ETSI GS ISI 001-1 V1.1.2 (2015-06)

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/f0a6393f-7b87-4119-8877-24acffdafc24/etsi-gs-isi-001-1-v1.1.2-2015-06

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
RGS/ISI-001-1ed2

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/f0c6393f-7887-4100-8877-2baeffda4524/etsi-gs-isi-001-1-v1.1.2-2015-06

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

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2015.
All rights reserved.

DECT™, **PLUGTESTS**™, **UMTS**™ and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE**™ are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/0a6393f-f887-4f19-8877-24aefbla4524/etsi-gs-isi-001-1-v1.1.2-2015-06

List of figures

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/f0a6393f-7b87-4119-8877-24aeffda4524/etsi-gs-isi-001-1-v1.1.2-2015-06

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 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 ETSI GS ISI 001-2 [3]) information security indicators, meant to measure the application and effectiveness of prevention measures.
- ETSI GS ISI 002 [4] addressing the underlying event classification model and the associated taxonomy.
- ETSI GS ISI 003 [i.5] addressing the key issue of assessing an organization's maturity level regarding overall event detection capabilities (technology/process/ people) and to weigh event detection results.
- ETSI GS ISI 004 [i.6] demonstrating through examples various means to produce these indicators and how to detect the underlying related events (with a classification of the main categories of use cases/symptoms).
- ETSI GS ISI 005 [i.2] addressing ways to produce security events and to test the effectiveness of existing detection mechanisms within an organization (for major types of events), which is use-case oriented thus more specific and complements the ISI 003 approach.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/ba6395fc-7b87-4110-8877-24effda4524/etsi-gs-isi-001-1-v1.1.2-2015-06

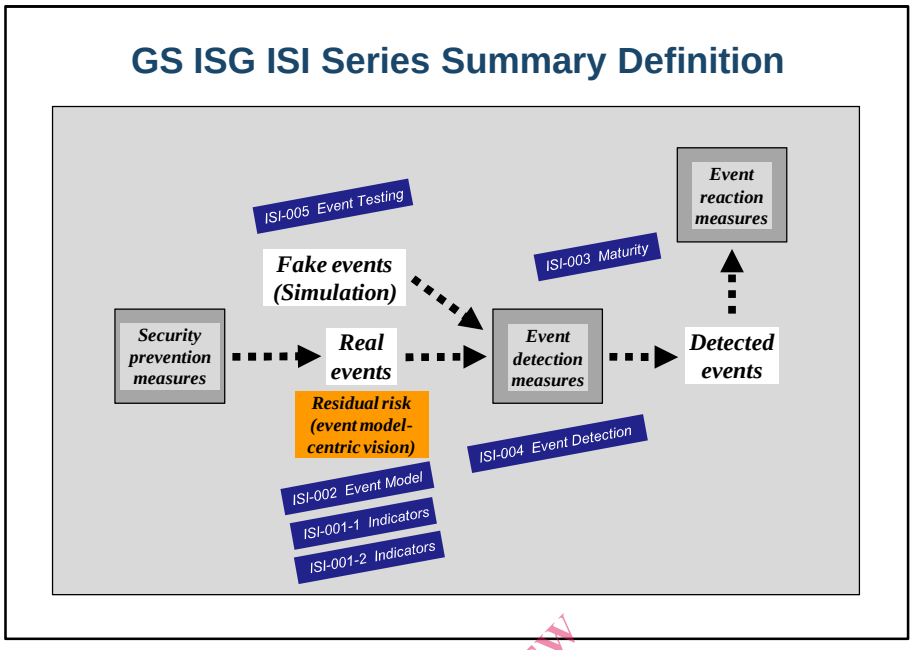

Figure 1: Positioning the 6 GS ISI against the 3 main security measures

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/0a6e93f-7187-4119-8877-24effd4524/etsi-gs-isi-001-1-v1.1.2-2015-06

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

Over the course of recent years, a general consensus has progressively taken place within the industry, recognizing that benchmarking the security of IT systems was worthwhile, on an equal footing with what is done in other areas or disciplines such as quality or management. In other words, it is 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** (refer to the chart in introduction of ETSI 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 has been confirmed worldwide by the publication of converging data, notably the figures from several 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** (demonstrating a trend towards practical outcomes as much as sheer compliance) also made it possible:

- To separate between two categories of indicators, the ones that can under no circumstances serve as reference points (in particular, the ones that are very risk-oriented and consequently specific to a given industry sector), and the ones that are common to all industry sectors and situated on the right level (see the associated event classification model in ETSI GS ISI 002 [4]),
- To map these indicators to the 11 domains of the ISO/IEC 27001/2 standards [6] and [2] to continuously assess the enforcement and effectiveness of an existing ISMS (Continuous Checking), to the ISO/IEC 27006 [i.7] standard on ISMS auditing, and to ISO/IEC 27004 [1] that primarily relates to security indicators.

Furthermore, to meet the requirements of governance (need to provide high-level information suitable for executive summary) and accuracy (need for clear description suitable for action), 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** of aggregated indicators (with high flexibility). Each incident and each vulnerability will be described following a structured language.

The typical list of some **95 indicators** and the associated **10 to 15 possible derived and consolidated indicators** (as provided in the present document) are generally shared by most advanced Cyber Defense and SIEM projects. They are meant as a priority list for CISOs, in order to help them assess and enforce their company's or organization's IT security governance. Some of them, or consolidated indicators, may also be used by Operational Risk Managers, CIOs and senior executives, providing them with an **overview of trends, drifts or progress** displaying the organization's whole security posture.

The proposed list of indicators is in use within the community and accepted. The present document groups them into 4 distinct categories, each with different maturity levels:

- Well-known indicators: indicators related to accidental security incidents (i.e. breakdowns and natural disasters).
- Indicators requiring improved definition: refined definition of indicators related to security incidents of the malicious and unawareness type (external intrusions and attacks, internal deviant behaviours).
- Under-developed indicators: indicators emerging in the community, related to impact measurements.
- Undeveloped indicators: indicators related to behavioural, software, configuration and general security vulnerabilities.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

The next remaining question is **how to use the present document** 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 according to the existing ISMS. This process leads 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 document is the publication (or not) of the proposed state-of-the-art figures, a state that can be directly associated with their qualification as a shared universal reference (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 which are highly convergent between organization. It is therefore possible to rely on these converging indicators in order to carry out benchmarking within one's organization or one's company.

These considerations, associated with a mapping of ISI to various reference frameworks and contexts are addressed in a separate **Guide** called **ETSI 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 [i.8]).

It should be finally mentioned that the present GS partially relies on a work carried out by Club R2GS (see annex C), a club composed of French companies created in 2008, specializing in Cyber Defense and Security Information and Event Management (SIEM). This body 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 Defense and SIEM field. The present document (and associated ETSI GS ISI 001-2 [3]), as well as all other GS ISI 00x, is therefore **based on factual 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. This ensures that the proposed indicators provide a dependable view of the factual state of vulnerability of the monitored information system. Moreover, it should be added that a survey amongst the members demonstrated that these members share a large subset (30 %) of these indicators. This core subset constitutes the set of indicators mentioned as Priority 1 in clause 5.7 (Recap of state-of-the-art figures). The use of this indicators subset ensures that they provide reliable and factual information on the security posture of the organizations that use them.

1 Scope

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

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 27004:2009: "Information technology - Security techniques - Information security management - Measurement".

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

[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 A security event classification model and taxonomy".

[5] 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.

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

[7] ETSI GS ISI 001: " Information Security Indicators (ISI); Indicators (INC)".

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] 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".

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standards: https://standards.iteh.ai/catalog/standards/sist/f0a63b3f-7b87-4110-9877-24affda452c1/etsi-gs-isi-001-1-v1.1.2-2015-06

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

[i.4] NIST SP 800-53 Rev. 4 (April 2013): "Recommended Security Controls for Federal Information Systems and Organizations".

[i.5] ETSI GS ISI 003: "Information security Indicators (ISI); Indicators; Key Performance Security Indicators (KPSI) for security event detection maturity evaluation".

[i.6] ETSI GS ISI 004: "Information Security Indicators (ISI); Guidelines for event detection implementation".

[i.7] ISO/IEC 27006:2001: "Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems".

[i.8] ISO 15408:2009: "Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purpose of the present document, the terms and definitions given in ETSI GS ISI 001-2 [3] apply.

3.2 Symbols

For the purpose of the present document, the symbols given in ETSI GS ISI 001-2 [3] apply.

3.3 Abbreviations

For the purpose of the present document, the abbreviations given in ETSI GS ISI 001-2 [3] apply.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
https://standards.iteh.ai/catalog/standards/sist/f0a8993f-7b87-4119-8871-24acffda1524/etsi-gs-isi-001-1-v1.1.2-2015-06

4 Fill the existing gap in continuous assurance standards

4.0 Introduction

There are numerous initiatives and emerging useful standards in the field of continuous assurance within the information security community all around the world. However, standardization on indicators and the associated security event classification model is missing (see figure 2). Standardization on this matter is becoming essential because such a set of measurements has to be widely published in order to stimulate the sharing of state-of-the-art figures within the security community. Such a trend could eventually lead to the **emergence of widely recognized and reliable statistics** representing the state-of-the-art in security posture through large centralized data bases (possibly European-wide), and organizations could benefit greatly from them to assess and benchmark themselves reliably. The present document should thus help to overcome the inconsistencies in the publication of today's multiple security information metrics, and therefore significantly improve their dependability.

4.1 Overview of existing continuous assurance standards

Figure 2 is a summary of the main standards that exist in the field of continuous assurance. They are all aimed at providing guides to implement in a practical manner and use the notions of security assurance, trust and dependability, and to help executives take the appropriate decisions and steps regarding security investments. Their scope ranges from basic (and often purely technical) specifications to wide-ranging organizational standards.

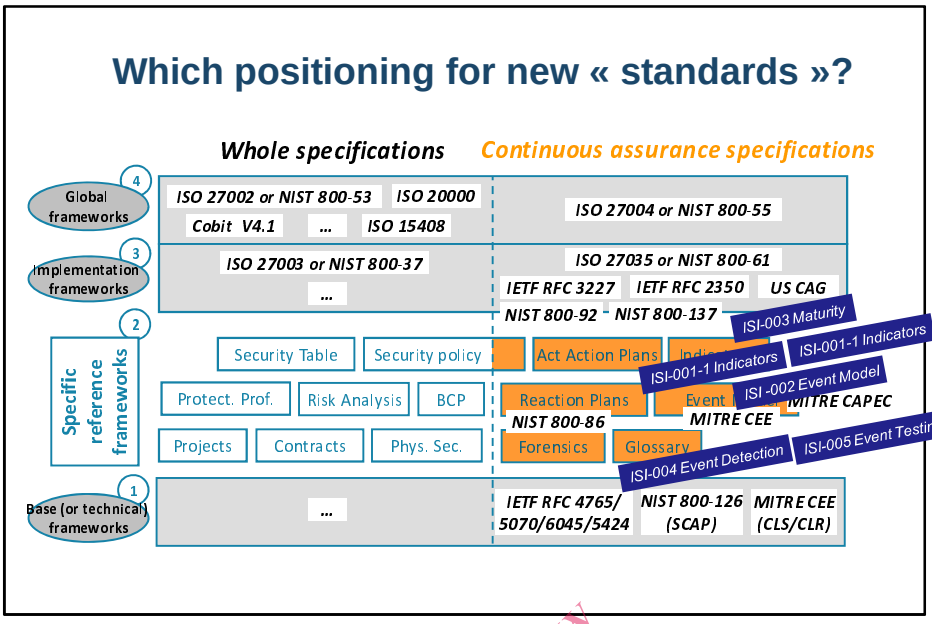

Figure 2: Positioning the 6 GS ISI against other main continuous assurance standards

4.2 Exchanging and sharing security events and indicators

A key aspect when security events (ETSI GS ISI 002 [4]) are detected and related information security indicators (ETSI GS ISI 001 [7]) are produced is more and more to share and exchange these results and associated threat with other members of the Cybersecurity community (CERTs, Government Agencies, regulators, professional bodies, etc.). A scheme or mechanism is provided in ETSI GS ISI 002 [4] (also applicable to ETSI GS ISI 001 [7]) to exchange both security events and indicators.

4.3 Position and target of the GS ISI series

Since there are already many standards in the field, filling the gap in a useful manner requires that this specification is correctly positioned with respect to the other. This requires a clear correspondence with other widespread and widely used lower or higher level specifications or standards. The goal of the GS ISI series of 6 deliverables ([3], [4], [i.2], [i.5], [i.6] and the present document) is also to build a future that can reconcile and bridge the gap between initiatives or standards such as ISO/IEC 27002 [2] or NIST SP 800-53 [i.4] or the US Consensus Audit Guidelines (CAG) [5] and technical level 1 standards; or in other words to bring together top-down (security governance) and bottom-up (IT field operational staff) approaches, and make these 2 populations exchange information better (see figure 2). With respect to indicators, they should be compatible with the structure and the examples given in ISO/IEC 27004 [1] or NIST SP 800-55 [i.1] (which both bridge the gap between the continuous assurance and operational world). And their definition should be closely associated with a structured security event classification model based on a clear taxonomy for security events.

Positioning the GS ISI series of 6 deliverables ([3], [4], [i.2], [i.5], [i.6] and the present document) with respect to the CAPEC (Common Attack Pattern Enumeration and Classification) reference framework is also useful, although it mainly addresses the event classification model. This correspondence is interesting since the present document deals with the same kinds of security events (though only security incidents of the malicious kind for CAPEC). CAPEC has been designed by The MITRE Corporation and it complements the NIST SP 800-126 [i.3] (SCAP) standard, part of it deals in particular with categorizing vulnerabilities and non-compliance. Relationships between GS ISI series of 6 deliverables ([3], [4], [i.2], [i.5], [i.6] and the present document) and CAPEC are addressed in ETSI GS ISI 002 [4] (Security Event Classification Model and Taxonomy).

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/f0a63f3f-2887-4110-8f77-2...ffda452/etsi-gs-isi-001-1-v1.1.2-2015-06

5 Description of the proposed security indicators

5.0 Introduction

This clause describes the complete set of the proposed security indicators, following the breakdown of the associated Event Classification Model (Representation and associated Taxonomy) developed in ETSI GS ISI 002 [4]. There are seven main categories (three relating to security incidents and four relating to vulnerabilities), as follows:

Security incidents

- Intrusions and external attacks (Category IEX) [i.6]
- Malfunctions (Category IMF)
- Internal deviant behaviours (Category IDB)

NOTE: This list also includes another category that gathers all categories of incidents (Category IWH).

Vulnerabilities

- Behavioural vulnerabilities (Category VBH)
- Software vulnerabilities (Category WSW)
- Configuration vulnerabilities (Category VCF)
- General security (technical or organizational) vulnerabilities (Category VTC or Category VOR)

iTeh STANDARD PREVIEW (standards.iteh.ai)

The description of each indicator includes the links with ISI 002 Event Classification Model categories (categories, sub-categories and families) and with the ISO/IEC 27002 [2] controls. The definition of the Indicators complies with the recommended template provided for that purpose in ISO/IEC 27004 [1]. Moreover, the stakeholders of the indicators are summarized in clause 5.7 table (Recap), by assigning indicators to 2 different populations: first CISOs, and then Operational Risk Managers, CIOs and Senior Executive Management.

5.1 Building a fully flexible indicators architecture

To meet the requirements of both **completeness** (need for a full set of more than 90 indicators for precise benchmarking purposes of most ISMS controls) and **governance** (need for a summary of 10 to 15 derived and consolidated indicators), the indicators are mapped and organized according to the underlying event classification model (representation and associated taxonomy), making it therefore possible to group them based on various criteria (origin, type of action, type of asset impacted, type of CIA consequence, type of impact, etc.) and to build a pyramidal structure with different aggregation levels (with high flexibility).

The model structure and taxonomy used to describe **incidents** (see ETSI GS ISI 002 [4]) are as follows (*8 areas* required to fully describe a **change** in a system): who and/or why (*subject*), what (*verb 1*), how (*verb 2*), status of incident (ongoing attempt or successful attack), which vulnerability is being exploited, on what kind of asset (*complement*), with what CIA consequence, with what kind of impact.

The model structure and taxonomy used to describe **vulnerabilities** (see ETSI GS ISI 002 [4]) are as follows (*5 areas* required to fully describe a **state**): what, on what kind of assets, who (only for behavioural vulnerabilities), for what purpose (only for behavioural vulnerabilities), to what kind of possible exploitation.

The following aggregated **top level key indicators** for incidents are recommended:

- External malicious incidents.
- Internal malicious incidents (that can be further decomposed depending on incident origin - employees, contractors, service providers and business partners).
- Internal incidents involving carelessness or lack of awareness (that can be further decomposed depending on origin - employees, contractors, service providers and business partners).
- Accidental or unwitting incidents.

- Incidents with type "A" impact (loss of availability, possibly further decomposed according to the various types of assets impacted - i.e. workstations, servers, mainframes, network).
- Incidents with type "C" impact (loss of confidentiality - the usually less known consequence, possibly refined with privacy, IPR, Defence secret, etc.).
- Incidents with fraud-related type "I" impact (loss of integrity, refined according to the most interesting types of them).
- Incidents with a specific impact on the organization (financial, legal, reputation, etc.).
- Incidents impacting workstations (possibly further decomposed by organization-owned or employee-owned - see BYOD).
- Incidents impacting Web servers.
- Incidents described according to the vulnerabilities exploited or on the status of the victim/target (regarding lack of patching for example).

It is however necessary to be aware that most of the time these top level indicators do not enable benchmarking, as they are highly specific to industry sectors.

5.2 The key issue of an organization's maturity level

iTeh STANDARD PREVIEW (standards.iteh.ai)

The absence of detection of an attack within an organization does not mean that no events occurred within it, so it is strongly advised to assess the level of event detection effectiveness. It is about building a dedicated, practical, simple and easy-to-use **N-level maturity scale** focused on security event detection. This maturity scale is based on hands-on experience, in order to evaluate the metrics and measurements defined by organizations depending on their security maturity level (tools, processes, organization, people) and therefore to propose evolutions of these measurements (see ETSI GS ISI 003 [i.5]). This concept is close to the "Implementation evidence" concept used in NIST SP 800-55 [i.1] in the description of examples of indicators (Appendix A - Candidate Measures). ETSI GS ISI 003 [i.5] addresses this issue in a simple way, relying in particular on the US CAG reference framework and its control points. Based on a questionnaire and on these control points with the associated special metrics, ETSI ISG ISI defines a set of KPSI (Key Performance Security Indicators) that will apply to the present indicators to measure the results. Another (more accurate) way to assess this maturity level is to test the effectiveness of the detection tools through a comprehensive set of testing scenarios (stimulation through fake security events); this is the objective of ETSI GS ISI 005 [i.2].

For each indicator described in clause 5, item 6 provides information about the **detection level** of associated events corresponding to the **state-of-the-art** (practices by the best organizations); there are 3 levels (from 1 low to 3 high), indicating the detection level by the best methodology and current tools in the profession, if known). Since we are far from reaching a 100 % event detection rate for many security events, it is mandatory to apply an **adjustment** to figures gathered from the SIEM projects and achievements within the profession (depending on the level of monitoring equipment and the seriousness of sampled organizations), if we want to obtain real state-of-the-art figures (representing the true reality). This sort of detection level figure should therefore be reckoned specifically for the organization depending on its maturity level (through KPSI as defined in ETSI GS ISI 003 [i.5]) to get the most likely figure applying to the organization.

Each indicator should as much as possible be associated with its **level of coverage**, i.e. the IT perimeter or scope on which the indicator is measured; a small scope of monitoring may therefore lead to a more partial and less reliable measure than a larger and possibly organization-wide scope.

5.3 Indicators detailed definition

The following is provided for each proposed indicator (except Impact indicators, which are of a different kind and have no correspondence with the ETSI GS ISI 002 [4] event classification model):

0) Its *category* (according to the 7 categories of the event classification model described in ETSI GS ISI 002 [4]).

1) Its *family and identifier* (XXX_YYY.number) and *name* (according to the ETSI GS ISI 002 [4] event classification model).

2) The precise *definition* of the base events that are included in the indicator, including comments (to be as precise as possible about the events that are counted).

3) The estimated *frequency* level of base events (main rationale for selecting the indicator). This frequency is being quantitatively and more precisely collected and reckoned by Club R2GS in the state-of-the-art value (see point 8).

4) The *severity* level of base events (1 being the lowest and 4 the highest).

5) The state-of-the-art *detection means* of most base events (manual vs. automatic, methods and technical tools for detecting events).

6) The *detection level* of most base events: 3 levels - from 1 low (less than 30 %) to 3 high (more than 70 %) - including the detection level provided by the best methodology and currently deployed tools in the industry, as defined in the related maturity KSPI - see item 10 and ETSI GS ISI 003 [i.5].

7) The *indicator production* as regards ISO/IEC 27004 [1] ("base measure", "derived measure 1", "derived measure 2", "indicator value").

8) The *state-of-the-art value* (**after necessary correction** - see explanations in clause 5.2 - in order to reckon the true average value due to the detection rate by best organizations - see previous item 6):

   - Indicated with the scattering of the figures at the basis of the supplied average value.

   - Expressed as monthly frequency of events occurrence or as a % (organization with 100 000 workstations accessing the Information System, with possible supplementary clarifications, if necessary).

   - Possibly not applicable or not uniform (definitions which are too variable depending on organizations).

9) Its possible *correspondence* to ISO/IEC 27002 [2], via the corresponding control area from amongst the 11 available ones ("control objective").

10) The *type of maturity KPSI* associated with the indicator (see ETSI GS ISI 003 [i.5]).

Annex A presents the positioning of these various items relative to the "template" recommended in ISO/IEC 27004 [1] for working out an indicator within an organization. As such, the proposed indicators are positioned, depending on the cases, as "base measure", "derived measure" or "indicator". The term "indicator" means that the measurement is appropriate to serve as a reference point for assessing progress made with the existing ISMS, while for their part, the terms "base measure" and "derived measure" can, in some cases, mean that we have no way of acting on the relevant controls (for example applied external pressure). It should also be noted that many subjects included in the ISO/IEC 27004 [1] "template", which are totally specific to the organization and not applicable here, are consequently not included in the present document.

The indicators described below (also available in an Excel spreadsheet referenced in annex B) are divided in **3 categories**:

- The ones relevant to security incidents (**ISMS effectiveness level**), which are complemented by forewarning indicators that measure the external malicious "pressure" (malicious attempts detected and that can herald security incidents of the "real intrusion" type).

- The ones relevant to behavioural, software, configuration and general security (technical and organizational) vulnerabilities (partly **ISMS actual application level**).

- The ones relevant to impact measurements (**Practical consequences**).

5.4 Indicators related to security incidents

The following are the recommended operational indicators related to security incidents (42 in all):

Category IEX (Intrusions and external attacks)

Indicators of this category give information on the occurrence of incidents caused by external malicious threat sources.

iTeh STANDARD PREVIEW (standards.iteh.ai)