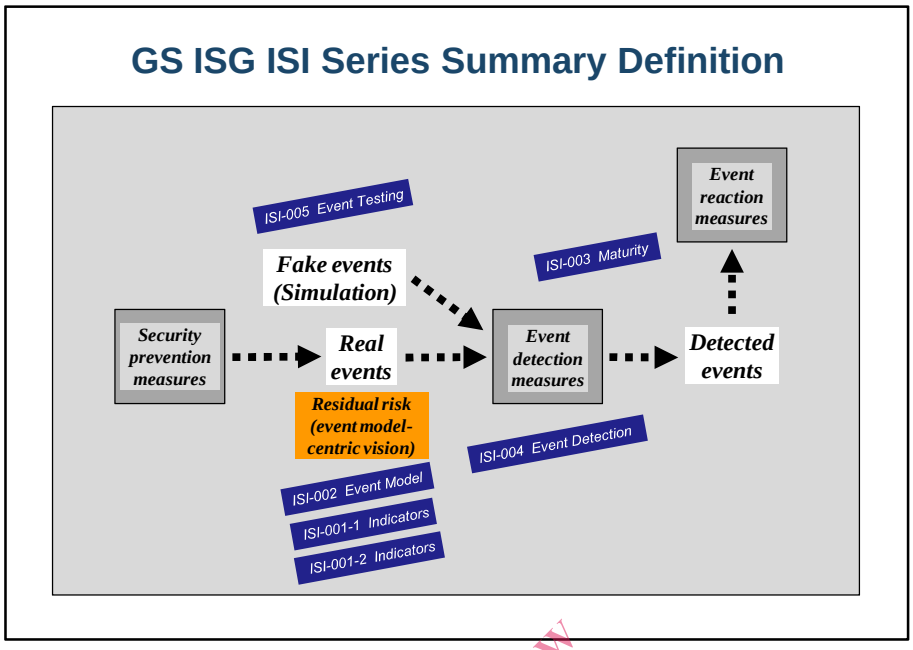

Figure 1: Positioning the 6 GS ISI against the 3 main security measures

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

Given that ETSI GS ISI 001-1 [5] indicators are positioned at the crossroads of governance and operational matters and may have to rest on global reference frameworks, it is key to help in this alignment and in the **use of ETSI GS ISI 001-1 [5] for selection of the appropriate indicators**.

As regards organization's existing ISMS which constitutes the prime security governance tool, the ETSI GS ISI 001-1 [5] proposed range of indicators should be considered as a simple but representative ground work, from which to make a selection while 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, while a second part consists of a sub-set of the list given in ETSI GS ISI 001-1 [5]. 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. For that purpose, various reference frameworks and contexts should be addressed, such as ISO/IEC 27002 [1] (first of all) and the Consensus Audit Guidelines [4] (sub-set of Priority One NIST SP 800-53 [i.9] controls), but also the more extended frameworks COBIT [3] and ISO/IEC 20000 (ITIL) [i.1] and [i.2].

Another different benefit of the indicators is being introduced with in this guide; it consists of linking them to the field work of **IT security evaluation** (with ISO/IEC 15408 [i.3], [i.4], [i.5] and ISO/IEC TR 17791 [i.15]).

1 Scope

The present document provides a guide to use the range of indicators provided in ETSI GS ISI 001-1 [5]. The present document is meant mainly to support CISOs and IT security managers in their effort to evaluate and benchmark accurately their organization's security posture.

2 References

2.1 Normative 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 reference 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.

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

[1] ISO/IEC 27002:2013: "Information technology - Security techniques - Code of practice for information security controls".

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

[3] ISACA COBIT V4.1: "The Control Objectives for Information and related Technology".

NOTE: See http://www.isaca.org/Knowledge-Center/cobit/Pages/Downloads.aspx.

[4] SANS Consensus Audit Guidelines V5: "20 Critical Security Controls for Effective Cyber Defense".

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

[5] ETSI GS ISI 001-1: "Information Security Indicators (ISI); Indicators (INC); Part 1: A full set of operational indicators for organizations to use to benchmark their security posture".

[6] ISO/IEC 27001:2013 : "Information technology - Security techniques - Information security management systems - Requirements".

[7] ISO/IEC 27006:2011: "Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems".

[8] ISO/IEC 27000:2012: "Information technology - Security techniques - Information security management systems - Overview and vocabulary".

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

2.2 Informative 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 reference document (including any amendments) applies.

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

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

[i.1] ISO/IEC 20000-1: 2011: "Information technology - Service management - Part 1: Service management system requirements".

[i.2] ISO/IEC 20000-2:2012: "Information technology - Service management - Part 2: Guidance on the application of service management systems".

[i.3] ISO/IEC 15408-1:2009: "Information technology - Security techniques - Evaluation criteria for IT Security - Part 1: Introduction and general model".

[i.4] ISO/IEC 15408-2:2008: "Information technology - Security techniques - Evaluation criteria for IT Security - Part 2: Security functional components".

[i.5] ISO/IEC 15408-3:2008: "Information technology - Security techniques - Evaluation criteria for IT Security - Part 3: Security assurance components".

[i.6] ISO/IEC 27007:2011: "Information technology - Security techniques - Guidelines for information security management systems auditing".

[i.7] ISO/IEC TR 27008:2011: "Information technology - Security techniques - Guidelines for auditors on information security controls".

[i.8] ISO/IEC TR 19791:2010: "Information technology - Security techniques - Security assessment of operational systems".

[i.9] NIST SP 800-53: "Recommended Security Controls for Federal Information Systems and Organizations".

[i.10] ISO/IEC 27003:2010: "Information technology - Security techniques - Information security management system implementation guidance".

[i.11] ISO/IEC 27005:2011: "Information technology - Security techniques - Information security risk management".

[i.12] ETSI GS ISI 003: "Information Security Indicators (ISI); Key Performance Security Indicators (KPSI) to evaluate the maturity of security event detection".

[i.13] ETSI GS ISI 004: "Information Security Indicators (ISI); Guidelines for event detection implementation".

[i.14] ETSI GS ISI 005: "Information Security Indicators (ISI); Event Testing; Part 5: Event Testing".

[i.15] ISO/IEC TR 17791:2013: "Health informatics -- Guidance on standards for enabling safety in health software".

[i.16] NIST 800-126: "Technical Specification for the Security Content Automation Protocol (SCAP)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ISO/IEC27000 [8] and the following apply:

NOTE: See also figure 2 at the end of this clause.

asset: information asset that has value to the organization and that can be broken down in primary assets (such as business activities, data, application software, etc. which hold the business value) and secondary/supporting assets (network or system infrastructure, which host primary assets)

assurance: planned and systematic activities implemented in a management system so that management requirements for a service will be fulfilled

NOTE: It is the systematic measurement, comparison with a standard, monitoring of processes and an associated feedback loop that confers error prevention. This can be contrasted with Management "Control", which is focused on process outputs.

base measure: measure defined in terms of an attribute and the specified measurement method for quantifying it

NOTE: E.g. number of trained personnel, number of sites, cumulative cost to date. As data is collected, a value is assigned to a base measure.

continuous checking: constant checking of a series of controls identified within the Information System, corresponding with the detection of incidents and of software, configuration, behavioural or global security framework vulnerabilities and/or non-conformities

NOTE: There are three checking levels (in principle, hierarchy notably implemented within banking and financial institutions):

- Detailed behavioural, global security framework or technical checking at the security software or equipment level (network, system, application software).
- Level 1 checking via monitoring of trends and deviations of a series of significant measurement points.
- Level 2 checking (verification of existence of a satisfactory assurance and coverage level of the chosen control and measurement points, and of implementation of regulatory requirements).

Continuous checking can also be either manual or automatic (for example, monitoring by means of tools suited to a SIEM approach). Finally, a continuous checking is generally associated with statistical indicators (levels of application and effectiveness of security controls), that are intended to provide information as regards the coverage and assurance level of the security controls in question.

criticality level (of a security event): level defined according to the criteria which affect its potential impact (financial or legal) on the company assets and information and which make it possible to evaluate the appropriate level of reaction to the event (incident treatment or vulnerability or nonconformity suppression)

NOTE: The criticality of a given event is determined by its severity (inherent to the event itself - see definition above) and by the sensitiveness of the target attacked or concerned (linked to the asset estimated value for the company - which value concerns the confidentiality, the integrity or the availability). This concept of criticality level (usually defined on a scale of four levels) is at the core of any SIEM approach, for which forming security events processing into a hierarchy is vital from both a security and economic point of view.

derived measure: measure derived as a function of two or more base measures

effectiveness (of security policy or of ISMS): complementary concept to application of security policy, that can be estimated through identified residual risk (that corresponds with the residual vulnerabilities that are actually exploited and that have led to security incidents)

NOTE: It should be added that the term **"Efficiency"** is sometimes also used, but generally with a different meaning of economy in the use of resources (not addressed here for reasons of lesser relevancy).

(security) incident: single or series of unwanted or unexpected security events that correspond with an existing vulnerability exploitation (or attempt of), and with an actual or potential threat (attempt underway), that have a significant probability of compromising business operations and threatening information security

NOTE: In case of success, an incident affects nominal operations of all or part of an information system (according to the Confidentiality, Integrity and Availability criteria - English acronym CIA). If an incident is new and a complex combination of more basic incidents and cannot be qualified and therefore inventoried or categorized, reference is then often made to an anomaly.

indicator: measure that provides an estimate or evaluation of specified attributes derived from an analytical model with respect to a defined information need

NOTE: Indicators are the basis for analysis and decision making.

log: continuous recording of software usage computer data, with some features that differentiate it from traces (more general concept - see definition above): detailed and known structure, time stamping, events that are registered in audit files as soon as they occur

non-conformity: security event that indicates that organization's security rules and requirements have not been met, and is therefore the consequence of a usage or implementation drift

NOTE: Continuous monitoring of non-conformities (similar to continuous checking - see this term above) enables to better make sure that organization's security policy is being enforced. Non-conformities can be grouped into ones that relate to configuration, behaviour, global security (technical and organizational) and material. Non-conformities are also vulnerabilities or incidents depending on the situation (see definition above).

periodic audit (periodic checking): using isolated audit means, periodic checking of a series of security controls

NOTE: A periodic checking can also be either manual or automatic (for example, carried out through scanner type tools). Finally, a periodic checking is generally of the Boolean type (all or nothing compliance level).

risk: combination of the probability of a security incident's occurrence involving an asset or some given information, with its consequence on this asset or information (corresponding with the CIA sensitivity level)

NOTE: The level of risks exposure (concept which is used in risk assessment methods) corresponds with the combination of the vulnerability level of the asset in question and of the threat level hanging over it.

risk not covered (by existing security measures): risk sometimes also referred to as "residual"

NOTE: This risk breaks down into 3 shares:

- Known and suffered risk, corresponding with the one with which the organization is confronted when security policy is not applied (configuration, behavioural or global security non-conformities), and when known and critical software vulnerabilities are not appropriately addressed.
- Known and accepted risk that corresponds with the one accepted once a choice has been made and backed up by economic, usage and security level considerations.
- Unknown risk corresponding with the one associated with various not updated vulnerabilities or innovative types of attacks.

security event: change of state in a system that may be security relevant and that indicates the appearance of a risk for the organization

NOTE: A security event is either an incident or a vulnerability occurrence or detection (see definition of these terms). 500 security events have been inventoried within the industry, and are grouped into 9 different major categories, with the 4 first corresponding with incidents, and the 5 other ones with vulnerabilities: external attacks and intrusions, malfunctions, usurpations of internal rights or of identity, other internal abnormal behaviours, behavioural vulnerabilities, software vulnerabilities, configuration vulnerabilities, global security technical vulnerabilities, global security organizational vulnerabilities.

severity level (of security incident): level (generally defined on a 4-level scale) inherent to the event itself and that depends on several criteria that vary according to the types of events

NOTE: These criteria are the following (in decreasing order of importance):

- *Dangerousness* is resulting from several objects with variable combinations according to circumstances or types of incidents: execution or spreading speed, virulence, effectiveness, scope and number of impacted assets, capability of harm and of target reach, capability of remotely acting, persistence, weakness or lack of curative means, and last depth which is can be or has been reached (concept of Defence in Depth or DiD).
- *Stealthiness* has several levels: obvious visibility, discretion but can be seen by basic means, detection by advanced technical tools, almost invisibility. It is a key factor within the framework of monitoring and detection concerns. Anonymization and camouflage active and passive means are stealthiness means. Stealthiness takes on an indirect meaning insofar it applies to similar not yet detected incidents.