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

GROUP SPECIFICATION

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

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 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.

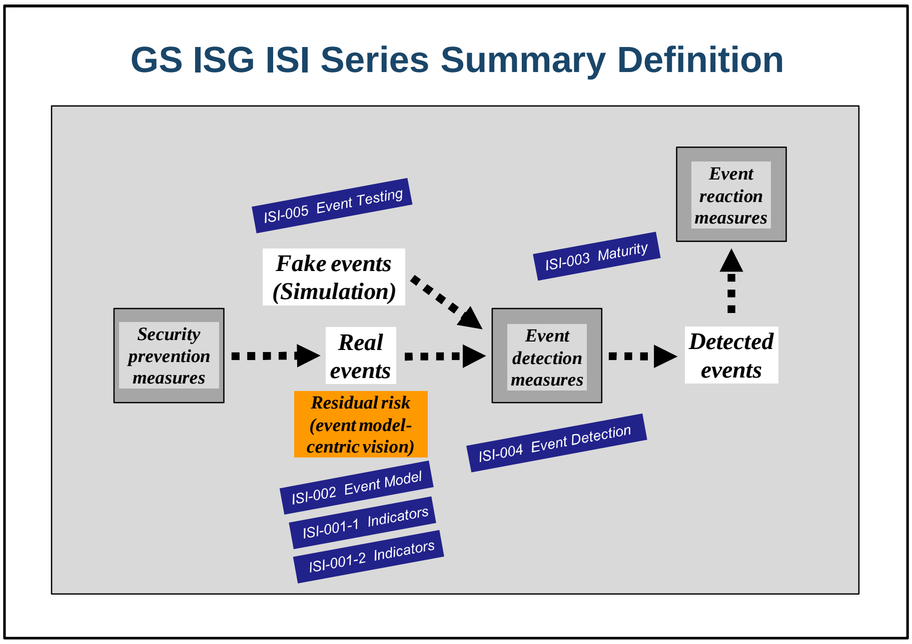

Figure 1: Positioning the 6 GS ISI against the 3 main security measures

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

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.

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".

[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.

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.

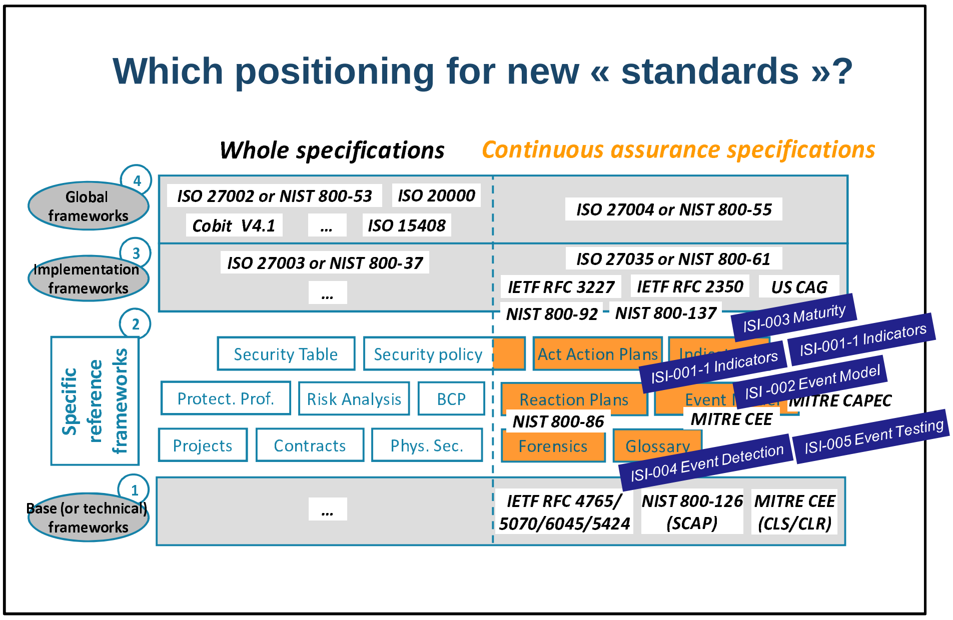
Which positioning for new « standards »?

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).

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)

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

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.

Family IEX_FGY: Website forgery

IEX_FGY.1: Forged domain or brand names impersonating or imitating legitimate and genuine names
Forged domains are addresses very close to the domain names legitimately filed with registration companies or organizations (forged domains are harmful only when actively used to entice customers to the website for fraudulent purposes). It also includes domain names that imitate another domain name or a brand.
Base events
Detection of a new forged domain address (primarily .com and .nn, with the latter also possibly including .gov.nn) that is close to the domain or brand names of the company or organization (including typing errors), and that is registered within a database corresponding with these 1st level domains **Frequency:** Frequency often high (companies with the general public as customers) **Severity:** 2 (if addresses actually used) **Detection means:** Semi-automatic production (search directly within databases administered by the registrars in charge of 1st level domains, or with intermediaries that offer parking pages) **Detection level:** 3
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of existing legitimate addresses **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** Not applicable (too dependent on companies or organizations, on their reputation or on the general public nature or not of their activities)
Link with ISO/IEC 27002 [2]
No (but implicit and derived link with A13)
Maturity KPSI

IEX_FGY.2: Wholly or partly forged websites (excluding parking pages) spoiling company's image or business
Forged websites correspond to two main threats (forgery of sites in order to steal personal data such as account identifiers and passwords, forgery of services in order to capitalize on a brand and to generate turnover that creates unfair competition). In this case, reference is often made to phishing (1st usage) or pharming.
Base events
Detection of a website or service with at least 25 % forged pages **Frequency:** Frequency often high (companies with the general public as customers) **Severity:** 2 **Detection means:** Semi-automatic production is possible (detection using recognition tools that search the Web for content that is identical with that of the company or organization, by means of an Internet crawler used together with an image analysis engine) **Detection level:** 2 (detection rate could be up to 40 % for business forgery and 60 % for phishing)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of the company's or the organization's exposed Websites **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** Not applicable (too dependent on companies or organizations, on their reputation or on the general public nature or not of their activities). However, one quarter of IEX_FGY.1 seems to lead to IEX_FGY.2
Link with ISO/IEC 27002 [2]
No (but implicit and derived link with A13)
Maturity KPSI
6

Family IEX_SPM: Spam

IEX_SPM.1: Not requested received bulk messages (spam) targeting organization's registered users
Spam are messages received in company's or organization's messaging systems in the framework of mass and not individualized campaigns, luring into clicking dangerous URLs (possibly Trojan laden) or enticing to carry out harmful to concerned individual actions.
Base events
Reception of a spam message, not detected and not blocked by messaging system entry filtering **Frequency:** Very high frequency (situation that leads to loss of effectiveness in exchanges for all companies' or organizations' users) **Severity:** 3 **Detection means:** Manual production (figures from messaging system to collect - Cf. messages filtered by antispam tools at organization's messaging system entry -, and messages declared « undesirable » by users themselves - Cf. monthly manual survey based on a sample of users) **Detection level:** 3 (detection rate can reach 100 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of messages received in messaging system during the last 30 days **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 0,2 % for internal business messaging systems (rather low scattering between companies and organizations, but very different situation for public messaging systems)
Link with ISO/IEC 27002 [2]
No
Maturity KPSI

Family IEX_PHI: Phishing

IEX_PHI.1: Phishing targeting company's customers' workstations spoiling company's image or business
Phishing involves a growing number of business sectors (financial organizations, e-commerce sites, online games, social sites etc.). It includes attacks via e-mail with messages that contain either malicious URL links (to forged websites) or malicious URL links (to malware laden genuine websites).
Base events
Customer reporting of a phishing attempt. **Frequency:** High frequency and strong impact on the image **Severity:** 2 **Detection means:** Manual production (via periodic tests of customers or users) **Detection level:** 2 or 3 (detection rate can be up to 80 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Number of unique campaigns detected during the last 30 days. A unique campaign consists of a series of coordinated phishing attacks coming from a single origin within a given time slot, with an average of 6 attacks per campaign. **Indicator value:** Ratio of Derived Measure 2 to the media exposure (communication measurement specific to each professional sector) **State-of-the-art value:** (Derived measure 2) 20 campaigns per month in English language (relatively high scattering between companies in a given business sector, primarily depending on the media exposure)
Link with ISO/IEC 27002 [2]
No
Maturity KPSI
6, 7

IEX_PHI.2: Spear phishing or whaling carried out using social engineering and targeting organization's specific registered users
Spear phishing are "spoofed" and customized messages looking like a usual professional relationship or an authority, and asking to click on or open dangerous URL links or dangerous attachments (malware laden)
Base events
Reception of a "spoofed" and customized messages looking like a usual professional relationship or an authority, and asking to click on or open dangerous URL links or dangerous attachments (malware laden), or asking to send confidential information by e-mail return **Frequency:** High frequency in some business sectors and organizations, and possible early indicator of subsequent successful intrusions **Severity:** 3 **Detection means:** Automatic production possible (usage of CERTs to detect more or less repetitive attack scenarios targeting different organizations and personalities, internal detection via the users themselves if moderately executed scenario) **Detection level:** 1 (detection rate can be up to 30 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** idem Derived Measure 1 **Indicator value:** Ratio of Number of events detected during the last 30 days to Number of messages received in messaging system during the last 30 days **State-of-the-art value:** Not applicable (too dependent on companies or organizations, on their reputation or on the sensitive kind of their business)
Link with ISO/IEC 27002 [2]
A13 control area
Maturity KPSI
6, 7

Family IEX_INT: Intrusion

IEX_INT.1: Intrusion attempts on externally accessible servers
Attempts are here systematic scans (excluding network reconnaissance) and abnormal and suspicious requests on externally accessible servers, detected by an IDS/IPS or not.
Base events
Detection of intrusion attempts (systematic scans (excluding network reconnaissance) and abnormal and suspicious requests on externally accessible servers. **Frequency:** High frequency and information of possible successful intrusions **Severity:** 2 or 3 (according to the type - flaw discovery scan vs. attack in progress) **Detection means:** Possible automatic production (logs of Web servers and/or of IDS/IPS and/or Deep Packet Inspection device, and very useful SIEM tool) **Detection level:** 2 (detection rate can be up to 60 to 70 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of unique events detected during the last 30 days (a unique event includes all intrusion attempts coming from a single origin in a one-day period) **Derived measure 2:** idem Derived Measure 1 **Indicator value:** Ratio of Number of events detected during the last 30 days to Number of externally accessible servers **State-of-the-art value:** (Derived measure 1) 400 incidents per externally accessible server (relatively low scattering between organizations)
Link with ISO/IEC 27002 [2]
A13 control area
Maturity KPSI
None

IEX_INT.2: Intrusion on externally accessible servers
Intrusion usually targets servers that host personal data (including data subject to regulations such as PCI DSS, for example). 3 objectives or motivations can be found wherever an intrusion exists**:** data theft (see before), installation of transfer links towards unlawful and rogue websites, getting a permanent internal access by installation of a backdoor for further purposes. This indicator does not include the figures from the Defacement and Misappropriation indicators, both of which however starting with an intrusion. However, it includes all means and methods to get access to servers, i.e. purely technical means (such as Command execution/injection attack) or identity usurpation to log on an admin or user account (see ETSI GS ISI 002 [4] specifications).
Base events
Detection of intrusion **Frequency:** Relatively high frequency **Severity:** 3 or 4 (depending on intrusion depth and according to successful access or not to personal data) **Detection means:** Automatic production possible (logs of server OS and/or of HTTP platforms and/or of Web applications, logs of IDS/IPS, and SIEM tool) **Detection level:** 1 (detection rate can be up to 15 %, very low rate proven in the USA for thefts of credit card numbers - 80 % post-mortem rate after discoveries of fraud and intensive investigations)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of unique events detected during the last 30 days (a unique event includes all intrusions coming from the same attacker) **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of externally accessible servers **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 0,7 incident per externally accessible server (low scattering rate between organizations)
Link with ISO/IEC 27002 [2]
A13 control area
Maturity KPSI
5, 6, 7, 8

IEX_INT.3: Intrusions on internal servers
This kind of incident typically comes after a PC malware installation or an intrusion on an externally accessible server often followed by a lateral movement. This indicator does not include the figures from the Misappropriation indicator which may however start with an intrusion on an internal server. This indicator includes the so-called APTs (Advanced Persistent Threats), which constitute however only a small part of this indicator. APTs are long lasting and stealthy incidents with large compromises of data through outbound links, which is not the case of most incidents of the IEX_INT.3 type. This type of incident is often the result of targeted attacks.
Base events
Detection of intrusion **Frequency:** Medium frequency **Severity:** 4 **Detection means:** Automatic production possible (logs of server OS and/or of HTTP platforms and/or of Web applications, server and/or network loads, and SIEM tool) **Detection level:** 1 (detection rate can be up to 15 %, very low rate assessed for thefts of credit card numbers - 70 % post-mortem rate after discoveries of fraud and intensive investigations)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of unique events detected during the last 30 days (a unique event includes all intrusions coming from the same attacker) **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of externally accessible servers **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 0,05 incident per internal server (high scattering rate between organizations because of targeting)
Link with ISO/IEC 27002 [2]
A13 control area
Maturity KPSI
5, 6, 7, 8

Family IEX_DFC: Website defacement

IEX_DFC.1: Obvious and visible websites defacements
Obvious defacements measures the defacement of homepages and of the most consulted pages of sites.
Base events
Detection of an obvious defacement **Frequency:** Relatively high frequency **Severity:** 3 **Detection means:** Automatic production possible (integrity checking software of the Tripwire type, and/or upstream monitoring software for anomalies in HTTP flows, and/or software to simulate transactions and to check responses, and SIEM tool for consolidation of all detection means) **Detection level:** 3 (detection rate can be up to 90 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of the company's or the organization's websites **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 0,2 incident per website (high scattering rate between organizations, depending on the site's reputation and secure development or not of Web applications)
Link with ISO/IEC 27002 [2]
A13 control area
Maturity KPSI
5, 6, 7

Family IEX_MIS: Misappropriation of resources

IEX_MIS.1: Servers resources misappropriation by external attackers
This indicator measures the amount of resources of servers misappropriated by an external attacker after a successful intrusion (on an externally accessible or an internal server).
Base events
Detection of a new server affected by a misappropriation **Frequency:** Significant frequency **Severity:** 2 **Detection means:** Semi-automatic production possible (logs of server OS and/or of HTTP platforms and/or of Web applications, logs of IDS/IPS, load data from system administration tools, and SIEM tool) **Detection level:** 1 (detection rate can be up to 15 % - same as IEX_INT.2 intrusions)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** idem Derived measure 1 **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 2 incidents for a standard organization (high scattering rate between organizations, depending on whether an enterprise-wide SIEM approach with attention paid on deviant behaviours exists or not)
Link with ISO/IEC 27002 [2]
A13 control area
Maturity KPSI
5, 6, 7

Family IEX_DOS: Denial of Service

IEX_DOS.1: Denial of service attacks on websites
This indicator measures denial-of-service attacks against websites, carried out either by sending of harmful requests (DoS), by sending a massive flow coming from multiple distributed sites (DDoS) or via other techniques. Due to the current state of the art of attack detection, the indicator is limited to DDoS attacks.
Base events
Detection of an attack on a given website coming from the same origin within a limited continuous timeframe, and a significant incident defined as a user noticeable disturbance and performance drop in the website access **Frequency:** Relatively high frequency, though very uneven over time **Severity:** 4 (if complete blockage of server or network) **Detection means:** Possible automatic production for DoS attacks (logs of databases and Web applications, system administration tools, and SIEM tool) and for DDoS attacks (network administration tools for perimeter areas) **Detection level:** 3 (detection rate can be up to 100 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of the company's or the organization's websites **Indicator value:** idem Derived measure 2 **State-of-the-art value:** (Derived measure 2) 0,006 (0,1 x 0,06) incident by website (very high scattering level between organizations depending on their visibility on Internet, as well as considerable unevenness over time for major attacks)
Link with ISO/IEC 27002 [2]
A13 control area
Maturity KPSI
5, 6, 7

Family IEX_MLW: Malware

IEX_MLW.1: Attempts to install malware on workstations
Malware installation attempts are detected by current conventional means (Antivirus and base IPS) and blocked by the same means. This indicator (which includes desktop and laptop PC based workstations, but does not include the different types of other workstations and mobile smart devices) provides an approximate insight into the malicious external pressure suffered in this regard. This indicator should be associated with indicator on successful malware installation in order to assess the actual effectiveness of conventional detection and blockage means in the fight against malware.
Base events
Detection of a malware on workstations by organization's Antivirus and IPS **Frequency:** Very high frequency **Severity:** 1 **Detection means:** Automatic production possible (detection by existing antivirus and base IPS at the network entrance or AV in workstations, with AV central administration software) **Detection level:** 3 (detection rate can be up to 100 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Number of unique malware installation attempts (or number of the different types of malware that were detected) **Indicator value:** idem Derived measure 2 **State-of-the-art value:** (Derived measure 2) 1 600 alarms for a standard organization with 100 000 Windows-based workstations (rather low scattering according to organizations, except if deficiency with activation or update of AV and base IPS)
Link with ISO/IEC 27002 [2]
A10 and A13 control areas
Maturity KPSI
5, 6, 7

IEX_MLW.2: Attempts to install malware on servers
Malware installation attempts are detected by current conventional means (antivirus and base IPS) and blocked by the same means. This indicator gives an approximate insight into the malicious external pressure suffered in this regard. This indicator should be associated with indicator on successful malware installation in order to assess the actual effectiveness of conventional detection and blockage means in the fight against malware.
Base events
Detection of a malware on servers by organization's AV and base IPS **Frequency:** Very high frequency **Severity:** 1 **Detection means:** Automatic production possible (detection by existing antivirus and base IPS at the network entrance or AV in servers, with AV central administration software) **Detection level:** 3 (detection rate can be up to 100 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Number of unique malware installation attempts (or number of the different types of malware that were detected) **Indicator value:** idem Derived measure 2 **State-of-the-art value:** (Derived measure 2) 110 alarms for 10 000 servers (rather low scattering according to organizations, except if deficiency with activation or update of AV and base IPS)
Link with ISO/IEC 27002 [2]
A10 and A13 control areas
Maturity KPSI
5, 6, 7

IEX_MLW.3: Malware installed on workstations
Malware could be not detected by conventional means (lack of activation or appropriate update), or non-inventoried and/or specific very stealthy incidents, most of the time not detectable by conventional means (AV and standard IPS), consequently requiring other supplementary detection means (network or WS load, outbound links, advanced network devices as DPI tools, users themselves reporting to help desks). This indicator (which includes desktop and laptop Windows-based workstations, but does not include the different types of other workstations and mobile smart devices) therefore applies to both classical viruses and worms, as well as all new malware such as Trojan horses (which are defined as malware meant to data theft or malicious transactions) or bots (which are defined here as vectors for spam or DDoS attacks).
Base events
Detection of a malware on workstations by non-conventional means (other than AV and standard IPS) **Frequency:** Relatively high frequency **Severity:** 2 to 4 (depending on the level of increase of the system load of PCs, or depending on the existence or not of Trojan horses or bots) **Detection means:** Possible automatic production (detection by monitoring unusual system loads - typically increase after PCs are put to sleep, and/or by means of suspicious outgoing HTTP links to proxies - case of Trojan horses or bots, and/or by IDS at outbound network perimeter, and/or by users. PC system administration tools and/or logs of proxies and/or of firewalls, and SIEM tool) **Detection level:** From 1 to 3 (depending on type and stealth of malware - detection of Trojan horses and bots virtually impossible without SIEM tools, with the latter case providing detection rates possibly attaining 50 % for the best ones, but detection rate most often much lower and even non-existent, notably for the most sophisticated state-sponsored attacks)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** idem Derived Measure 1 **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 40 incidents for a standard organization (fairly high scattering rate between organizations depending on their sensitivity and their detection means - for example, can be up to 80 incidents in some sensitive companies or organizations). Estimated figures regarding the current park of once infected workstations - whether cleaned or not - are from 3 to 10 % for major companies, 20 % for professionals and SME, and 35 % for the general public. Estimated figure regarding the overall current park of still infected workstations (all categories taken together) is 0,7 %
Link with ISO/IEC 27002 [2]
A10 and A13 control areas
Maturity KPSI
3, 5, 6, 7, 8

IEX_MLW.4: Malware installed on internal servers
Malware could be not detected by conventional means (lack of activation or of appropriate update), or non-inventoried and/or specific very stealthy incidents, most of the time not detectable by conventional means (AV and standard IPS), consequently requiring other supplementary detection means (network or server load, outbound links, advanced network devices as DPI tools, administrators themselves). This indicator therefore applies to both classical viruses and worms, as well as all new malware such as Trojan horses (which are defined as malware meant to data theft or malicious transactions)
Base events
Detection of a malware on internal servers (not including perimeter servers) by non-conventional means (other than AV and standard IPS) **Frequency:** Relatively high frequency **Severity:** 2 to 4 (depending on the level of increase of the system load, or depending on the existence or not of Trojan horses) **Detection means:** Automatic production possible (detection by means of monitoring unusual system loads - typically an increase of 35 to 40 %, or by means of suspicious outbound HTTP links to proxies. System administration tools for servers and/or logs of proxies and/or of firewalls, and SIEM tool) **Detection level:** From 1 to 3 (depending on type and stealth of malware - detection of Trojan horses difficult without SIEM tools, with detection rates possibly attaining 50 % in the latter case)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** idem Derived Measure 1 **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 0,5 incidents per 10 000 internal servers (rather high scattering rate between organizations depending on their sensitivity)
Link with ISO/IEC 27002 [2]
A10 and A13 control areas
Maturity KPSI
3, 5, 6, 7, 8

Family IEX_PHY: Physical intrusion or action

IEX_PHY.1: Human intrusion into the organization's perimeter
This indicator measures illicit entrance of individuals into security perimeter.
Base events
Detection of a violation of physical access control **Frequency:** Possibly rather high frequency in some cases (not critical and basic organizations) **Severity:** 3 **Detection means:** Manual detection and production (random detection only really possible) **Detection level:** 1 (detection rate can be up to 15 %, if policy requiring to wear identification badges is strictly enforced)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** idem Derived Measure 1 **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 50 incidents for a standard organization (high scattering rate between organizations, depending on their sensitivity)
Link with ISO/IEC 27002 [2]
A9 control area
Maturity KPSI
6

Category IMF (Malfunctions)

Indicators of this category provides information on the occurrence of incidents caused by malfunctions, breakdowns or human errors.

Family IMF_BRE: Accidental breakdowns or malfunctions

IMF_BRE.1: Workstations accidental breakdowns or malfunctions
Breakdowns or malfunctions apply to both hardware and software, caused by system errors (components failure or bugs).
Base events
Detection of a workstation breakdown or malfunction **Frequency:** High frequency **Severity:** Part of availability sensitivity definition of the information hosted by PCs, and also identical to the criticality of the incidents (with the policy for assets availability classification taking the severity of incidents into account through determination of the sensitivity of the assets according to the duration of their downtime) **Detection means:** Semi-automatic production possible (PC administration tools) **Detection level:** 3 (detection rate can be up to 100 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** idem Derived Measure 1 **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** Figures not uniform according to companies or organizations (indicator definition very variable, regarding the consideration or not of some types of errors)
Link with ISO/IEC 27002 [2]
A14 control area
Maturity KPSI
6, 7

IMF_BRE.2: Servers accidental breakdowns or malfunctions
Breakdowns or malfunctions apply to both hardware and software, caused by system errors (components failure or bugs).
Base events
Detection of a server breakdown or malfunction **Frequency:** Relatively high frequency **Severity:** Part of availability sensitivity definition of the information hosted by servers, and also identical to the criticality of the incidents (with the policy for assets availability classification taking the severity of incidents into account through determination of the sensitivity of the assets according to the duration of their downtime) **Detection means:** Semi-automatic production possible (System administration tools) **Detection level:** 3 (detection rate can be up to 100 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** idem Derived Measure 1 **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** Figures not uniform according to companies or organizations (indicator definition very variable, regarding the consideration or not of some types of errors)
Link with ISO/IEC 27002 [2]
A14 control area
Maturity KPSI
6, 7

IMF_BRE.3: Mainframes accidental breakdowns or malfunctions
Breakdowns or malfunctions apply to both hardware and software, caused by system errors (components failure or bugs).
Base events
Detection of a Mainframe breakdown or malfunction **Frequency:** Important to monitor closely **Severity:** Part of availability sensitivity definition of the information hosted by mainframes, and also identical to the criticality of the incidents (with the policy for assets availability classification taking the severity of incidents into account through determination of the sensitivity of the assets according to the duration of their downtime) **Detection means:** Semi-automatic production possible (mainframe administration tools) **Detection level:** 3 (detection rate can be up to 100 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** idem Derived Measure 1 **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** Figures not uniform according to companies or organizations (indicator definition very variable, regarding the consideration or not of some types of errors)
Link with ISO/IEC 27002 [2]
A14 control area
Maturity KPSI
6, 7

IMF_BRE.4: Networks accidental breakdowns or malfunctions
Breakdowns or malfunctions apply to both hardware and software, caused by system errors (components failure or bugs).
Base events
Detection of a network breakdown or malfunction **Frequency:** Relatively high frequency **Severity:** Part of availability sensitivity definition of the information accessed or running through the network, and also identical to the criticality of the incidents (with the policy for assets availability classification taking the severity of incidents into account through determination of the sensitivity of the assets according to the duration of their downtime) **Detection means:** Possible semi-automatic production (network administration tools) **Detection level:** 3 (detection rate can be up to 100 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** idem Derived Measure 1 **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** Figures not uniform according to companies or organizations (indicator definition very variable, regarding the consideration or not of some types of errors)
Link with ISO/IEC 27002 [2]
A14 control area
Maturity KPSI
6, 7

Family IMF_MDL: Misdelivery of content

IMF_MDL.1: Delivery of email to wrong recipient
This indicator measures errors from the sender when selecting or typing email addresses leading to misdelivery incidents. Consequences may be very serious when confidentiality is critical.
Base events
Detection of such an incident **Frequency:** Rather low frequency **Severity:** 1 to 4 (depending on the content and the recipient) **Detection means:** Manual production (by spontaneous internal user notification or by detected consequences) **Detection level:** 1 (detection rate generally low, i.e. less than 15%, employees being reluctant to notify this kind of error
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of users concerned detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of the company's or the organization's users **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 0,2 % (extremely low scattering level according to companies or organizations, due to the sheer human error nature of this type of incident)
Link with ISO/IEC 27002 [2]
A10 and A13 control areas
Maturity KPSI
6

Family IMF_LOM: Loss or theft of mobile devices

IMF_LOM.1: Loss (or theft) of mobile devices belonging to the organization
This indicator measures the loss of all types of systems containing sensitive or not information belonging to the organization, whether encrypted or not (laptop computers, USB tokens, CD-ROMs, diskettes, magnetic tapes, smartphones, tablets, etc.). In some cases, it could be difficult to differentiate losses from thefts.
Base events
Device loss and theft declared to a central level and that can be therefore consolidated **Frequency:** Relatively high frequency **Severity:** 3 **Detection means:** Manual production **Detection level:** 3 (detection rate can be up to 100 %, especially for laptops centrally registered and managed)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of the company's or the organization's devices **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 0,08 % (applicable only to laptop computers) (relatively low scattering level according to companies or organizations)
Link with ISO/IEC 27002 [2]
A8 and A10 control areas
Maturity KPSI
6

Family IMF_LOG: Logging malfunction

IMF_LOG.1: Downtime or malfunction of the log production function with possible legal impact
This type of event could have two main causes**:** an accidental system malfunction or a system manipulation error by an administrator. Logs taken into account here are systems logs and applications logs of all servers.
Base events
Detection of a log outage or malfunction (including logs integrity loss) **Frequency:** Both important and significant frequency (production of logs often viewed as limiting and of relative importance by administrators, and therefore handled with lesser attention except in the event of a strict security monitoring and a strong reaction). **Severity:** 3 or 4 (depending on the cause) **Detection means:** Automatic production possible (logs of the monitored systems and SIEM tool) **Detection level:** 2, given it is impossible to monitor all application software (detection rate can be up to 60 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of the company's or the organization's systems **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** Figures not uniform according to companies or organizations (indicator definition very variable, regarding the consideration or not of incidents other than outages)
Link with ISO/IEC 27002 [2]
A10 control area
Maturity KPSI
5, 6

IMF_LOG.2: Absence of possible tracking of the person involved in a security event with possible legal impact
Concerns unique data related to a given and known to organization user (identifier tied to application software or directory). This indicator is a sub-set of indicator IMF_LOG.1.
Base events
Detection of a production server or production application software affected by incidents of this type **Frequency:** Relatively high frequency (due to errors in the configuration and formatting of logs) **Severity:** 1 or 2 (depending on the event's severity) **Detection means:** Automatic production possible (logs of the monitored systems and SIEM tool) **Detection level:** 1 or 2 (detection rate can be up to 60 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of the company's or the organization's systems **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 10 % (with a relatively low scattering level according to companies or organizations)
Link with ISO/IEC 27002 [2]
A10 and A15 control areas
Maturity KPSI
5, 6

IMF_LOG.3: Downtime or malfunction of the log production function for recordings with evidential value for access to or handling of information that, at this level, is subject to law or regulatory requirements
This indicator primarily relates to Personal Identifiable Information (PII) protected by privacy laws, to information falling under the PCI-DSS regulation, to information falling under European regulation in the area of breach notification (Telcos and ISPs to begin with), and to information about electronic exchanges between employees and the exterior (electronic messaging and Internet connection). This indicator does not include possible difficulties pertaining to proof forwarding from field operations to governance (state-of-the-art unavailable). This indicator is a sub-set of indicator IMF_LOG.1, but can be identical to this one in advanced organizations.
Base events
Detection of a log outage or malfunction (including logs integrity loss) **Frequency:** Both important and significant frequency (production and recordings of logs often viewed as limiting and of relative importance by administrators, and therefore handled with lesser attention except in the event of a strict security monitoring and a strong reaction). **Severity:** 3 or 4 (depending on the cause) **Detection means:** Automatic production possible (logs of the monitored systems and SIEM tool) **Detection level:** 3, given it is possible to monitor all software which is subject to regulations (detection rate can be up to 100 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of the company's or the organization's systems that are subject to regulations or legislations requiring recordings with evidential value **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** Figures not uniform according to companies or organizations (indicator definition very variable, regarding the consideration or not of incidents other than outages)
Link with ISO/IEC 27002 [2]
A10 and A15 control areas
Maturity KPSI
5, 6

Category IDB (Internal deviant behaviours)

Indicators of this category provide information on the occurrence of incidents regarding internal deviant behaviours (including especially usurpation of rights or of identity).

Family IDB_UID: Identity usurpation

IDB_UID.1: User impersonation
A person within the organization impersonates a registered user (employee, partner, contractor, external service provider) using identifier, passwords or authentication devices that had previously been obtained in an illicit manner (using a social engineering technique or not). This measures cases of usurpation for malicious purposes, and not ones that relate to user-friendly usage. Moreover, assumption is made that ID/Password is the main way of authentication.
Base events
Detection of usurpation of identity **Frequency:** High frequency **Severity:** 4 (sheer malice) **Detection means:** Automatic production possible (logs for access control to servers and/or applications, and SIEM tool) **Detection level**: 1(detection rate can be up to 10 %, provided that a SIEM tool configured with rich and diversified correlation rules is used. Incident among the most difficult to detect)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** idem Derived Measure 1 **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 20 incidents for a standard organization with 50 000 VPN accesses (not high scattering level according to companies or organizations, except in ones with advanced SIEM initiatives and reactions regarding the personnel in question, where this figure is in a downward slope)
Link with ISO/IEC 27002 [2]
A8 and A11 control areas
Maturity KPSI
4, 5, 6, 7

Family IDB_RGH: Rights (or privileges) usurpation or abuse on servers or applications

IDB_RGH.1: Privilege escalation by exploitation of software or configuration vulnerability on an externally accessible server.
Exploited vulnerabilities are typically tied to the underlying OS that supports the Web application, exploited notably through injection of additional characters in URL links. This behaviour specifically involves external service providers and company's business partners that wish to access additional information or to launch unlawful actions (for example, service providers seeking information about their competitors). This type of behaviour is less frequent amongst employees, since it is often easier to get the same results by means of social engineering methods.
Base events
Detection of a privileges escalation through system vulnerability exploitation **Frequency:** Frequency that can be high (e.g. in large Extranet networks) **Severity:** 3 **Detection means:** Semi-automatic production possible (logs of server OS and/or of HTTP platforms and/or of Web applications, and SIEM tool) **Detection level:** 1 (detection rate can be up to 30 %, provided that a SIEM tool with rich and varied detection rules is used)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** idem Derived Measure 1 **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 20 incidents for a standard organization with a network of 50 000 business partner users (not very high scattering level according to the companies or organizations - given behaviour of external service providers or business partners are driven by similar curiosity in all of the companies and networks, except in ones with advanced SIEM initiatives and strong reaction vis-à-vis the business partners or service providers in question, where this figure is clearly lower)
Link with ISO/IEC 27002 [2]
A8 and A11 control areas
Maturity KPSI
4, 5, 6, 7, 8

IDB_RGH.2: Privilege escalation on a server or central application by social engineering
It is often easier to get the same results by means of social engineering methods than with technical means. Help desk teams are often involved in this kind of behaviour.
Base events
Detection of a privileges escalation through social engineering means **Frequency:** Frequency that can be significant **Severity:** 3 **Detection means:** Semi-automatic production possible (logs of HIDS) **Detection level:** 1 or 2 (detection rate can be up to 50 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** idem Derived Measure 1 **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 2 incidents for a standard organization (not high scattering level according to companies or organizations, except in ones with advanced SIEM initiatives and reactions regarding the personnel in question, where this figure is in a downward slope)
Link with ISO/IEC 27002 [2]
A8 and A11 control areas
Maturity KPSI
4, 5, 6, 7, 8

IDB_RGH.3: Use on a server or central application of administrator rights illicitly granted by an administrator
Illicitly granting administrator privileges generally comes from simple errors or more worrisome negligence on the part of the administrators (malicious action is rarer). The case of forgotten temporary rights (see next indicator), is not included in this indicator.
Base events
Detection of the usage of illicit administrator rights **Frequency:** Significant frequency **Severity:** 3 **Detection means:** Automatic production possible (logs of access controls to servers, logs of the reference database of the rights, and SIEM tool) **Detection level:** 3 (detection rate can be up to 100 %, provided that a SIEM tool is used that has a reference database of the official administrator rights)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** idem Derived Measure 1 **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 13 users for a standard organization (low scattering level according to companies or organizations, except in ones with advanced SIEM initiatives and reaction vis-à-vis these situations, where this figure is clearly lower)
Link with ISO/IEC 27002 [2]
A8, A10 and A11 control areas (with monitoring of administrators also targeted indirectly)
Maturity KPSI
4, 5, 6, 7, 8

IDB_RGH.4: Use on a server or central application of time-limited granted rights after the planned period
This indicator measures situations where time-limited user accounts (created for training, problem resolution, emergency access, test, etc.) are still in use after the initial planned period.
Base events
Detection of the use of time-limited granted rights after the planned period (accounted only once in case of different incidents involving the same person) **Frequency:** Significant frequency **Severity:** 2 **Detection means:** Automatic production possible (logs for access controls to servers, and SIEM tool) **Detection level:** 2 (detection rate can be up to 50 %, provided that a SIEM tool is used that has a follow-up database of the time limited granted rights and their time)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** idem Derived Measure 1 **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 2 incidents for a standard organization (low scattering level according to organizations, except in ones with advanced SIEM initiatives and reaction to these situations, where this figure gets closer to less than one)
Link with ISO/IEC 27002 [2]
A8, A10 and A11 control areas
Maturity KPSI
4, 5, 6, 7, 8

IDB_RGH.5: Abuse of privileges by an administrator on a server or central application
The motivation of rights usurpation by an administrator is often the desire to breach the confidentiality of sensitive data (for example, human resources data). This indicator is similar to the indicator IDB_RGH.6 (but with consequences that may be however often potentially more serious).
Base events
Detection of an abuse of privileges by an administrator **Frequency:** Significant frequency **Severity:** 3 or 4 (depending on the underlying motivation) **Detection means:** Automatic production possible (logs of HIDS connected to the server) **Detection level:** 1 or 2 (detection level can be up to 40 %, provided that HIDS tools are used)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Number of administrators with such a behaviour during the last 30 days **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 6 administrators for a standard organization (low scattering level according to companies or organizations, except in ones with advanced SIEM initiatives and strong reaction to the personnel in question, where this figure is clearly lower)
Link with ISO/IEC 27002 [2]
A8, A10 and A11 control areas
Maturity KPSI
4, 5, 6, 7, 8

IDB_RGH.6: Abuse of privileges by an operator or a plain user on a server or central application
This indicator applies for example to authorized users having access to personal identifiable information about celebrities with no real need for their job (thereby violating the "right to know").
Base events
Detection of an abuse of privileges on an application (central system) by an operator or a plain user **Frequency:** Significant frequency **Severity:** 1 **Detection means:** Semi-automatic production possible (logs of accesses and commands to applications) **Detection level:** 3 (detection rate can be up to 90 %, provided that a dedicated data base related software and a SIEM tool are used that focus on the average rates of access to records)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of applications **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 2 incidents per application (low scattering level according to organizations, except in ones with advanced SIEM initiatives and strong reaction vis-à-vis the deviant personnel, where this figure is in a downward trend)
Link with ISO/IEC 27002 [2]
A8 and A11 control areas
Maturity KPSI
4, 5, 6, 7, 8

IDB_RGH.7: Illicit use on a server or central application of rights not removed after departure or position change within the organization
This indicator also takes into account the problem of generic accounts (whose password might have been changed each time a user knowing this password is leaving organization).
Base events
Detection of an illicit use of rights, which were not removed after departure or after a change of position within the organization **Frequency:** Significant frequency **Severity:** 3 **Detection means:** Automatic production possible (logs of access controls to servers, logs of the reference database of the rights, and SIEM tool) **Detection level:** 1 (detection rate can be up to 30 %, provided that a SIEM tool is used and connected to a reference database of organization's rights)
Indicator production
Base measure: Date of the event, identity of the user **Derived measure 1:** Number of users with such a behaviour detected during the last 30 days **Derived measure 2:** idem Derived Measure 1 **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** Not applicable, since far too variable according to companies or organizations (in principle, however, figure dropping sharply with advanced IAM achievements)
Link with ISO/IEC 27002 [2]
A8, A10 and A11 control areas
Maturity KPSI
4, 5, 6, 7, 8

Family IDB_MIS: Misappropriation of resources

IDB_MIS.1: Server resources misappropriation by an internal source
This indicators measures misappropriation of on-line IT resources for one's own use (personal, association etc.).
Base events
Detection of a server misappropriation for one's own use (personal, association, etc.) **Frequency:** Significant frequency **Severity:** 3 **Detection means:** Semi-automatic production possible (detection by means of monitoring unusual system loads, typically an increase of 25 to 30 %, based on administration system of servers) **Detection level:** 1 or 2 (detection rate can be up to 40 %, provided that a SIEM tool is used and coupled with system administration that provides accurate information on system load)
Indicator production
Base measure: Date of the event, identity of the user **Derived measure 1:** Number of users with such a behaviour detected during the last 30 days **Derived measure 2:** idem Derived Measure 1 **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 2 users for a standard organization (low scattering level according to organizations, except in ones that launch strong reaction to the concerned user, where this figure is in a downward trend)
Link with ISO/IEC 27002 [2]
A8 and A10 control areas
Maturity KPSI
4, 5, 6, 7

Family IDB_IAC: Illicit access to Internet

IDB_IAC.1: Access to hacking Website
This indicator measures unauthorized access to a hacking Website from an internal workstation
Base events
Detection of an access to a Hacking website **Frequency:** Simultaneous high severity and sometimes significant frequency **Severity:** 4 **Detection means:** Automatic production possible (logs of Internet outbound devices and of URL filtering software, and SIEM tool) **Detection level:** 2 (detection rate can be up to 60 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of incidents detected during the last 30 days **Derived measure 2:** idem Derived Measure 1 **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 100 incidents for a standard organization (low scattering level according to companies or organizations)
Link with ISO/IEC 27002 [2]
A8 control area
Maturity KPSI
5, 6

Family IDB_LOG: Deactivating of logs recording

IDB_LOG.1: Deactivating of logs recording by an administrator
This event is generally decided and deployed by an administrator in order to improve performance of the system under his/her responsibility (illicit voluntary stoppage). This indicator is a reduced subset of indicator IUS_RGH.5.
Base events
Detection of deactivation of logs recording by an administrator **Frequency:** Both important and significant frequency (production of logs often viewed as limiting and of relative importance by administrators, and therefore handled with lesser attention except in the event of a strict security monitoring and a strong reaction). **Severity:** 2 or 3 **Detection means:** Automatic production possible (logs of access controls to servers, SIEM tool) **Detection level:** 3 (detection rate can be up to 80 %)
Indicator production
Base measure: Date of the event, identity of the administrator **Derived measure 1:** Number of administrators with such a behaviour detected during the last 30 days **Derived measure 2:** idem Derived Measure 1 **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 1 administrator for 100 servers (low scattering level according to organizations, except in ones with strong reaction vis-à-vis the personnel in question, where this figure is in a downward trend)
Link with ISO/IEC 27002 [2]
A8 and A10 control areas
Maturity KPSI
5, 6

Category IWH (Whole incident categories)

Indicators of this category are indicators that concern all categories of incidents.

Family IWH_VNP: Non-patched or poorly patched vulnerability exploitation

IWH_VNP.1: Exploitation of a software vulnerability without available patch
This indicators measures security incidents that are the result of an exploitation of a disclosed software vulnerability that has no available patch (with or without an applied workaround measure). It is used to assess the intensity of the exploitation of recently disclosed software vulnerabilities (zero day or not). Patching here applies only to standard software (excluding bespoke software), and the scope is limited to workstations (OS, browsers and various add-ons and plug-ins, office automation standard software).
Base events
Detection of an incident due to the exploitation of a software vulnerability without available patch **Frequency:** Key to know what is the status of software vulnerabilities that are possibly exploited to generate incidents **Severity:** 3 **Detection means:** Semi-automatic production (need to manually analyse and consolidate incidents) **Detection level:** 2 (detection rate can be up to 50 %, with the non-detected complement corresponding with little qualified incidents)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of all detected and categorized security incidents **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 60 days **State-of-the-art value:** (Derived measure 2) 10 % for a standard organization (low scattering level according to companies or organizations)
Link with ISO/IEC 27002 [2]
A13 control area
Maturity KPSI
3, 4, 5, 6

IWH_VNP.2: Exploitation of a non-patched software vulnerability
This indicators measures security incidents that are the result of the exploitation of a non-patched software vulnerability though a patch exists. It is used to assess effectiveness or application of patching-related organization and processes and tools (patching not launched). It is linked with indicator VOR_VNP.2 that is intended to assess problems of exceeding the "time limit for the window of exposure to risks". It has the same limitations as IWH_VNP.1 regarding scope.
Base events
Detection of an incident due to the exploitation of a non-patched software vulnerability **Frequency:** Key to know what is the status of software vulnerabilities that are possibly exploited to generate incidents **Severity:** 3 **Detection means:** Semi-automatic production (need to manually analyse and consolidate incidents) **Detection level:** 2 (detection rate can be up to 50 %, with the non-detected complement corresponding with little qualified incidents)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of all detected and categorized security incidents **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 60 days **State-of-the-art value:** (Derived measure 2) 15 % for a standard organization (low scattering level according to companies or organizations, except in ones with very efficient patch management processes, where this figure can be cut in half). It should be noted however that it is contrary to economic and effectiveness considerations to patch everything, given the low to mean severity level of many vulnerabilities does not justify it
Link with ISO/IEC 27002 [2]
A13 control area
Maturity KPSI
3, 4, 5, 6

IWH_VNP.3: Exploitation of a poorly-patched software vulnerability
This indicator measures security incidents that are the result of the exploitation of a poorly patched software vulnerability. It is used to assess effectiveness of patching-related organization and processes and tools (process launched but patch not operational - Cf. no reboot, etc.). It is linked with indicator VOR_VNP.1, IWH_VNP.1 and IWH_VNP.2. It has the same limitations as IWH_VNP.1 regarding scope.
Base events
Detection of an incident due to the exploitation of a poorly-patched software vulnerability **Frequency:** Key to know what is the status of software vulnerabilities that are possibly exploited to generate incidents **Severity:** 3 **Detection means:** Semi-automatic production (need to manually analyse and consolidate incidents) **Detection level:** 2 (detection rate can be up to 50 %, with the non-detected complement corresponding with little qualified incidents)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of all detected and categorized security incidents **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 60 days **State-of-the-art value:** (Derived measure 2) 5 % for a standard organization (low scattering level according to companies or organizations, except in ones with very efficient patch management processes, where this figure can be cut in half)
Link with ISO/IEC 27002 [2]
A13 control area
Maturity KPSI
3, 4, 5, 6

Family IWH_VCN: Configuration vulnerability exploitation

IWH_VCN.1: Exploitation of a configuration flaw
This indicator measures security incidents that are the result of the exploitation of a configuration flaw on servers or workstations. A configuration flaw should be considered as a nonconformity against state-of-the-art security policy.
Base events
Detection of an incident due to the exploitation of a configuration vulnerability **Frequency:** Key to know incidents made possible by configuration flaws **Severity:** 3 **Detection means:** Semi-automatic production (need to manually analyse and consolidate incidents) **Detection level:** 2 (detection rate can be up to 50 %, with the non-detected complement corresponding with little qualified incidents)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of all detected and categorized security incidents **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 60 days **State-of-the-art value:** (Derived measure 2) 30 % for a standard organization (high scattering level according to companies or organizations, depending on their maturity level, on the existence of low-level technical security policies and on a continuous checking of non-conformities)
Link with ISO/IEC 27002 [2]
A13 control area
Maturity KPSI
2, 4, 5, 6

Family IWH_UKN: Unknown incidents

IWH_UKN.1: Not categorized security incidents
This indicator measures all types of incidents that are new and/or a complex combination of more basic incidents and cannot be fully qualified and therefore precisely categorized.
Base events
Detection of a not inventoried security incident **Frequency:** Key to know such incidents since they generally correspond with exploitation of new vulnerabilities or weaknesses and/or to weakened SOC skills **Severity:** 3 or 4 (according to incidents criticality) **Detection means:** Manual production **Detection level:** 2 (detention rate can be up to 70 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of all detected and categorized security incidents **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 4 % for a standard organization (appreciable scattering level according to companies or organizations, depending on their level of maturity in the usage of monitoring and detection tools, and on their dedication to SIEM approaches)
Link with ISO/IEC 27002 [2]
A13 control area
Maturity KPSI
4, 5, 6

Family IWH_UNA: Incidents on not addressed assets

IWH_UNA.1: Security incidents on non-inventoried and/or not managed assets
This indicator measures security incidents tied to assets (on servers) non-inventoried and not managed by appointed teams. It is a key indicator insofar as a high percentage of incidents corresponds with this indicator on average in the profession (according to some public surveys).
Base events
Detection of a security incident on an not inventoried asset **Frequency:** Key to know such incidents since they are the immediate and easier way of progress **Severity:** 3 or 4 (according to incidents criticality) **Detection means:** Manual production **Detection level:** 2 (detention rate can be up to 70 % , with the non-detected complement corresponding with very little qualified incidents)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of all detected and categorized security incidents **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 40 % for a standard organization (notable scattering level according to companies or organizations, depending on their level of attention to the identification of equipment or servers or PCs connected to the network and to systems and applications mapping). NOTE**:** The 70 % figure provided corresponds with a series of companies and organizations that have faced notable and often obvious IT security problems, and that could therefore be considered to be amongst the least efficient
Link with ISO/IEC 27002 [2]
A7 control area
Maturity KPSI
1, 5, 6

5.5 Indicators related to vulnerabilities

The recommended operational indicators (with behavioural, software, configuration, general security technical and organizational vulnerabilities) are the following (51 in all).

Category VBH (Behavioural vulnerabilities)

Indicators of this category apply to the existence of abnormal behaviours that could lead to security incidents.

Family VBH_PRC: Dangerous protocols used

VBH_PRC.1: Server accessed by an administrator with unsecure protocols
This indicator measures the use of insecure protocols set up by an administrator to get access to organization-based externally accessible servers making an external intrusion possible. Insecure protocol means unencrypted, without time-out, with poor authentication means etc. (for example Telnet).
Base events
Detection of unsecure protocols used by administrators to get access to externally accessible servers **Frequency:** High severity (any possible drift should be closely monitored) **Severity:** 2 or 3 (according to existence or not of a timeout on the used protocol, since exploitation in the system by an intruder is possible if the administrator is absent) **Detection means:** Possible automatic production (logs of concerned perimeter-based systems or equipment, and SIEM tool) **Detection level:** 2 (detection rate can be up to 50 %, therefore limited since completeness of the monitoring is impossible)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of system administrators **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) Twice by administrator (appreciable scattering level according to companies or organizations, depending on the existence or not of a SIEM approach and on a reaction to the administrators in question)
Link with ISO/IEC 27002 [2]
A8 control area
Maturity KPSI
4, 5, 6

VBH_PRC.2: P2P client in a workstation
This indicator measures the installation of P2P clients set up by a user on its professional workstation with the risk of partial or full sharing of the workstation content. It applies to workstations that are either connected to the organization's network from within the organization or directly connected to the public network from outside (notably home). There is a high risk of accidental sharing (in one quarter of all cases) of files that may host confidential company data. It is most often carried out through HTTP channel (proposed on all of these services).
Base events
Detection of a P2P client installed in a workstation **Frequency:** Simultaneously high severity and high frequency (these days, one of the most frequent security flaws within organizations, even in case of filtering of the most commonly used P2P protocols at perimeter level - see usage of HTTP) **Severity:** 2 to 4 (according to level of sharing) **Detection means:** Automatic production possible (logs of central management tools for proactive PC protection software - see especially logs regarding ActiveX installation attempts, logs of outbound network devices, and SIEM tool) **Detection level:** 2 (detection level possibly attaining 50 %, therefore limited due to imperfect software configuration and to SIEM processing load limits)
Indicator production
Base measure: Date of the event, identity of the user that performed the installation **Derived measure 1:** Number of users that have performed this installation detected during the last 30 days **Derived measure 2:** idem Derived Measure 1 **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 30 users for a standard organization (appreciable scattering level according to companies or organizations, depending on the existence or not of a SIEM approach and on an individual reaction to the faulty users). 10 % of this figure leads to an external exploitation of unwitting PC file sharing
Link with ISO/IEC 27002 [2]
A8 control area
Maturity KPSI
5, 6

VBH_PRC.3: VoIP clients in a workstation
This indicator measures VoIP clients installed by a user on his/hers own workstation in order to use a peer-to-peer service. It applies to workstations connected to an organization's network from within the organization or directly connected to the public network from outside (notably home). The associated risk is to exchange dangerous Office documents. It is most often carried out through HTTP channel (proposed on all of these services).
Base events
Detection of a VoIP client installed in a workstation **Frequency:** Simultaneously high severity and medium frequency (these days, one of the most frequent security flaws within organizations, even in case of filtering of the most commonly used VoIP protocols at perimeter level - Cf. usage of HTTP) **Severity:** 3 **Detection means:** Automatic production possible (logs of central management tools for proactive PC protection software - Cf. especially logs regarding ActiveX installation attempts, logs of outbound network devices, and SIEM tool) **Detection level:** 2 (detection level possibly attaining 50 %, therefore limited due to SIEM processing load limits)
Indicator production
Base measure: Date of the event, identity of the user that performed the installation **Derived measure 1:** Number of users that have performed this installation detected during the last 30 days **Derived measure 2:** idem Derived Measure 1 **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 20 users for a standard organization (appreciable scattering level according to companies or organizations, depending on the existence or not of a SIEM approach and on an individual reaction to the faulty users)
Link with ISO/IEC 27002 [2]
A8 control area
Maturity KPSI
5, 6

VBH_PRC.4: Outbound connection dangerously set up
This indicator measures outbound connection dangerously set up to get remote access to the company's internal network without using an inbound VPN link and a focal access point with possible exploitation by an external intruder. The outbound connection method consists for example in using a GoToMyPC™ software or a LogMeIn® software or a computer to computer connection in tunnel mode.
Base events
Detection of an outbound connection set up from an internal workstation **Frequency:** Frequency still relatively high (situation notably due to a sought sensation of freedom, to a desire for remote access to their professional environment by users who do not have a VPN access, etc.) **Severity:** 2 or 3 (depending on the software used) **Detection means:** Automatic production possible (logs of the Web proxy outbound devices, and SIEM tool) **Detection level:** 2 (detection rate can be up to 60 %, therefore limited since many possibilities to carry out this action)
Indicator production
Base measure: Date of the event, identity of the user that performed the installation **Derived measure 1:** Number of users that have performed this installation detected during the last 30 days **Derived measure 2:** idem Derived Measure 1 **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 40 users for a standard organization (appreciable scattering level according to companies or organizations, depending on the size of users population with remote access rights, on the existence or not of a SIEM approach and on an individual reaction to the faulty administrators)
Link with ISO/IEC 27002 [2]
A8 control area
Maturity KPSI
5, 6

VBH_PRC.5: Not compliant laptop computer used to establish a connection
This indicator measures remote or local connection to the organization's internal network from a roaming laptop computer that is organization-owned and is configured with weak parameters. In this situation and in case of the existence of a software to check compliance of roaming computers, another related software blocks the connection in principle and prevents its continuation.
Base events
Detection of not compliant lap top computers used to establish a connection **Frequency:** Both high severity and still high frequency (several possible causes, including the presence of personal software, deactivated AV or firewall, etc.) **Severity:** 3 (more serious for roaming laptop PCs than for desktop PCs) **Detection means:** Automatic production possible (logs of the compliance checking software, and SIEM tool) **Detection level:** 1 or 2 (detection rate possibly attaining 40 %, provided that the SIEM tool has been closely coupled with the tool used to check compliance of PCs - Cf. list of roaming laptop PCs)
Indicator production
Base measure: Date of the event, identity of the user **Derived measure 1:** Number of users that have performed this connection detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of lap top computers **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 1 % for a standard organization with assumption of 10 000 authorized VPN accesses (appreciable scattering level according to companies or organizations, depending on the existence or not of a SIEM approach and on an individual reaction to the faulty users)
Link with ISO/IEC 27002 [2]
A8 control area
Maturity KPSI
2, 5, 6

VBH_PRC.6: Other unsecure protocols used
This indicator measures other unsecure or dangerous protocols set up with similar behaviours. The other cases are the other than the 5 previous ones (VBH_PRC.1 to VBH_PRC.5). It relates to dangerous or abusive usages, i.e. situations where usages are not required and where other more secure solutions exist.
Base events
Detection of unsecure protocols used (other than the 5 previous ones) **Frequency:** Rather high frequency (notably in the Windows and open worlds) **Severity:** 2 (global level, but appreciable variations depending on the cases) **Detection means:** Semi-automatic production possible (logs of the systems in question and SIEM tool) **Detection level:** 2 (detection rate can be up to 50 %, therefore limited since impossible completeness of the monitoring)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** idem Derived Measure 1 **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 100 events for a standard organization (appreciable scattering level according to companies or organizations, depending on the existence or not of a SIEM approach and on an individual reaction to the faulty administrators)
Link with ISO/IEC 27002 [2]
A8 control area
Maturity KPSI
5, 6

Family VBH_IAC: Internet illicit access

VBH_IAC.1: Outbound controls bypassed to access Internet
This indicator measures the detection of Internet access from the internal network by means that bypass the outbound security devices. It primarily relates to Internet accesses from a perimeter area or to tunnelling (SSL port 443) or to straight accesses (via an ADSL link or public Wi-Fi access points and the telephone network) or to accesses via Smartphones connected to the workstation. The main underlying motivation is to prevent user tracking.
Base events
Detection of outbound controls bypassed to access Internet from the internal network **Frequency:** Significant frequency **Severity:** 2 to 4 (depending on the level of danger of accessed sites, or depending on the sensitivity of the network to which the PC is connected - Cf. possibility of PC access from the exterior) **Detection means:** Automatic production possible (logs of PC management tools and of PC based HIDS software, and SIEM tool) **Detection level:** 1 (detection rate can be up to 30 %)
Indicator production
Base measure: Date of the event, identity of the user **Derived measure 1:** Number of users that have performed this kind of connection detected during the last 30 days **Derived measure 2:** idem Derived Measure 1 **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 50 users for a standard organization (high scattering level according to companies or organizations, depending on restricting or not workstations, and on the existence or not of a SIEM approach associated with an individual reaction to the faulty users)
Link with ISO/IEC 27002 [2]
A8 and A11 control areas
Maturity KPSI
5, 6

VBH_IAC.2: Anonymization site used to access Internet
This indicator measures the detection of anonymous Internet access from an internal workstation through an anonymization site. The goal is to maintain free access and to avoid organization's filtering of accesses to forbidden websites.
Base events
Detection of an anonymization site used to access Internet **Frequency:** Sometimes significant frequency **Severity:** 3 **Detection means:** Automatic production possible (logs of Internet outbound devices and of URL filtering software, and SIEM tool) **Detection level:** 3 (detection rate can be up to 80 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of unique users that have performed this kind of connection detected during the last 30 days **Derived measure 2:** idem Derived Measure 1 **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 200 users for a standard organization (low scattering level according to companies or organizations)
Link with ISO/IEC 27002 [2]
A8 and A15 control areas
Maturity KPSI
5, 6

Family VBH_FTR: File illicit transfer with outside

VBH_FTR.1: Files recklessly downloaded
This indicator measures the download of files from an external website that is not known (no reputation) within the profession to an internal workstation. "No reputation" can be assessed by information provided by URL outbound filtering devices.
Base events
Detection of files recklessly downloaded from an unknown website **Frequency:** High frequency **Severity:** 2 **Detection means:** Automatic production possible (logs of the Web proxy outbound devices, and SIEM tool) **Detection level:** 2 (detection rate can be up to 60 %, therefore limited since difficulties assessing dependable sites)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** idem Derived Measure 1 **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 350 events for a standard organization (high scattering level according to companies or organizations, depending on the existence or not of a SIEM approach and on an individual reaction to the faulty users)
Link with ISO/IEC 27002 [2]
A8 and A10 control areas
Maturity KPSI
5, 6

VBH_FTR.2: Personal public instant messaging account used for business file exchanges
This indicator measures the use of personal public instant messaging accounts for business exchanges with outside. This file exchange method has to be avoided due to network AV software bypassing and to identify lesser effectiveness of AV software.
Base events
Detection of personal public instant messaging accounts used for business file exchanges **Frequency:** Medium severity and rather high frequency **Severity:** 3 **Detection means:** Automatic production possible (logs of proactive PC protection software central administration tools, and SIEM tool) **Detection level:** 2 (detection rate can be up to 50 %)
Indicator production
Base measure: Date of the event, identity of the user **Derived measure 1:** Number of users with this behaviour detected during the last 30 days **Derived measure 2:** idem Derived Measure 1 **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 300 users for a standard organization (relatively high scattering level according to companies or organizations, depending on organizations' maturity regarding security and quality, and on an individual reaction to faulty users)
Link with ISO/IEC 27002 [2]
A8 control area
Maturity KPSI
5, 6

VBH_FTR.3: Personal public messaging account used for business file exchanges
This indicator measures the use of personal public messaging accounts for business file exchanges with the exterior. The risk is to expose information to external attackers.
Base events
Detection of personal public messaging accounts used for business file exchanges **Frequency:** Medium severity and rather significant frequency **Severity:** 2 **Detection means:** Automatic production possible (logs of proactive PC protection software central administration tools, and SIEM tool) **Detection level:** 1 or 2 (detection rate can be up to 40 %)
Indicator production
Base measure: Date of the event, identity of the user **Derived measure 1:** Number of users with this behaviour detected during the last 30 days **Derived measure 2:** idem Derived Measure 1 **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 400 users for a standard organization (relatively high scattering level according to companies or organizations, depending on organizations' maturity regarding security and quality, and on an individual reaction to faulty users)
Link with ISO/IEC 27002 [2]
A8 control area
Maturity KPSI
5, 6

Family VBH_WTI: Workstation used without relevant usual security

VBH_WTI.1: Workstations accessed in administrator mode
This indicator measures access to workstations in administrator mode without authorization.
Base events
Detection of workstations accessed in Administrator mode **Frequency:** High severity and sometimes significant frequency **Severity:** 2 or 3 (according to connection possibilities with the WS) **Detection means:** Semi-automatic production possible (periodic even WS checking with a compliance checking tool that checks for non-compliant configurations, and SIEM tool connected to WS local accesses management - Cf. Active Directory for example, if existing - for continuous monitoring of accesses in non-authorized administrator mode) **Detection level:** 2 (detection rate can be up to 50 %)
Indicator production
Base measure: Date of the event, identity of the user **Derived measure 1:** Number of users with this behaviour detected during the last 30 days **Derived measure 2:** idem Derived Measure 1 **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 60 days **State-of-the-art value:** (Derived measure 2) 75 users for a standard organization (very high scattering level according to companies or organizations, depending on securing or not workstations, and on the existence or not of a SIEM approach associated with an individual reaction to the faulty users)
Link with ISO/IEC 27002 [2]
A8 and A15 control areas
Maturity KPSI
2, 4, 5, 6

VBH_WTI.2: Personal storage devices used
This indicator measures the use personal storage devices on a professional workstation to input or output information or software. Mobile or removable personal storage devices include USB tokens, smartphones, tablets, etc. It is not applicable to personal devices authorized by security policy (Cf. VBH_WTI.3 and BYOD).
Base events
Detection of personal storage devices used **Frequency:** Very high frequency **Severity:** 3 **Detection means:** Automatic production possible (SIEM tool connected to WS local accesses management for continuous monitoring of storage devices accesses) **Detection level:** 1 (detection rate can be up to 10 to 20 %, provided strong local accesses management exists)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** idem Derived Measure 1 **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 350 events for a standard organization (high scattering level according to companies or organizations, depending on securing or not workstations, and on the existence or not of a SIEM approach associated with an individual reaction to the faulty users)
Link with ISO/IEC 27002 [2]
A8 control area
Maturity KPSI
2, 4, 5, 6

VBH_WTI.3: Personal devices used without compartmentalization (BYOD)
This indicator measures the lack of or the removal of basic security measures meant to compartmentalize professional activities on personal devices. Personal devices (BYOD) include PCs, tablets, smartphones, etc.
Base events
Detection of personal devices used for professional activities and not compartmentalized **Frequency:** Very high frequency **Severity:** 2 **Detection means:** Automatic production possible (SIEM tool connected to BYOD devices accesses management) **Detection level:** 1 (detection rate can be up to 10 to 20 %, provided strong local accesses management exists)
Indicator production
Base measure: Date of the event, identity of the user **Derived measure 1:** Number of users with this behaviour detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of personal devices **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 50 % for a standard organization (high scattering level according to companies or organizations, depending on the existence or not of a SIEM approach associated with an individual reaction to the faulty users)
Link with ISO/IEC 27002 [2]
A8 control area
Maturity KPSI
2, 4, 6

VBH_WTI.4: Not encrypted sensitive files exported
This indicator measures the lack of encryption of sensitive files uploaded from a professional workstation to professional mobile or removable storage devices.
Base events
Detection of not ciphered sensitive files exported from a workstation to professional mobile or removable storage devices **Frequency:** Significant frequency **Severity:** 4 **Detection means:** Semi-automatic production possible (SIEM tool connected to PC local accesses management for continuous monitoring of storage devices accesses, and asset sensitivity classification) **Detection level:** 1 (detection rate can be up to 10 to 20 %, provided strong local accesses management and detailed asset sensitivity classification exist)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** idem Derived Measure 1 **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 30 events for a standard organization (high scattering level according to companies or organizations, depending on securing or not workstations, and on the existence or not of a SIEM approach associated with an individual reaction to the faulty users)
Link with ISO/IEC 27002 [2]
A8 control area
Maturity KPSI
5, 6

VBH_WTI.5: Personal software used
This indicator measures the presence of personal software on a professional workstation that does not comply with the corporate security policy. It corresponds with all types of local unauthorized software (with a user licence or not), such as common personal software (games, office automation etc.) or more dangerous ones (hacking etc.). It should be added that VBH_PRC.2 and VBH_PRC.3 are a share of this indicator, and that this indicator is a subset of VBH_WTI.1.
Base events
Detection of personal software used on a professional workstation **Frequency:** Number of users in question generally significant **Severity:** 2 or 3 (depending on the type of software) **Detection means:** Automatic production (periodic checking of PCs with a scanner or a compliance checking tool) **Detection level:** 3 (detection rate can be up to 100 %)
Indicator production
Base measure: Date of the event, identity of the user **Derived measure 1:** Number of users with this behaviour detected during the last 30 days **Derived measure 2:** idem Derived Measure 1 **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 60 days **State-of-the-art value:** (Derived measure 2) 65 users for a standard organization (fairly high scattering level according to companies or organizations, depending on organizations' maturity regarding security and quality)
Link with ISO/IEC 27002 [2]
A8 and A15 control areas
Maturity KPSI
2, 5, 6

VBH_WTI.6: Mailbox or Internet access with admin mode
This indicator applies to users using their admin account on a workstation.to access their own mailbox or Internet. This behaviour is particularly dangerous since malware (through attached pieces on email or drive-by download on Web browser) are far easier to install on the workstation in this case.
Base events
Detection of such a behaviour **Frequency:** Number of users in question low **Severity:** 4 **Detection means:** Semi-automatic production (SIEM tool connected to Web proxies, and to PC local software and accesses management - Cf. Active Directory for example, if existing - for continuous monitoring of accesses in administrator mode) **Detection level:** 3 (detection rate can be up to 100 %)
Indicator production
Base measure: Date of the event, identity of the user **Derived measure 1:** Number of users with this behaviour detected during the last 30 days **Derived measure 2:** idem Derived Measure 1 **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 60 days **State-of-the-art value:** (Derived measure 2) 15 users for a standard organization (medium scattering level according to companies or organizations, depending on organizations' maturity regarding security)
Link with ISO/IEC 27002 [2]
A8 and A15 control areas
Maturity KPSI
2, 4, 5, 6

Family VBH_PSW: Passwords illicitly handled or managed

VBH_PSW.1: Weak passwords used
The required strength of passwords depends on the organization's security policy, but usable general recommendations in ISO/IEC 27002 [2].
Base events
Detection of an account with weak password (password cracked using a dictionary-based attack method for 4 hours for each password (operation run each month)) **Frequency:** Simultaneously generally high frequency and high severity **Severity:** 3 **Detection means:** Possible automatic production (access to user passwords files on systems, with "cracking" tools) **Detection level:** 2 (detection rate possibly attaining 70 %, using current "cracking" tools and running them for a fixed time - 4 hours in the presently selected hypothesis)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of user accounts **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 20 % for a standard organization (high scattering level according to companies or organizations, depending on the existence or not of an enterprise-wide SIEM approach and on an individual reaction to the faulty users)
Link with ISO/IEC 27002 [2]
A8 and A11 control areas (adopted definition of password solidity is that of clause A11.3.1 of the ISO/IEC 27002 [2] standard)
Maturity KPSI
2, 4, 6

VBH_PSW.2: Passwords not changed
This indicators measures password not changed in due periodic time (case of changes not periodically imposed). Situations in which changes are not periodically imposed by accessed systems themselves remain fairly frequent within organizations (apart from Active Directory), the figure being around 25 % of the cases on average.
Base events
Detection of an account with not-changed password **Frequency:** Simultaneously high frequency and rather high severity **Severity:** 2 **Detection means:** Automatic production possible (logs of systems in question) **Detection level:** 2 since doubtful cases - holidays, departure, … (detection rate can be up to 60 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of user accounts **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 25 % for a standard organization (high scattering level according to companies or organizations, depending on the existence or not of a SIEM approach and on an individual reaction to the faulty users)
Link with ISO/IEC 27002 [2]
A8 and A11 control areas
Maturity KPSI
2, 4, 6

VBH_PSW.3: Administrator passwords not changed
This indicators measures password not changed in due periodic time by an administrator in charge of an account used by automated applications and processes (case of changes not periodically imposed). Situations in which changes are not periodically imposed by accessed systems themselves remain fairly frequent within organizations (apart from Active Directory), the figure being around 25 % of the cases on average.
Base events
Detection of an administrator account with not-changed password **Frequency:** Simultaneously high severity and high frequency **Severity:** 3 **Detection means:** Automatic production possible (logs of systems in question) **Detection level:** 2 since doubtful cases - holidays, etc. (detection rate can be up to 60 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of administrator accounts **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 20 % for a standard organization (high scattering level according to companies or organizations, depending on the existence or not of a SIEM approach and on an individual reaction to the faulty administrators)
Link with ISO/IEC 27002 [2]
A8 and A11 control areas
Maturity KPSI
2, 4, 6

Family VBH_RGH: Access rights illicitly granted

VBH_RGH.1: Not compliant user rights granted illicitly by an administrator
This indicator measures the granting of not compliant user rights by an administrator outside any official procedure. This vulnerability may originate with an error, negligence or malice.
Base events
Detection of not compliant user rights granted by an administrator **Frequency:** Simultaneously high severity and high frequency **Severity:** 3 (since non-compliant rights are generally exploited unlawfully by users - see IUS_RGH.3) **Detection means:** Automatic production possible (logs of access controls to systems in question, logs of the reference database of rights, and SIEM tool) **Detection level:** 3 (detection rate can be up to 100 %, provided that a SIEM tool is used with an updated reference database of administrator rights)
Indicator production
Base measure: Date of the event, identity of the administrator **Derived measure 1:** Number of administrators with such a behaviour (unique events) during the last 30 days **Derived measure 2:** Ratio of Number of administrators with such a behaviour during the last 30 days to Number of administrators **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 0,8 % for a standard organization (low scattering level according to companies or organizations)
Link with ISO/IEC 27002 [2]
A8, A11 and A15 control areas
Maturity KPSI
2, 4, 5, 6

Family VBH_HUW: Human weakness

VBH_HUW.1: Human weakness exploited by a spear phishing message meant to entice or appeal to do something possibly harmful to the organization
This vulnerability typically includes clicking on an Internet link or opening an attached document
Base events
Detection of these human weaknesses successfully exploited **Frequency**: High frequency **Severity:** 2 **Detection means:** Manual production (by periodic polling on a changing sample of users) **Detection level:** 1 (detection rate can be no more than 20 %)
Indicator production
Base measure: Detection of such vulnerabilities **Derived measure 1:** Number of users with such a behaviour detected during the last 30 days **Derived measure 2:** Previous number measured to the total number of users **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 10 % for a standard organization (high scattering level according to companies or organizations depending on the intensity of awareness campaigns and on periodic field exercises)
Link with ISO/IEC 27002 [2]
A8 control area
Maturity KPSI
6, 7

VBH_HUW.2: Human weakness exploited by exchanges meant to entice or appeal to tell some secrets to be used later
This vulnerability applies to discussions through on-line media leading to leakage of personal identifiable information (PII) or various business details to be used later (notably for identity usurpation)
Base events
Detection of these human weaknesses successfully exploited **Frequency:** High frequency **Severity:** 2 **Detection means:** Manual production (by periodic polling on a changing sample of users) **Detection level:** 1 (detection rate can be no more than 30 %)
Indicator production
Base measure: Detection of such vulnerabilities **Derived measure 1:** Number of users with such a behaviour detected during the last 30 days **Derived measure 2:** Previous number measured to the total number of users **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** Not applicable (too variable and too many different cases)
Link with ISO/IEC 27002 [2]
A8 control area
Maturity KPSI
6, 7

Category VSW (Software vulnerabilities)

Indicators of this category apply to the existence of weaknesses in software that could be exploited and lead to security incidents.

Family VSW_WSR: Web server software vulnerabilities

VSW_WSR.1: Web applications software vulnerabilities
This indicators measures software vulnerabilities detected in Web applications running on externally accessible servers.
Base events
Detection of software vulnerabilities in web applications running in externally accessible servers **Frequency:** High frequency (any possible upward drift should be closely monitored given possible direct relationship with secure software development) **Severity:** 3 or 4 **Detection means:** Semi-automatic production (Periodic software vulnerability scanning) **Detection level:** 2 (detection rate can be up to 70 %, since most frequent vulnerabilities are well established and known within the profession, and scanning tools or services automated)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of web applications **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 80 vulnerabilities per Web application software (high scattering level according to companies or organizations, depending on the existence or not of strict secure software development)
Link with ISO/IEC 27002 [2]
A12 control area
Maturity KPSI
3, 6

Family VSW_OSS: OS software vulnerabilities

VSW_OSW.1: OS software vulnerabilities regarding servers
This indicators measures software vulnerabilities detected in OS running on externally accessible servers.
Base events
Detection of software vulnerabilities in operating systems running in externally accessible servers **Frequency:** High frequency (any possible upward drift should be closely monitored given risk of exploitation) **Severity:** 1 to 4 **Detection means:** Semi-automatic production (Periodic OS vulnerability scanning with tools or services) **Detection level:** 2 (detection rate can be up to 70 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of externally visible servers **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 1 vulnerability per OS (appreciable scattering level according to companies or organizations, depending on the existence or not of strict secure patching processes)
Link with ISO/IEC 27002 [2]
A12 control area
Maturity KPSI
3, 6

Family VSW_WBR: Web browser software vulnerabilities

VSW_WBR.1: Web browsers software vulnerabilities
This indicators measures software vulnerabilities detected in Web browsers running on workstations.
Base events
Detection of software vulnerabilities in web browsers running in workstations **Frequency:** High frequency (any possible upward drift should be closely monitored given risk of exploitation) **Severity:** 2 to 4 **Detection means:** Semi-automatic production (Periodic Web browser vulnerability scanning with tools or services) **Detection level:** 2 (detection rate can be up to 70 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of workstations **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 1 vulnerability per browser (appreciable scattering level according to companies or organizations, depending on the existence or not of strict secure patching processes)
Link with ISO/IEC 27002 [2]
A12 control area
Maturity KPSI
3, 6

Category VCF (Configuration vulnerabilities)

Indicators of this category apply to the existence of weaknesses in the configuration of IT devices that could be exploited and lead to security incidents.

Family VCF_DIS: Dangerous or illicit services

VCF_DIS.1: Dangerous or illicit services on externally accessible servers
This indicator measures the presence of illicit and dangerous system services running on an externally accessible server.
Base events
Detection of vulnerable or useless services running in externally accessible servers **Frequency:** Rather high severity **Severity:** 2 or 3 (depending on the usability of system software) **Detection means:** Manual or semi-automatic production (continuous checking with logs of OS) **Detection level:** 2 (detection rate can be up to 70 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of externally accessible servers **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 1 % for a standard organization (very high scattering level according to companies or organizations, depending on organizations' maturity regarding security and quality)
Link with ISO/IEC 27002 [2]
A15 control area
Maturity KPSI
1, 2, 5, 6

Family VCF_LOG: Log production shortcomings

VCF_LOG.1: Insufficient size of the space allocated for logs
Such event could cause an overflow in case of quick series of unusual actions.
Base events
Detection of a production server or production application software having insufficient size of the space allocated for logs **Frequency:** Significant frequency (production of logs often viewed as limiting and of relative importance by administrators, and therefore handled with secondary priority against optimization of the size of the memory and system performance, except in the event of a precise policy, a strict security monitoring and a strong reaction) **Severity:** 1 **Detection means:** Automatic production possible (system administration and SIEM tool) **Detection level:** 2 (detection rate can be up to 50 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of the company's or the organization's systems **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 4 % (high scattering level according to companies or organizations, depending on the level of the IT security awareness of administrators)
Link with ISO/IEC 27002 [2]
A10 and A15 control areas
Maturity KPSI
2, 5, 6

Family VCF_FWR: Weak firewall configuration

VCF_FWR.1: Weak firewall filtering rules
This indicator measures the gaps between the active firewall filtering rules and the security policy.
Base events
Detection of firewall filtering rules not conform with the security policy **Frequency:** Simultaneously rather high severity and relatively high frequency (significant number of errors due to continual changes of network access authorizations regarding partners and service providers) **Severity:** 2 **Detection means:** Automatic production possible (logs of firewall compliance checking tools, SIEM tool) **Detection level:** 1 (precise origin of all links very difficult to obtain reliably - detection rate possibly attaining 30 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of firewall **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 12 events per firewall (relatively high scattering level according to companies or organizations, depending on the existence or not of checking tools used before modification of the existing rules)
Link with ISO/IEC 27002 [2]
A10, A11 and A15 control areas
Maturity KPSI
2, 6

Family VCF_WTI: Workstation wrongly configured

VCF_WTI.1: Workstation with a disabled or not updated AV and/or FW
This indicator measures the use of workstation with a disabled or lacking update AV and/or FW. The lack of update includes signature file older than x days (generally at least 6 days).
Base events
Detection of workstations with disabled or not updated AV and/or FW **Frequency:** Both medium severity and high frequency **Severity:** 4 **Detection means:** Semi-automatic production possible (AV and FW centralized monitoring and management) **Detection level:** 3 (detection rate possibly attaining 100 %)
Indicator production
Base measure: Date of the event, identity of the user **Derived measure 1:** Number of users with this behaviour detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of workstations within organization **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 60 days **State-of-the-art value:** (Derived measure 2) 10 % for a standard organization (high scattering level according to companies or organizations, depending on the existence or not of a strict PC sourcing and security policy, of a SIEM approach and on an individual reaction to the faulty users)
Link with ISO/IEC 27002 [2]
A10 and A15 control areas
Maturity KPSI
2, 5, 6

VCF_WTI.2: Autorun feature enabled on workstations
This indicator measures the presence of Autorun feature enabled on workstations.
Base events
Detection of Autorun feature enabled on workstations **Frequency:** High severity and sometimes rather high frequency **Severity:** 2 to 3 **Detection means:** Automatic production possible (logs of PC management tools, SIEM tool) **Detection level:** 3 (detection rate possibly attaining 90 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of workstations **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 60 days **State-of-the-art value:** (Derived measure 2) 10 % (high scattering level according to companies or organizations, depending on the existence or not of strict workstation sourcing and security policy and of workstation security policy enforcement continuous checking)
Link with ISO/IEC 27002 [2]
A10 and A15 control areas
Maturity KPSI
2, 6

Family VCF_UAC: User accounts wrongly configured

VCF_UAC.1: Access rights configuration not compliant with the security policy
This indicator measures access rights configuration that are not compliant with corporate security policy. This indicator is more reliable in case of existence of a central repository of user rights within organization (and of an IAM achievement)
Base events
Detection of access rights configuration not compliant with the security policy **Frequency:** Often high frequency, especially when IAM approaches are not existing (since assigned rights which are associated with not unique user identifiers are very difficult and even impossible to check) **Severity:** 3 **Detection means:** Possible automatic production (logs of the reference database for rights and/or of servers access controls and of the unique directory, and suited SIEM tool) **Detection level:** 2 (detection rate can be up to 70 %)
Indicator production
Base measure: Date of the event, identity of the user **Derived measure 1:** Number of unique users detected during the last 30 days **Derived measure 2:** idem Derived Measure 1 **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 60 days **State-of-the-art value:** (Derived measure 2) 60 non-conformities for a standard organization (relatively high scattering level according to companies or organizations, depending on the existence or not of more or less completed IAM achievement)
Link with ISO/IEC 27002 [2]
A11 and A15 control areas
Maturity KPSI
2, 4, 5, 6

VCF_UAC.2: Not compliant access rights on logs
This indicator measures non-compliant access rights on logs in servers which are sensitive and/or subject to regulations. This situation representing a key weakness since the necessary high confidence in the produced logs has been reduced to nothing. This indicator is a subset of VCF_UAC.1.
Base events
Detection of not compliant access rights configuration on logs in servers which are sensitive and/or subject to regulations **Frequency:** Often high frequency **Severity:** 2 or 3 (depending on ease of access to logs data for the system in question) **Detection means:** Possible automatic production (logs of the reference database for rights and/or of servers access controls and of the unique directory, and suited SIEM tool) **Detection level:** 2 or 3 (detection rate can be up to 80 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of servers **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 60 days **State-of-the-art value:** (Derived measure 2) 1 non-conformity per server (low scattering level according to companies or organizations)
Link with ISO/IEC 27002 [2]
A11, A13 and A15 control areas
Maturity KPSI
2, 4, 5, 6

VCF_UAC.3: Generic and shared administrator accounts
This indicator measures generic and shared administration accounts that are unnecessary or accounts that are necessary but without patronage. It concerns operating systems, databases and applications.
Base events
Detection of generic and shared administrator accounts **Frequency:** Rather high severity and often significant frequency **Severity:** 2 or 3 (depending on possible tracking or not of players by other systems) **Detection means:** Possible automatic production if access rights are accessible (administration of access rights) **Detection level:** 2 (detection rate can be up to 50 %, if IAM achievement)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of operating systems, database and application **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 60 days **State-of-the-art value:** (Derived measure 2) 4 by operating system , database or application (very low scattering level according to companies or organizations)
Link with ISO/IEC 27002 [2]
A10 and A15 control areas
Maturity KPSI
2, 4, 6

VCF_UAC.4: Accounts without owners
This indicator measures accounts without owners that have not been erased. These are accounts that have no more assigned users (for example after internal transfer or departure of the users from organization).
Base events
Detection of user accounts without owner **Frequency:** Both high severity and high frequency (existence of such accounts almost unavoidable with or without an IAM achievement) **Severity:** 3 **Detection means:** Automatic production easier if existence of an advanced IAM achievement (logs of central user rights management, logs of servers and SIEM tool) **Detection level:** 2 or 3 (detection rate can be up to 80 %, if IAM achievement)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of operating systems, database and application **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 60 days **State-of-the-art value:** (Derived measure 2) 10 per operating system , database or application (non-existent scattering level according to companies or organizations)
Link with ISO/IEC 27002 [2]
A11 control area
Maturity KPSI
2, 6

VCF_UAC.5: Inactive accounts
This indicator measures accounts inactive for at least 2 months that have not been disabled. These accounts are not used by their users due to prolonged but not definitive absence (long term illness, maternity, etc.), with the exclusion of messaging accounts (which should remain accessible to users from their home).
Base events
Detection of user accounts inactive for at least 2 months but not disable **Frequency:** Very often significant frequency (prolonged absence of users not taken into account and not managed at Information System level, in particular when IAM achievements do not exist) **Severity:** 2 **Detection means:** Automatic production easier if existence of an advanced IAM achievement (logs of central user rights management, logs of the unique directory and SIEM tool) **Detection level:** 2 if IAM achievement (detection rate possibly attaining 50 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of operating systems, database and application **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 60 days **State-of-the-art value:** (Derived measure 2) 11 per operating system , database or application (very low scattering level according to companies or organizations)
Link with ISO/IEC 27002 [2]
A11 control area
Maturity KPSI
2, 4, 6

Category VTC (General security technical vulnerabilities)

Indicators of this category measure the existence of weaknesses in the IT and physical architecture that could be exploited and lead to security incidents.

Family VTC_BKP: Back-up malfunction

VTC_BKP.1: Malfunction of server-hosted sensitive data safeguards
On servers hosting sensitive data with respect to availability, it concerns malfunctions of safeguards due to lack of periodic testing. This kind of event may be very serious since usually put trust is betrayed in a critical function.
Base events
Detection of sensitive data safeguards that are not up-and-running **Frequency:** Significant frequency **Severity:** 3 **Detection means:** Semi-automatic production (periodic testing campaigns) **Detection level:** 3 (detection rate can be up to 100 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of servers hosting sensitive safeguards **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 20 % (high scattering level according to companies or organizations, due to technical solutions)
Link with ISO/IEC 27002 [2]
A10 control area
Maturity KPSI
6, 7

Family VTC_IDS: IDS/IPS malfunction

VTC_IDS.1: Full unavailability of IDS/IPS
Many causes are possible, including deliberate disconnection by a network administrator (to streamline operations or since IDS/IPS output is deemed too difficult to use), unwitting disconnection (error by a network administrator), breakdown, software malfunction, etc.
Base events
Detection of a full unavailability of IDS/IPS **Frequency:** Rather high severity **Severity:** 3 **Detection means:** Automatic production possible (network devices management) **Detection level:** 3 (detection rate can be up to 100 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of IDS/IPS **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 0,01 per IDS or IPS (high scattering level according to companies or organizations)
Link with ISO/IEC 27002 [2]
A15 control area
Maturity KPSI
5, 6

Family VTC_WFI: Illicit Wi-Fi access points

VTC_WFI.1: Wi-Fi devices installed on the network without any official authorization
Many causes are possible, including for example local decisions for easier access of mobile users, rogue user behaviours or workstations configured as access points.
Base events
Detection of installation of Wi-Fi devices on the network without any official authorization **Frequency:** High severity and rather significant frequency **Severity:** 4 **Detection means:** Semi-automatic production possible (network devices scanning and discovery) **Detection level:** 3 (detection rate can be up to 100 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of Wi-Fi authorized access points **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 180 days **State-of-the-art value:** Not applicable
Link with ISO/IEC 27002 [2]
A10 control area
Maturity KPSI
2, 6

Family VTC_RAP: Illicit remote access

VTC_RAP.1: Remote access points used to gain unauthorized access
This indicator is interesting to assess whether such accesses are localized (local areas, countries, etc.) or involve the whole organization or are increasing and spreading to whole organization.
Base events
Detection of remote access points used to gain unauthorized access **Frequency:** Interesting figure **Severity:** 3 **Detection means:** Possible semi-automatic production (based on IDB_UID.1 and the seven IDB_RGH.x + logs of remote access points) **Detection level:** 1 (idem IDB_UID.1 and IDB_RGH.x - detection rate can be up to 30 %, provided that a SIEM tool is used and connected to a reference database of organization's rights, and to logs of remote access points)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of authorized access points **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 180 days **State-of-the-art value:** Not applicable, since far too variable according to companies or organizations (in principle, however, figure dropping sharply with advanced IAM achievements)
Link with ISO/IEC 27002 [2]
A11 control area
Maturity KPSI
5

Family VTC_NRG: Illicit network connections

VTC_NRG.1: Devices or servers connected to the organization's network without being registered and managed
According to some convergent studies, this event may be at the origin of some 70 % of all security incidents associated to malice.
Base events
Detection of devices or servers connected to the organization's network without being registered and managed **Frequency:** High severity and significant frequency **Severity:** 3 **Detection means:** Manual production (asset management and network scanning and discovery) **Detection level:** 2 or 3 (detection rate can be up to 80 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of authorized equipment **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 3 % (rather low scattering level according to companies or organizations, since it is difficult to maintain an equal and continuous quality of management and scanning)
Link with ISO/IEC 27002 [2]
A7 control area
Maturity KPSI
1

Family VTC_PHY: Physical access control

VTC_PHY.1: Not operational physical access control means
This indicator includes access to protected internal areas. The 1st cause is the lack of effective control of users at software level. The 2nd cause is hardware breakdown of a component in the chain.
Base events
Detection of not operational physical access control means **Frequency:** High severity and sometimes rather significant frequency **Severity:** 2 or 3 (according to the area sensitiveness level) **Detection means:** Automatic production possible (access control logs) **Detection level:** 3 (detection rate can be up to 100 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of protected areas **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 3 events per protected area (rather high scattering level according to companies or organizations)
Link with ISO/IEC 27002 [2]
A9 control area
Maturity KPSI
None

Category VOR (General security organizational vulnerabilities)

Indicators of this category measure the existence of weaknesses in the organization that could be exploited and lead to security incidents.

Family VOR_DSC: Discovery of attacks

VOR_DSC.1: Incidents with excessive time to discovery
This indicator measures stealthy security incidents difficult to detect. As most studies show, the time to discovery is often several months, time frame especially used to steal sensitive data. Incidents taken into account here are IEX_INT.3, IEX_MLW.3 and IEX_MLW.4. This indicator give landmarks regarding what may be deemed excessive, i.e. with an assumption which is above one week.
Base events
Detection of incidents of such types and with late discovery (8 months after they occur) **Frequency:** Extremely high frequency **Severity:** 4 **Detection means:** Semi-automatic production (with advanced monitoring tools and methods to detect concerned incidents and to investigate them) **Detection level:** 1 (detection rate can be up to 20 %)
Indicator production
Base measure: Date of the incident detection **Derived measure 1:** Number of such incidents detected during the last 30 days **Derived measure 2:** Ratio of Number of such incidents late detected during the last 30 days to Number of stealthy security incidents detected **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 90 % (high scattering level according to companies or organizations, depending on their maturity level)
Link with ISO/IEC 27002 [2]
A10 and A13 control areas
Maturity KPSI
6

Family VOR_VNP: Not patched vulnerabilities

VOR_VNP.1: Excessive time of window of risk exposure
This indicator measures situations in which the time of the window of risk exposure exceeds the time limit expressed in security policy. The window of risks exposure is the period of time between the public disclosure of a software vulnerability and the actual and checked application of a patch that corresponds with the vulnerability's remediation (independently of the time needed for the vendor to provide the patch). This indicator only applies to workstations (OS, application software and browsers), and to critical vulnerabilities (as publicly determined via the CVSS scale) that require an action as quickly as possible.
Base events
Detection of a case where the time of the window of risk exposure exceeds the time limit expressed in security policy **Frequency:** Potentially serious and rather frequent **Severity:** 3 or 4 **Detection means:** Semi-automatic production possible (if computerized patch management process) **Detection level:** 2 (detection rate possibly attaining 60 %, if formalized patch management process)
Indicator production
Base measure: Date of the event, time of the window of risk exposure **Derived measure 1:** Excessive time of the window of risk exposure for critical vulnerabilities that should be patched **Derived measure 2:** idem Derived Measure 1 **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 3,5 days on average (high scattering level according to companies or organizations, largely depending on the patch management process maturity level)
Link with ISO/IEC 27002 [2]
A12 control area
Maturity KPSI
3

VOR_VNP.2: Rate of not patched systems
This indicator measures the rate of not patched systems for detected critical software vulnerabilities (see VOR_VNP.1 for criticality definition). Not patched systems to be taken into account are the ones which are not patched beyond the time limit defined in security policy. This indicator only applies to workstations (OS, application software and browsers).
Base events
Detection of systems that are not patched beyond the time limit defined in security policy **Frequency:** Corresponding with a rather significant rate as regards causes of security incidents in an Information System (25 % on average in the profession) **Severity:** 2, if rate above 15 % **Detection means:** Manual production **Detection level:** 3 (detection rate can be up to 100 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of systems to be patched **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 10 % (high scattering level according to companies or organizations, largely depending on the patch management process maturity level)
Link with ISO/IEC 27002 [2]
A12 control area
Maturity KPSI
3

Family VOR_VNR: Not reconfigured systems

VOR_VNR.1: Rate of not reconfigured systems
This indicator measures the rate of not reconfigured systems for detected critical configuration vulnerabilities. Configuration vulnerabilities are either non-conformities relative to a level 3 security policy, or discrepancies relative to a state-of-the-art available within the profession (and that can correspond with a configuration master produced by a vendor and applied within the organization). This indicator only applies to workstations (OS, application software and browsers). Not reconfigured systems to be taken into account are the ones which are not reconfigured beyond the time limit defined in security policy.
Base events
Detection of not reconfigured systems for detected critical configuration vulnerabilities **Frequency:** Corresponding with a significant rate as regards causes of security incidents in an Information System (30 % on average in the profession) **Severity:** 2, if rate above 20 % **Detection means:** Semi-automatic production possible (if automated configuration and change management processes) **Detection level:** 3 (detection rate can be up to 90 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of systems to be reconfigured **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 35 % (low scattering level according to companies or organizations, with better score related to change and configuration management processes maturity level)
Link with ISO/IEC 27002 [2]
A12 control area
Maturity KPSI
2

Family VOR_RCT: Reaction plans

VOR_RCT.1: Reaction plans launched without experience feedback
This indicator applies to plans for responding to incidents formalized in security policy launched without experience feedback.
Base events
Detection of a reaction plan launched without experience feedback **Frequency:** Significant frequency **Severity:** 2 **Detection means:** Manual production **Detection level:** 3 (detection rate can be up to 100 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of launched reaction plan **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 30 % (high scattering level according to companies or organizations, depending on their maturity level)
Link with ISO/IEC 27002 [2]
A13 control area
Maturity KPSI
6, 7

VOR_RCT.2: Reaction plans unsuccessfully launched
This indicator measures failure in the performance of plans, leading to non-recovery of incidents and to subsequent possible launch of an escalation procedure.
Base events
Detection of an unsuccessfully launched reaction plan **Frequency:** Significant frequency **Severity:** 4 **Detection means:** Manual production **Detection level:** 3 (detection rate can be up to 80 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of launched reaction plan **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 15 % (high scattering level according to companies or organizations, depending on their maturity level)
Link with ISO/IEC 27002 [2]
A13 control area
Maturity KPSI
6, 7

Family VOR_PRT: Security in IT projects

VOR_PRT.1: Launch of new IT projects without information classification
This indicator measures the launch of new IT projects without information classification. Availability of a classification model and scheme within the organization would make easier this task.
Base events
Detection of launch of new IT projects without information classification **Frequency:** Frequent in all organizations **Severity:** 3 **Detection means:** Manual production **Detection level:** 3 (detection rate can be up to 100 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of launched projects **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 40 % (low scattering level according to companies or organizations, with lower rate related to ISO/IEC 27001 [6] certification or compliance with strong regulations)
Link with ISO/IEC 27002 [2]
A7 control area
Maturity KPSI
6

VOR_PRT.2: Launch of new specific IT projects without risk analysis
This indicator measures the launch of new specific IT projects without performing a full risk analysis.
Base events
Detection of launch of new specific IT projects without risk analysis **Frequency:** Frequent in some business sectors with low regulatory constraints **Severity:** 3 **Detection means:** Manual production **Detection level:** 3 (detection rate can be up to 100 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of launched projects **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 40 % (high scattering level according to companies or organizations, depending on the greater or lesser regulatory constraints weighing on them)
Link with ISO/IEC 27002 [2]
None
Maturity KPSI
6

VOR_PRT.3: Launch of new IT projects of a standard type without identification of vulnerabilities and threats
This indicator measures the launch of new IT projects of a standard type without identification of vulnerabilities and threats and of related security measures. For these IT projects, potential implementation of a simplified risk analysis method or of pre-defined security profiles can be applied.
Base events
Detection of launch of new IT projects without security policy **Frequency:** Frequent in some business sectors with low regulatory constraints **Severity:** 3 **Detection means:** Manual production **Detection level:** 2 (detection rate possibly attaining 60 % - Cf. difficulties identifying all new "typical" projects)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Ratio of Number of events detected during the last 30 days to Number of launched projects **Indicator value:** Ratio of Derived Measure 2 to Average per month for the last 90 days **State-of-the-art value:** (Derived measure 2) 50 % (high scattering level according to companies or organizations, depending on the greater or lesser regulatory constraints weighing on them)
Link with ISO/IEC 27002 [2]
None
Maturity KPSI
6

5.6 Indicators as regards impact measurement

The recommended operational indicators are the following (4 in all):

IMP_COS.1: Average cost to tackle a critical security incident
The average cost taken into account includes the following kinds of overhead: disruption to business operations (increased operating costs, etc.), fraud (money, etc.) and incident recovery costs (technical individual time, asset replacement, etc.). It does not include possible (generally very heavy) breach notification costs to customers and enforcement bodies (according to US and recently EU laws or regulations). **Rationale:** may be a powerful tool for CISOs and CIOs to make trade-offs between IT security equipment investments and risk treatment
Base events
Critical security incident that has been detected and tackled
Indicator production
Base measure: cost for each critical security incident detected and addressed by an appropriate response **Derived measure 1:** cost of all incidents of this kind during the last 30 days **Derived measure 2:** average cost of an incident of this kind during the last 30 days **Indicator value:** ratio of Derived Measure 2 to average cost of incidents of this kind for the last 120 days
State-of-the-art figure (and scattering)
State-of-the-art value: (Derived measure 2) 150 k€ (significant scattering level according to companies or organizations, depending on the kinds of security incidents most often tackled - see for example the cost expensive so-called APTs, and on the greater or lesser degree of maturity as regards security incident response)
Maturity KSPI
None

IMP_TIM.1: Average time of Websites downtime due to whole security incidents
Applies to all 4 classes, but main security incidents concerned are malfunctions or breakdowns (software or hardware), DoS or DDoS attacks and Website defacements **Rationale:** among all applications, Internet-facing applications are those with potential broadest impact (especially companies or organizations addressing general public)
Base events
Detection of security incidents causing unavailability of a Website
Indicator production
Base measure: time for recovering each security incident causing unavailability of a Website **Derived measure 1:** total time for all incidents of this kind during the last 30 days **Derived measure 2:** average time of an incident of this kind during the last 30 days **Indicator value:** ratio of Derived Measure 2 to average time for the last 90 days
State-of-the-art figure (and scattering)
State-of-the-art value: (Derived measure 2) 24 hours (significant scattering level according to companies or organizations, depending on the kinds of security incidents most often tackled - see for example the difficult and long to recover DDoS attacks, and depending on the greater or lesser degree of maturity as regards security incident response)
Maturity KSPI
None

IMP_TIM.2: Average time of Websites downtime due to successful malicious attacks
This indicator is a subset of the previous one (IMP_TIM.1) focusing on 3 possible classes (IEX, IUS, IMD) **Rationale:** idem above
Base events
Idem above
Indicator production
Base measure: idem above **Derived measure 1:** idem above **Derived measure 2:** idem above **Indicator value:** idem above
State-of-the-art figure (and scattering)
State-of-the-art value: (Derived measure 2) 36 hours (idem above)
Maturity KSPI
None

IMP_TIM.3: Average time of Websites downtime due to malfunctions or unintentional security incidents
This indicator is a subset of IMP_TIM.1 focusing on one class (IMF) **Rationale:** idem above
Base events
Idem above
Indicator production
Base measure: idem above **Derived measure 1:** idem above **Derived measure 2:** idem above **Indicator value:** idem above
State-of-the-art figure (and scattering)
State-of-the-art value: (Derived measure 2) 5 hours (significant scattering level according to companies or organizations depending on the greater or lesser degree of maturity as regards security incident response)
Maturity KSPI
None

5.7 Recap of available state-of-the-art figures

The state-of-the-art figures indicated below correspond to an organization with 100 000 workstations, with possible clarifications on the reference base (site, server or equipment, etc.). These state-of-the-art figures are from all around the world (mainly North America and Europe) and stemming from Club R2GS figures. They should be used with caution, since they are a snapshot at a given time and they are here only to illustrate the benchmarking approach feasibility.

Capture of the table columns:

- *Categories: Incidents* (IEX, IMF, IDB, IWH), *Vulnerabilities* (VBH, WSW, VCF, VTC, VOR), *Impact* (IMP)
- *Reference base* (Standard - if applicable to overall organization with 100 000 workstations with useless supplementary clarifications, specific reference base - if further clarifications needed)
- *State-of-the-art statistical figures or values* (N/A - not applicable, N/U - definition not uniform according to organizations, number of occurrences of events per month or number of users at fault or number of items or rate as a % per month - if applicable)
- *State-of-the-art figures that converge strongly and have a low scattering of sample data and have therefore high reliability level (R)* (**X** or no)
- *Priority 1 measurement that becomes some kind of Core Measurements* (**P** or no)
- *Main recipient, i.e. generally and first of all CSO or CISO* **(CSO),** *but also sometimes Operational Risk Managers, CIOs and Senior Executive Management* **(MAN)**

Indicator	Designation	Reference base	State-of-the-art	R	P 1 M	Recipient	Comments
IEX_FGY.1	Forg. dom/brand names	Standard	N/A			CSO	
IEX_FGY.2	Forged Websites	Standard	N/A			CSO	Link with IEX_FGY.1
IEX_SPM.1	Spam	Standard	0,2 %	**X**	**P**	CSO	Internal business mess. system
IEX_PHI.1	Phishing targeting customers	Standard	20 camp.			CSO	Campaigns in English language (different elsewhere)
IEX_PHI.2	Spear phishing attacks	Standard	N/A			CSO	
IEX_INT.1	Tech. intrusion attempts	By Website	400	**X**	**P**	CSO	
IEX_INT.2	Intrusions on externally accessible Websites	By Website	0,7		**P**	CSO	Link with IEX_DFC.1 and IEX_MIS.1
IEX_INT.3	Intrusions on internal servers	By server	0,05			CSO	
IEX_DFC.1	Defacement of Websites	By Website	0,2			CSO	With secure Web devts
IEX_MIS.1	Online res misappropr.	Standard	2	**X**		CSO	With secure Web devts
IEX_DOS.1	Dos and DDoS attacks	By Website	0,006 (DDoS)			CSO	High scattering
IEX_MLW.1	Attempt inst mal on WS	Standard	1,600	**X**	**P**	CSO	
IEX_MLW.2	Attempt inst mal on serv	By 10 000 servers	110	**X**	**P**	CSO	
IEX_MLW.3	Malware install. on WS	Standard	40		**P**	CSO	High scattering
IEX_MLW.4	Malware install. on servers	By 10 000 intern. serv.	0,5		**P**	CSO	WS prevailing over server
IEX_PHY.1	Physical intrusions/actions	Standard	50		**P**	CSO	
IMF_BRE.1	PC breakdowns/malf	Standard	N/U		**P**	CSO	Pb of variable definitions
IMF_BRE.2	Server breakdowns/malf	Standard	N/U		**P**	CSO	Pb of variable definitions
IMF_BRE.3	Mainframe break/malf	Standard	N/U		**P**	CSO	Pb of variable definitions
IMF_BRE.4	Network break/malf	Standard	N/U		**P**	CSO	Pb of variable definitions

Indicator	Designation	Reference base	State-of-the-art	R	P 1 M	Recipient	Comments
IMF_MDL.1	Misdelivery of content	Standard	0,2 %	X		CSO	
IMF_LOM.1	Mobile dev. loss/theft	Standard	0,08 %	X	P	CSO	For laptop computers
IMF_LOG.1	Malf. of log prod funct	Standard	N/U		P	CSO	Pb of variable definitions
IMF_LOG.2	Abs. of person logging	Standard	10 %	X		CSO	
IMF_LOG.3	Malf. of EV recordings	Standard	N/U			CSO	Pb of variable definitions
IDB_UID.1	Identity usurpation	Standard	20	X		CSO	Network of 50K VPN accesses
IDB_RGH.1	Ext. rights by vul exploit	Standard	20	X	P	CSO	Network of 50K part. users
IDB_RGH.2	Ext. rights by soc. engin.	Standard	2	X		CSO	
IDB_RGH.3	Illicit use of admin rights	Standard	13 users	X		CSO	
IDB_RGH.4	Time limit. rights still used afterwards	Standard	2	X		CSO	
IDB_RGH.5	Abuse of privileges by admin	Standard	6 users	X	P	CSO	
IDB_RGH.6	Abuse of privileges by operator or plain user	By applic	2	X		CSO	
IDB_RGH.7	Illicit use of rights after departure	Standard	N/A		P	CSO	Depends on IAM or not
IDB_MIS.1	Misapprop. IT resources	Standard	2 users	X		CSO	
IDB_IAC.1	Access to hacking sites	Standard	100	X		CSO	
IDB_LOG.1	Disab. of logs by adm	By 100 servers	1 admin	X	P	CSO	
IWH_VNP.1	Inc. due to vul no patch	Standard	10 %	X		CSO/MAN	Link with VOR_VNP.1
IWH_VNP.2	Inc. due vul not patched	Standard	15 %	X	P	CSO/MAN	Link with VOR_VNP.2
IWH_VNP.3	Inc. due vul poorly patched	Standard	5 %	X		CSO/MAN	Link with VOR_VNP.1
IWH_VCN.1	Inc. due to config vul	Standard	30 %			CSO/MAN	High scattering
IWH_UKN.1	Unknown incidents	Standard	4 %			CSO/MAN	Appreciable scattering
IWH_UNA.1	Inc. on not invent. assets	Standard	40 %		P	CSO/MAN	Appreciable scattering
VBH_PRC.1	Access in admin mode with unsecured protocol	By admin	2			CSO	
VBH_PRC.2	Use of a P2P service	Standard	30 users	X		CSO	
VBH_PRC.3	Use of a VoIP service	Standard	20 users			CSO	
VBH_PRC.4	Outbound connect. for remote acc without VPN	Standard	40 users		P	CSO	
VBH_PRC.5	Remote/loc. connection with not compliant WS	Standard	1 %			CSO	With 10K VPN access
VBH_PRC.6	Other similar behaviours	Standard	100			CSO	
VBH_IAC.1	I-net access with bypass	Standard	50 users			CSO	
VBH_IAC.2	I-net access (anony site)	Standard	200	X		CSO	

Indicator	Designation	Reference base	State-of-the-art	R	P1M	Recipient	Comments
VBH_FTR.1	Dang. download to WS	Standard	350			CSO	
VBH_FTR.2	Use public IM(file exch)	Standard	300 users	X		CSO	
VBH_FTR.3	Use pers. messaging for business files exchange	Standard	400 users	X		CSO	
VBH_WTI.1	WS in adm not compliant	Standard	75 users		P	CSO	One of the most basic vulnerabilities
VBH_WTI.2	Use of pers. storage devices on profes. WS	Standard	350	X		CSO	
VBH_WTI.3	Lack of compartmentization on pers. devices	Standard	50 %			CSO	
VBH_WTI.4	Not encrypted sensitive files on mobile devices	Standard	30			CSO	
VBH_WTI.5	Pres of personal SW	Standard	65 users	X		CSO	
VBH_WTI.6	Email/Inet access in admin mode	Standard	15 users			CSO	
VBH_PSW.1	Psw not compliant	Standard	20 %			CSO	
VBH_PSW.2	Psw not changed (user)	Standard	25 %			CSO	Users at fault
VBH_PSW.3	Psw not changed (adm)	Standard	20 %	X		CSO	App SW & auto processing
VBH_RGH.1	NC rights grant by adm	Standard	0,8 %	X		CSO	Difficult to decrease
VBH_HUW.1	Hum. weak. exploit. by spear phishing	Standard	10 %	X		CSO	
VBH_HUW.1	Hum. weak. exploit. by exchanges	Standard	N/A			CSO	
VSW_WSR.1	SW vul in I-net applic.	By Web app	80		P	CSO	
VSW_OSW.1	SW vul in I-net serv. OS	By OS	1			CSO	
VSW_WBR.1	SW vul in WS based Web browsers	By browser	1			CSO	
VCF_DIS.1	Pres of dang syst serv	By server	1 %			CSO	High scattering
VCF_LOG.1	Insuf. space for record.	Standard	4 %			CSO	Relatively high scattering
VCF_FWR.1	Weak FW rules	By FW	12			CSO	Without checking tools
VCF_WTI.1	Lack of AV/FW in a WS	Standard	10 %		P	CSO	Very high scattering
VCF_WTI.2	Autorun enabled on WS	Standard	10 %			CSO	Without strict sourcing
VCF_UAC.1	Not compliant user rights	Standard	60		P	CSO	Depends on IAM + or - completed
VCF_UAC.2	Log acc rights not compl	By server	1	X		CSO	
VCF_UAC.3	Unnecessary generic admin/serv accts	By syst/app/ database	4	X	P	CSO	Difficult to decrease
VCF_UAC.4	Accounts without owners not deleted	By syst/app/ database	10	X		CSO	Difficult to decrease
VCF_UAC.5	Inactive accounts not disabled	By syst/app/ database	11	X		CSO	Difficult to decrease

Indicator	Designation	Reference base	State-of-the-art	R	P 1 M	Recipient	Comments
VTC_BKP.1	Back-up malfunction	By sensitive server	20 %		p	CSO	
VTC_IDS.1	IDS/IPS malfunction	By IDS/IPS	0,01		P	CSO	
VTC_WFI.1	Wi-Fi devices not official	Standard	N/A		P	CSO	
VTC_RAP.1	Remote access points used for unauth access	Standard	N/A	X	P	CSO	
VTC_NRG.1	Equipt connection without being registered	Standard	3 %	X	P	CSO	
VTC_PHY.1	Not op. phys. acc. cont.	By protect-ted area	3	X		CSO	
VOR_DSC.1	Incidents with excessive time to discovery	By all stealthy incidents	90%			CSO	
VOR_VNP.1	Time of window of risks expo	Standard	3,5 days			CSO/MAN	
VOR_VNP.2	Rate of not patched system	By system concerned	10 %		P	CSO/MAN	
VOR_VNR.1	Rate of not reconfigured system	By system concerned	35 %		P	CSO/MAN	Inefficient without change & configuration mgmt
VOR_RCT.1	Rate of plans without lessons learned	By plan launched	30 %			CSO/MAN	Very dependent on maturity level
VOR_RCT.2	Rate of unsuccessful plans	By plan launched	15 %			CSO/MAN	Very dependent on maturity level
VOR_PRT.1	Proj. launched without classification	By project	40 %	X	P	CSO/MAN	European state-of-the-art
VOR_PRT.2	Proj. launched without risk analysis	By project	40 %		P	CSO/MAN	European state-of-the-art
VOR_PRT.3	Proj launch without vul & threats identification	By project.	50 %		P	CSO/MAN	European state-of-the-art
IMP_COS.1	Average cost to tackle critical security incident	By incident	150 k€			CSO/MAN	
IMP_TIM.1	Average time of Websites downtime (whole sec inc)	By incident	24 hours			CSO/MAN	
IMP_TIM.2	Average time of Websites downtime (malice)	By incident	36 hours			CSO/MAN	
IMP_TIM.3	Average time of Websites downtime (malfunction)	By incident	5 hours			CSO/MAN	

Annex A (normative): Description of the proposed indicators with reference to the template recommended in ISO/IEC 27004 standard

Topics of the ISO/IEC 27004 [1] Template		ETSI Indicator Items
Measurement Construct Identification		
Measurement Construct Name	Measurement Name	Item 1
Numerical Identifier	Unique organization-specific numerical identifier	Item 1
Purpose of Measurement Construct	Describes the reasons for introducing the measurement	Item 3
Control/process Objective	Control objective under measurement (planned or implemented)	Item 8 (one of the 11 controls)
Control (1)	Control/process under measurement	No
Control (2) …	Optional: further controls within the grouping included in the same measure, if applicable	No
Object of Measurement and Attributes		
Object of Measurement	Object (entity) that is characterized through the measurement of its attributes. An object may include processes, plans, projects, resources, and systems or system components.	Item 2 + Item 7 + Item 10
Attribute	Property or characteristic of an object of measurement that can be distinguished quantitatively or qualitatively by human or automated means.	Item 2 + Item 5
Base Measure Specification (for each base measure [1…n])		
Base measure	A base measure is defined in terms of an attribute and the specified measurement method for quantifying it (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.	Item 7
Measurement Method	Logical sequence of operations used in quantifying an attribute with respect to a specified scale.	Item 5 (production method)
Type of Measurement Method	Depending on the nature of the operations used to quantify an attribute, two types of method may be distinguished: - Subjective - quantification involving human judgment - Objective - quantification based on numerical rules such as counting	Item 6 (objectivity level)
Scale	Ordered set of values or categories to which the base measure's attribute is mapped	Item 7
Type of Scale	Depending on the nature of the relationship between values on the scale, 4 types of scale are commonly defined: Nominal, Ordinal, Interval, and Ratio	Item 8 ("ordinal" for most of the indicators, unless indicated otherwise)
Unit of Measurement	Particular quantity, defined and adopted by convention, with which any other quantity of the same kind can be compared to express the ratio of the 2 quantities as a number	Item 7 (Indicator value)
Derived Measure Specification		
Derived Measure	A measure that is derived as a function of two or more base measures	Item 7
Measurement Function	Algorithm or calculation performed to combine 2 or more base measures. The scale and unit of the derived measure depend on the scales and units of the base measures from which it is composed of as well as how they are combined by the function.	Item 7

Topics of the ISO/IEC 27004 [1] Template		ETSI Indicator Items
Indicator Specification		
Indicator	Measure that provides an estimate or evaluation of specified attributes derived from an analytical model with respect to a defined information need. Indicators are the basis for analysis and decision making.	Item 7
Analytical Model	Algorithm or calculation combining one or more base and/or derived measures with associated decision criteria. It is based on an understanding of, or assumptions about, the expected relationship between the base and/or the derived measure and/or their behaviour over time. An analytical model produces estimates or evaluations relevant to a defined information need.	Item 7
Decision Criteria Specification		
Decision Criteria	Thresholds, targets, or patterns used to determine the need for action or further investigation, or to describe the level of confidence in a given result. Decision Criteria help to interpret the results of measurement.	Item 8 (to be completed with the accepted variation against the state-of-the-art figure)
Measurement Results		
Indicator Interpretation	A description of how the sample indicator (see sample figure in indicator description) should be interpreted.	No
Reporting Formats	Reporting formats should be identified and documented. Describe the observations that the organization or owner of the information may want on record. Reporting formats will visually depict the measures and provide a verbal explanation of the indicators. Reporting formats should be customized to the information customer.	No (but representation with monthly bar graphs desirable)
Stakeholders		
Client for measurement	Person or organizational unit requesting and requiring the measurement in support of their business functions.	No (see clause 5.7)
Reviewer for measurement	Person or organizational unit that reviews and validates that the decision criteria are appropriate for measuring the effectiveness of controls and ISMS processes.	N/A
Information Owner	Person or organizational unit that owns the information about an object of measurement and attributes used to create base measures and is responsible for the measurement.	N/A
Information Collector	The person or organizational unit responsible for collecting, recording, and storing the data.	Security Operations Centre or local administrators
Information Communicator	The person or organizational unit responsible for analyzing data and reporting the results.	IT security correspondents
Frequency		
Frequency of Data Collection	How often data is collected.	Item 7 (monthly)
Frequency of Data Analysis	How often data is analyzed.	No
Frequency of Reporting Measurement Results	How often measurement results are reported (this may be less frequent than it is collected).	N/A
Measurement Revision	Date of measurement revision (expiry or renovation of measurement validity).	N/A
Period of Measurement	Defines the period being measured.	N/A

Annex B (informative): Authors & contributors

The following people have contributed to the present document:

Rapporteur:
Gerard Gaudin, G²C, Chairman of ISG ISI

Other contributors:
Herve Debar, Institut Telecom, Vice-Chairman of ISG ISI

Frederic Martinez, Alcatel-Lucent (Bell Labs), Secretary of ISG ISI

And in alphabetical order:

Christophe Blad, Oppida

Philippe Bramaud, CEIS

Eric Caprioli, Caprioli & Associés

Erwan Chevalier, BNP Paribas

Paolo De Lutiis, Telecom Italia

Jean-François Duchas, Bouygues Telecom

Gene Golovinski, Qualys Inc.

François Gratiolet, Qualys Inc.

Philippe Jouvellier, Cassidian (an EADS company)

Stéphane Lu, BNP Paribas

Stéphane Lemée, Cassidian (an EADS company)

Jean-Michel Perrin, Groupe La Poste

Axel Rennoch, Fraunhofer Fokus

Annex C (informative): Bibliography

Club R2GS 4-page data sheet V3 (2012): "Presentation of the work in progress".

NOTE: Available on ETSI ISG ISI portal.

Club R2GS presentation V4 (March 2012): "The Club and its objectives".

NOTE: Available on ETSI ISG ISI portal.

Club R2GS reference framework V1.3 (May 2011): "A set of operational security indicators that organizations can use to benchmark themselves".

NOTE: Available on ETSI ISG ISI portal.

History

Document history		
V1.1.1	April 2013	Publication
V1.1.2	June 2015	Publication