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

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

Disclaimer

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

Reference
RGS/ISI-001-2ed2

Keywords
ICT, security

ETSI

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

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

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

Contents

List of figures

Intellectual Property Rights

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

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

Foreword

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

The present document is part 2 of a multi-part deliverable covering the Information Security Indicators (ISI); Indicators (INC), as identified below:

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

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

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

- The present document addressing (together with its base list of indicators described in ETSI GS ISI 001-1 [5]) information security indicators, which are meant to measure application and effectiveness of preventative measures.
- ETSI GS ISI 002 [9] addressing the underlying event classification model and the associated taxonomy.
- ETSI GS ISI 003 [i.12] addressing the key issue of assessing organization's maturity level regarding overall event detection (technology/process/ people) and to weigh event detection results.
- ETSI GS ISI 004 [i.13] addressing demonstration through examples how to produce indicators and how to detect the related events with various means and methods (with a classification of the main categories of use cases/symptoms).
- ETSI GS ISI 005 [i.14] addressing ways to produce security events and to test the effectiveness of existing detection means within organization (for major types of events), which is a more detailed and a more case by case approach than the ETSI GS ISI 003 [i.12] and which can therefore complement it.

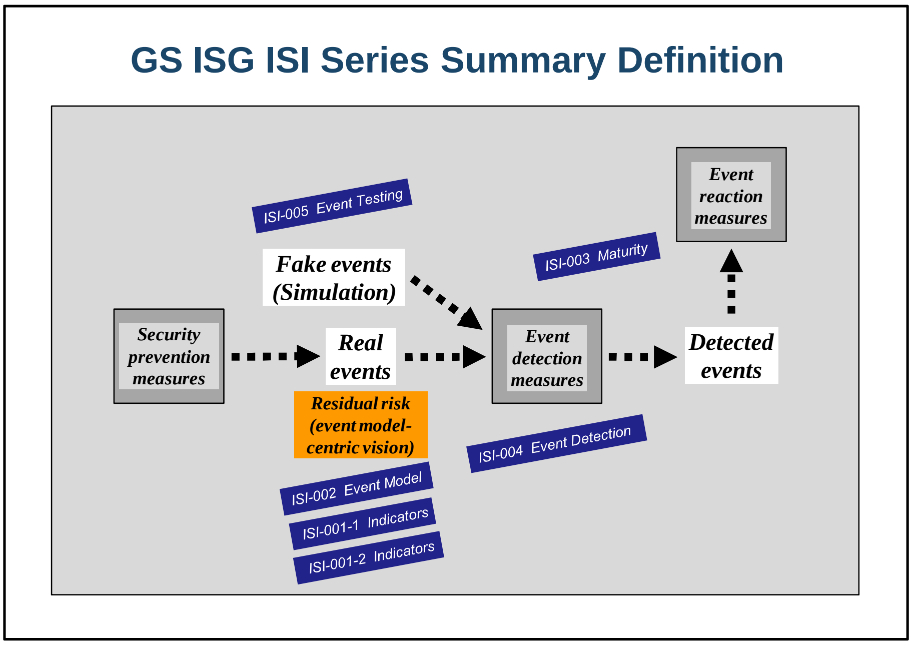


Figure 1: Positioning the 6 GS ISI against the 3 main security measures

Modal verbs terminology

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

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

Introduction

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

As regards organization's existing ISMS which constitutes the prime security governance tool, the ETSI GS ISI 001-1 [5] proposed range of indicators should be considered as a simple but representative ground work, from which to make a selection while completely **relying on the existing ISMS**. Proceeding in this manner will lead to a series of unique indicators that are specific to each organization, amongst which a first part will typically consist of specific indicators, while a second part consists of a sub-set of the list given in ETSI GS ISI 001-1 [5]. The main characteristic of the former will be "effective ISMS implementation", while that of the latter will be more "operational". As such, the structuring side of the ISMS will clarify and validate the choice of a given indicator from the proposed ground work. For that purpose, various reference frameworks and contexts should be addressed, such as ISO/IEC 27002 [1] (first of all) and the Consensus Audit Guidelines [4] (sub-set of Priority One NIST SP 800-53 [i.9] controls), but also the more extended frameworks COBIT [3] and ISO/IEC 20000 (ITIL) [i.1] and [i.2].

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

1 Scope

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

2 References

2.1 Normative references

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.2 Informative references

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3 Definitions and abbreviations

3.1 Definitions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

NOTE: This risk breaks down into 3 shares:

- Known and suffered risk, corresponding with the one with which the organization is confronted when security policy is not applied (configuration, behavioural or global security non-conformities), and when known and critical software vulnerabilities are not appropriately addressed.

- Known and accepted risk that corresponds with the one accepted once a choice has been made and backed up by economic, usage and security level considerations.

- Unknown risk corresponding with the one associated with various not updated vulnerabilities or innovative types of attacks.

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

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

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

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

- *Dangerousness* is resulting from several objects with variable combinations according to circumstances or types of incidents: execution or spreading speed, virulence, effectiveness, scope and number of impacted assets, capability of harm and of target reach, capability of remotely acting, persistence, weakness or lack of curative means, and last depth which is can be or has been reached (concept of Defence in Depth or DiD).

- *Stealthiness* has several levels: obvious visibility, discretion but can be seen by basic means, detection by advanced technical tools, almost invisibility. It is a key factor within the framework of monitoring and detection concerns. Anonymization and camouflage active and passive means are stealthiness means. Stealthiness takes on an indirect meaning insofar it applies to similar not yet detected incidents.

- *Feasibility* is in relation to the attacker's motivation and in inverse ratio to the sum of the necessary means (regarding skills, tools, financial means, collusion, initial access, etc.) combined with the presence of exploitable vulnerabilities; feasibility can be tied often to the frequency of attacks that can be detected in the world. Its assessment is not simple, because it is subject to evolution: actually, if a hacking tool is difficult to be created, once it is available on Internet, it can be used by not seasoned criminals. Feasibility takes on an indirect meaning insofar it first applies to potential threat (see definition of this term), but it gives good clues on several amongst its components, including criminals' actual capability.

This notion appeared in the mid-1990s within the framework of the ITSEC certification, then towards the end of this decade with the issue of global and public management of vulnerabilities and "malware" (security software vendors and CERTs). It is once again being developed at the present time with the recent distribution of log analysis and correlation tools that completely integrate this concept along with criticality.

severity level (of vulnerability or of nonconformity): severity level definition is about the same as incidents' one with a few slight differences

NOTE: These differences are the following:

- *Dangerousness*: depth of tied attacks, weakness of treatment means, possible remote exploitation, scope of the park concerned, importance to organization of the security rule that was violated.
- *Stealthiness*: same definition as for incident.
- *Exploitability* (by attackers), which is the opposite standpoint of incident feasibility.

The definition proposed is homogeneous with the CVSS (NIST 800-126 [i.16]) standard one for software vulnerabilities.

security policy: overall intention and direction as formally expressed by security management. 2 levels are used: general statement, detailed rules

NOTE: Rules concern network and systems configuration, user interaction with systems and applications, and detailed processes and organization (governance, operational teams, audit). Violation of a rule brings about a nonconformity, which is either an incident or a vulnerability.

sensitivity level: level which corresponds to the potential impact (financial, legal or concerning brand image) of a security event on an asset, an impact linked to the estimated value of the asset for the company regarding its 4 possible aspects: its Confidentiality, Integrity and Availability (CIA) and sometimes its accountability

Security Information and Event Management (SIEM): combination of the formerly disparate product categories of SIM (security information management) and SEM (security event management)

NOTE: SEM deals with real-time monitoring, correlation of events, notifications and console views. SIM provides long-term storage, analysis and reporting of log data. As an extension, it is talked about SIEM approaches, which encompass all organizations, process and human aspects necessary to go along tools, and which include vulnerability and nonconformity management; it is referred to Cyber Defense approaches in this case.

taxonomy: science of identifying and naming species, and arranging them into a classification

NOTE: The field of taxonomy, sometimes referred to as "biological taxonomy", revolves around the description and use of taxonomic units, known as taxa (singular taxon). A resulting taxonomy is a particular classification ("the taxonomy of ..."), arranged in a hierarchical structure or classification scheme.

threat: potential cause of an unwanted incident, which may result in harm to a system or organization

NOTE: There are 4 categories of threats:

- Natural threats:
  - Environmental causes: public service outage, fire, and other disasters,
  - System failure: physical or software computer or network breakdowns,
- Human threats:
  - Unwitting or unintentional (error, carelessness, irresponsibility, unawareness, etc.): conception and design, development, operation and usage, due to chance, to haste, tiredness, credulity, incompetency,
  - Internal or external malice: theft, economic spying, sabotage, intrusion, fraud, etc.

The frontier between error, carelessness and malice is often fuzzy: it is always possible for an unscrupulous employee to plead error even though he has been negligent or malicious. However the difference between unintentional and malicious actions can often be found with the following clues:

- An unintentional action is little stealthy, with impact rather on availability, low dangerousness and high feasibility. The resulting severity is often low to fairly low.
- A malicious action is stealthier (notably to make attacker's anonymity possible and provide him with a long course of action), with impact rather on confidentiality and integrity and with high dangerousness.

trace: computer data that proves the existence of a business operation

NOTE: As an example, logs (see definition above) are traces, but all traces are not logs.

vulnerability: not desirable state of a system whose occurrence or detection is a security event

NOTE: It corresponds with a flaw or weakness of an asset or group of assets (at the level of a technical system, process or behaviour) that can be exploited by a threat. Occurrence and actual detection of a vulnerability (often delayed in time) are considered the same in the present document. There are 6 types of vulnerabilities (only the first 4 ones being in the scope of a SIEM approach and being dealt with in the present GS):

- Behavioural.
- Software (that can lead to malicious exploitation by an attacker via an "exploit").
- Security equipment or software configuration (same as above).
- General security technical or organizational (vulnerabilities defined as having an overall and powerful effect on Information System's security level, and having a level equivalent to the ISO/IEC 27002 [1] standard reference points).
- Conception (overall system design at architecture and processes levels).
- Material level (corresponding with vulnerabilities which make it possible physical incidents - of an accidental, negligent or malicious kind).

A behavioural, configuration, global security (technical and organizational) or material vulnerability becomes a nonconformity (see definition above) when it violates the organization's security policy and rules. It is talked about a usage or implementation drift in this case.

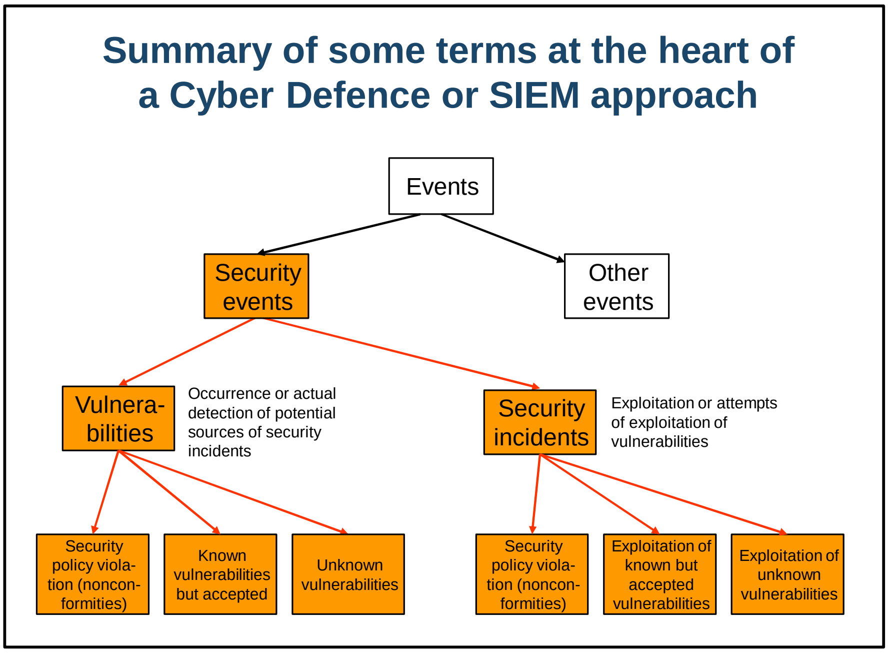

Summary of some terms at the heart of
a Cyber Defence or SIEM approach
Events
Security events
Other events
Vulnera-bilities
Occurrence or actual detection of potential sources of security incidents
Security incidents
Exploitation or attempts of exploitation of vulnerabilities
Security policy viola-tion (noncon-formities)
Known vulnerabilities but accepted
Unknown vulnerabilities
Security policy viola-tion (noncon-formities)
Exploitation of known but accepted vulnerabilities
Exploitation of unknown vulnerabilities

Figure 2: Relationships between different kinds of events

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

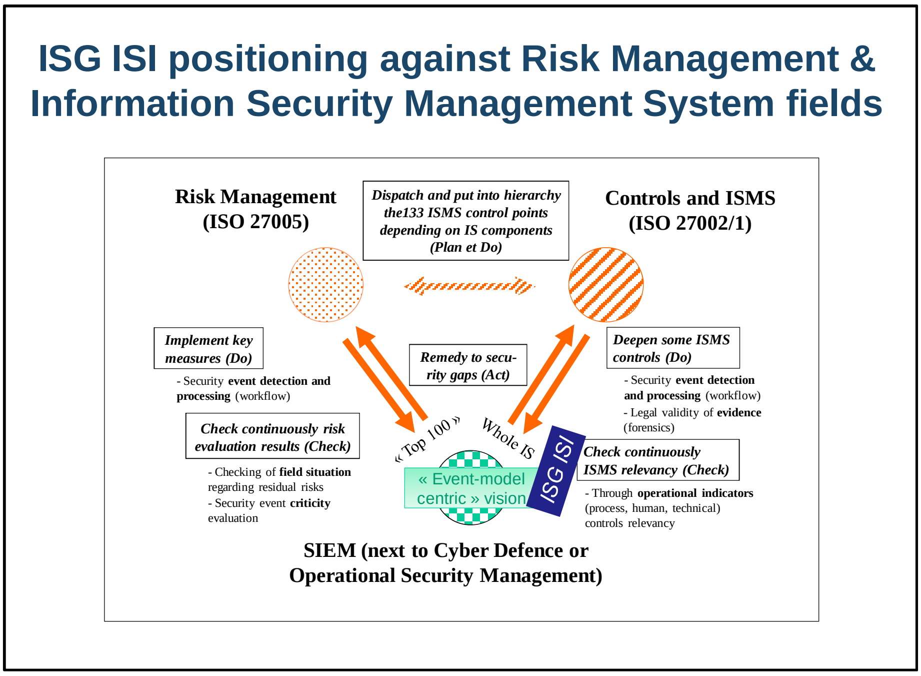
CAG	Consensus Audit Guidelines
CC	Critical Controls
CCMB	Common Criteria Management Board
CIA	Confidentiality Integrity Availability
COBIT	Control OBjectives for Information and related Technology
CVSS	Common Vulnerability Scoring System
DS	Deliver and Support
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ME	Monitor and Evaluate
NIST	National Institute of Standards and Technology (USA)
NOC	Network Operations Center
OE	Operational Environment
PDCA	Plan Do Check Act
SFR	Security Functional Requirements
SIEM	Security Information and Event Management
SOC	Security Operations Centre
SP	Special Publication
TOE	Target Of Evaluation

4 Position ETSI GS ISI 001-1 within the framework of ISO/IEC 27001 to 27008

4.0 Introduction

The first target for the ETSI ISG ISI Group Specifications is Europe, special focus is stressed on relations and links to ISO/IEC 27001 to 27008 [6], [1], [i.10], [2], [i.11], [7], [i.6] and [i.7] assurance standards as they are the most widely used in Europe, thus assigning a lesser priority to other standards such as related NIST standards.

To position the ETSI GS ISI 001-1 [5] range of indicators against ISO/IEC 27001 to 27008 [6], [1], [i.10], [2], [i.11], [7], [i.6] and [i.7] standards, it should be first of all considered their link to the 14 control categories of the ISO/IEC 27001/2 [6], [1] standards by bearing in mind the aim of a continuous assessment and checking of the application and effectiveness of an existing ISMS (see figure 3). Another standard to be especially considered is ISO/IEC 27004 [2] that primarily relates to security indicators.



ISG ISI positioning against Risk Management & Information Security Management System fields

Risk Management (ISO 27005)

Dispatch and put into hierarchy the133 ISMS control points depending on IS components (Plan et Do)

Controls and ISMS (ISO 27002/1)

Implement key measures (Do)

- Security **event detection and processing** (workflow)

Remedy to security gaps (Act)

Deepen some ISMS controls (Do)

- Security **event detection and processing** (workflow)
- Legal validity of **evidence** (forensics)

Check continuously risk evaluation results (Check)

- Checking of **field situation** regarding residual risks
- Security event **criticity** evaluation

« Top 100 »

Whole IS

« Event-model centric » vision

ISG ISI

Check continuously ISMS relevancy (Check)

- Through **operational indicators** (process, human, technical) controls relevancy

SIEM (next to Cyber Defence or Operational Security Management)

Figure 3: GS ISI positioned against Risk Management and ISMS

4.1 Link of the proposed security indicators to existing ISMS

All various types of security indicators can only claim true effectiveness when they are defined relatively to an ISMS that is widely known to every stakeholders involved. Indeed, improvements or downgrading that these indicators should make it possible to precisely and continuously measure can only be assessed against a global and consistent reference framework, which alone can ensure that no weak link (critical in IT security) will be forgotten. This essential basic principle therefore obviously applies to the indicators proposed in the present document**,** which are **more a supplement to the organization's specific indicators**, supplement that evaluates the compliance or effectiveness of the security measures or processes that are considered to be central for the organization. For the latter, this can include for example:

- quality of information classification processes or existence of notes regarding appointments to positions that contribute to the IT security chain;
- link between user awareness and observed improvement of daily practices;
- level of development and application of level 3 (most detailed ones) policies within the various units;
- frequent correlation between the malware infection rate of user workstations and the non-compliant usage of (personal or other) software prohibited by the organization.

In this environment, the operational indicators proposed here are generic reference points that are common to most organizations, that are of a more technical or more behavioural level, and that are often very refined regarding their content. They are furthermore directly associated with the current status of techniques used in information systems, of internal or external computer roguery and of the security-related user maturity.

ISO/IEC 27004 [2] which insists that indicators be worked out on the basis of ISO/IEC 27002 [1] compliant ISMS, is also used herein with templates that set out items that should be defined in order to obtain an indicator's complete definition.

4.2 The 3 notions involved in ISMS monitoring and auditing

As part of an enterprise-wide SIEM approach, the 1st objective of continuous checking is to constantly measure, using appropriate indicators, **the application and effectiveness of all security-related measures** that have been taken. Such a continuous monitoring can be positioned relative to the 3 notions that apply to an ISMS (Information Security Management System), only notions 2 and 3 being relevant in the present document:

- Its coverage level against the 133 reference points of ISO/IEC 27002 [1] or 27001 [6] standards.
- The level of confidence that can be allocated to its actual application within the organization, and that at least corresponds with the checking of the security resources implementation (technical, organizational and human), this notion being a mix of level of application (measured by non-conformities) and level of assurance (measured by the level of means used to do the checking).
- Its effectiveness level that corresponds with measuring actual results provided by the means implementation (measured by the level of decrease of the number of incidents).

The **1st notion** is a choice made by the organization (that has to be periodically reviewed) regarding the security coverage level that it considers necessary to impose upon itself because of the risks to which it is exposed (SoA or Statement of Applicability). An enterprise-wide SIEM approach may allow for the progressive improvement of this coverage level of the standard relative to some very operational aspects (for example, appointments of the stakeholders in the security chain kept up-to-date, or increasingly precise and extended classification of the "assets"). Some studies regarding the Cyber Defence and SIEM domain described the noteworthy improvements and the potential leverage effects at this level, while presenting them according to the ISO/IEC 27002/1 [1] and [6] standards 11 control areas.

The **2nd notion** corresponds with the various confidence levels that can be assigned to the application of security rules and measures that make up the ISMS. This notion defines 4 successive confidence levels (listed below by increasing confidence level), that correspond with equally increasing maturity levels:

- IT security steering committee and auditing only through periodic audits.
- Same as above + initial operational scoreboards (with vulnerabilities and/or non-conformities) within the framework of a very partial (and primarily manual) continuous checking.
- Same as above + implementation of security assurance reference frameworks (event classification model, operational indicators, strictly formalized reaction plans, forensics).
- Same as above + continuous monitoring tools that use logs and/or files in an advanced manner with implementation of elaborate analysis techniques (and focus on internal and behavioural events).

Meant to provide a reference framework for ISMS relevancy measurement, ISO/IEC 27004 [2] is intended to serve as a reference point for the concrete implementation of this 2nd notion.

The **3rd notion** reinforces the 2nd one by precisely assessing the effectiveness of the implemented security measures and means (notably preventative ones), and by providing with benchmarking against state-of-the-art figures (produced by the IT security community). Initial state-of-the-art figures as presented in the ETSI GS ISI 001-1 [5] for some 95 indicators are the ones produced by some private sources, with one of the potential objectives of upcoming professional associations being to create a similar state-of-the-art in some European countries.

ISO/IEC 27004 [2] is also intended to serve as a reference point for the concrete implementation of this 3rd notion, which is an integral part of the scope of the present document.

4.3 Link to ISO/IEC 27001 and ISO/IEC 27002 standards

Over and above the link with the existing ISMS (mentioned in clauses 4.1 and 4.2) and the targeted orientation for the continuous assessment of its relevancy, all of the proposed operational indicators can be tied in with the ISO/IEC 27001/2 [6], [1] standards 14 control categories (see annex A). This approach could make it possible to better position and present the interest value of indicators for the IT production teams that are often in charge of working them out, and to contribute to the harmonization between the top-down governance approaches originating in management, and the more technical bottom-up approaches originating in the field. Moreover, this could lead to better awareness of stakeholders involved in the IT system as regards their exact respective contributions and roles in terms of organization's IT system security level. In an environment with quick adoption of ISO/IEC 27001 to 27008 [6], [1], [i.10], [2], [i.11], [7], [i.6] and [i.7] standards, this attachment will also be both increasingly necessary and natural. Moreover, to make easier selection of indicators, ETSI GS ISI 001-1 [5], clause 5.7 (recap of available indicators and state-of-the-art figures) includes a list of 36 priority 1 indicators that can be considered as the ones for which the implementation is most essential.

It should be added that in the majority of cases, it is proposed indicators that will provide useful information about precise improvement actions to be applied (bearing in mind the Act in the PDCA cycle). The follow-up of process aspects, which is an important part of a continuous checking, is only tackled very partially in the present document, as a result of the current frequent absence of a state-of-the-art on this topic and of the probable greater disparity of situations within organizations in this regard. Moreover, security processes are often too specific to each industry sector.

4.4 Link to ISO/IEC 27004 standard

ISO/IEC 27004 [2] is clearly the one from amongst all eight ISO/IEC 27001 to 27008 standards [6], [1], [i.10], [2], [i.11], [7], [i.6] and [i.7] that is closest to the SIEM mind and concepts, and the only one in which the continuous checking reality is truly perceived. As such, the SIEM concepts "blend" particularly well with topics covered in the present document. Indeed, it highlights the following aspects:

- Continuous quantitative measurement of ISMS relevancy (effectiveness and application).
- Systematic attachment to the ISO/IEC 27001 [6] and ISO/IEC 27002 [1] standards control points.
- Positioning of measurement indicators relative to the PDCA cycle.

Indicators described in ETSI GS ISI 001-1 [5] can be positioned against the definitions and concepts introduced in the information security measurement model presented in ISO/IEC 27004 [2] (in particular "base measure", "derived measure" and "indicator" - see annex A of ETSI GS ISI 001-1 [5]).

5 Position ETSI GS ISI 001- [i.10] 1 against COBIT and ISO/IEC 20000

5.0 Introduction

IT security is part of a wider IT world with its own practices, that rest mainly on 2 very common framework: the 1st one COBIT dedicated to IT governance, and the 2nd one ISO/IEC 20000 [i.1] and [i.2](or ITIL best practice framework) dedicated to day-to-day IT operations. For this reason and because of the growing trend in using these 2 frameworks alongside ISO/IEC 27001 to 27008 [6], [1], [i.10], [2], [i.11], [7], [i.6] and [i.7] series, it is of paramount importance to position ETSI GS ISI 001-1 [5] against COBIT [3] and ISO/IEC 20000 [i.1],[i.2].

5.1 Link to COBIT

COBIT is ISACA's business framework for the governance and management of enterprise IT. This framework provides globally accepted principles, practices, analytical tools and models to help increase the trust in, and value from, information systems. And of course it addresses IT security concerns. The COBIT 4.1 version [3] is used given its widespread understanding and use.

The relevant security controls to be taken into account fall in the Deliver and Support (DS) category, namely **DS5 (Ensure Systems Security)**, which is the security part. The category Monitor and Evaluate (ME) is also concerned; however, since it deals with DS controls compliance monitoring and checking, it overlaps the comprehensive correspondence made here with ETSI GS ISI 001-1 [5] indicators, whose aim is just to monitor and evaluate. It is therefore not addressed here.

A cross-checking work has been carried out during working out of the present document, and is summarized in table B.1. This cross-checking is of particular importance given the frequent use of the COBIT framework by Government Auditors, who can therefore reinforce their trust in the company overall security compliance through the implementation of ETSI GS ISI 001-1 [5] relevant indicators and the related possible benchmarking.

5.2 Link to ISO/IEC 20000

ISO/IEC 20000 [i.1] and [i.2] (or ITIL best practice framework) is an IT service management framework, which complements governance framework such as COBIT or ISO/IEC 27002 [1]. It provides a comprehensive, consistent and coherent best practice framework for IT service management and related processes, promoting a high-quality approach for achieving business effectiveness and efficiency in IT service management. The goal is to provide IT services that are:

- Matched to business needs and user requirements.
- Effectively and efficiently sourced and delivered.

The role of the ITIL framework is to describe approaches, functions, roles and processes, upon which organizations may base their own practices, and to give guidance at the lowest level possible. It is positioned at the operational level, being used in IT day-to-day operations and in particular in NOC (Network Operations Center) and SOC (Security Operations Centre). It may be useful to think of the service management structure as a pyramid with the international standard ISO/IEC 20000 [i.1] and [i.2] at the summit. Below the summit is the layer of ITIL best practice guidance, which helps to ensure and demonstrate that the provisions of the ISO/IEC 20000 standard [i.1] and [i.2] are being met.

As regards governance frameworks, ITIL processes may be used to achieve and demonstrate compliance with them. There is therefore no special need to prove compliance with the ITIL framework and achieve a mapping with ETSI GS ISI 001-1 [5] operational indicators. External auditors rely generally only on governance frameworks, and not on such more operational frameworks which are too far from regulation or legislation layers for their purpose.

6 Different other useful cross-references

6.0 Introduction

Given the wide-spread use of some other general reference frameworks or their relevancy for the continuous assurance issue, 2 other correspondences are proposed hereafter. They could make it easier for security professionals (governance or operational personnel), which are familiar with their day-to-day environment, to get accustomed to ETSI GS ISI 001-1 [5].

6.1 Correspondence with the Consensus Audit Guidelines (CAG)

A group of US federal agencies and private organizations, including the National Security Agency and the Department of Homeland Security, has released at the beginning of 2009 a set of guidelines defining the top 20 things organizations should do to prevent cyber attacks, called The Consensus Audit Guidelines (CAG) [4]. The present document describes the 20 key actions, referred to as critical controls, which organizations should take to defend their computer systems. These 20 controls are a perfect, malice-oriented and risk-based subset of the NIST SP 800-53 [i.9] Priority One controls, that measures security effectiveness and that puts emphasis on automatic and continuous monitoring for 15 of all the controls. This initiative is gaining rapid agreement among the security community in the US and is being progressively adopted in other countries (Australia, UK, etc.).

The importance of this reference framework for ISG ISI relies on its positioning which can be summarized as being a right compromise between governance and operations for such a general framework. In this context, ETSI GS ISI 001-1 [5] brings exactly what is still lacking, i.e. a way to measure the effectiveness of all controls in a precise and quantitative manner.

A cross-checking work has been carried out during working out of the present document, and is summarized in the table in annex C.

6.2 Link to ISO/IEC 15408 standard

The Common Criteria (ISO/IEC 15408 [i.3], [i.4] and [i.5]) is a standard for the evaluation of IT products in labs. The Common Criteria standard permits to specify in a document called "Security target" both security functions and activities to be performed by an evaluator to gain assurance that these security functions are effectively implemented in the IT product under evaluation. The Common Criteria standard is composed of an introduction document and two catalogues (Part 2 [i.4] & Part 3 [i.5]).

The first catalogue (CC Part 2 [i.4]) is a catalogue of security functional requirements that can be used to specify the list of the security functions that should be implemented and then evaluated. The catalogue is composed of the common features such as Identification & Authentication, Access Control, Logs, Cryptographic mechanisms, Configuration, etc.

The second catalogue (CC Part 3 [i.5]) is a catalogue of activities (security assurance requirements) that can be performed by an evaluator to check the correct implementation of the selected security functional requirements in the IT product. The evaluator can select any combination of components of the CC Part 3 [i.5] catalogue or can select one of the predefined packages of components (EAL1 to EAL7 packages).

The limitations of the Common Criteria standard are:

- The Common Criteria standard has been built to specify security requirements for IT products "on-the-shelf". Security targets and evaluation have been done for large systems but the results of the evaluation are currently not valuable because of the always limited representativity of [i.4] the tested system (usually integration platforms) with the operational system continuously in evolution.

- The security assurance (i.e. the assurance that the IT product effectively offers the expected security functions) is gained through the implementation of controls in the product development process (complete specifications, traceability, intensive functional testing done by the developer before product release, configuration management, security of the development environment, availability of guides, product maintenance) and the independent verification of these controls by the evaluator.

In order to enlarge the scope of the Common Criteria standard, an initiative has been conducted at ISO to build new catalogues of security functional requirements and security assurance requirements to embrace operational systems and not only IT products "on-the-shelf". The challenge was to take into account specificities of operational systems such as combination of IT security mechanisms with procedures and moreover the temporal aspect of the security in operations (continuous evolution, large scale infrastructures).

The ground for these new catalogues was to use the hierarchy structure of the CC catalogues (decomposition into classes, families, components, requirements) to organize security functional requirements and assurance requirements mainly extracted from the existing ISO/IEC 27002 [1] standard.

The result of this initiative is the ISO/IEC19791 [i.8] standard. Few nation members of the Common Criteria Management Board (CCMB) actively participate to the edition of the ISO/IEC19791 [i.8] standard but the standard has not been officially endorsed by the CCMB. However, the parallel initiative to standardize the British standards at ISO level succeeds and led to the ISO/IEC 27001 [6] and ISO/IEC 27002 [1] standards. Evaluation and certification scheme have been developed by governments and private companies for the ISO/IEC 27001 [6] standard rather than for the ISO/IEC TR 19791 [i.8] standard.

The security evaluation is undertaken not in the target environment and is based on the assumptions about the operational environment (OE). It is the objective to continue the validation of the target system through a quantitative and repeatable assessment of the effectiveness of the security functionality of the TOE also after the initial security evaluation, and to extend the validation and (passive) testing from the product development to the deployment and operational phase. Resulting observations (based on ETSI GS ISI 001-1 [5] indicators) could be used for some later evaluation (e.g. covering more/stronger requirements).

The linking from the ISG information security indicators (ISI) to CC Security Functional Requirements (SFR) may also allow to consider test (pattern) associated to CC SFRs also during product operation to retrieve attack pattern for the target system in operation. The detailed technical approach will be subject of ETSI GS ISI 005 [i.14] addressing Testing.

Annex A (normative): Position the proposed operational indicators against ISO/IEC 27002 control categories (Summary table)

Table A.1

ISO/IEC 27002 [1] control categories	Incident type indicators	Vulnerability (behavioural, software, configuration, general security) type indicators	Comments
A5			Non-continuous checking
A6			Purely organizational issues
A7	IMF_LOM.1 IMF_MDL.1 IDB_UID.1 IDB_RGH.1 to 7 IDB_MIS.1 IDB_IAC.1 IDB_LOG.1	VBH_PRC.1 to 6 VBH_IAC.1 to 2 VBH_FTR.1 to 3 VBH_WTI. 1 to 6 VBH_PSW.1 to 3 VBH_RGH.1 VBH_HUW.1 to 2	Focus on internal deviant behaviours
A8	IWH_UNA.1	VTC_NRG.1 VOR_PRT.1	Information classification + asset management
A9	IDB_UID.1 IDB_RGH.1 to 7	VBH_IAC.1 VBH_PSW.1 to 3 VBH_RGH.1 VCF_FWR.1 VCF_UAC.1 to 2 VCF_UAC.4 to 5 VTC_RAP.1	
A10		VBH_WTI.4	
A11	IEX_PHY.1	VTC_PHY.1	Marginal topic for a SIEM approach
A12	IEX_MLW.1 to 4 IMF_LOM.1 IMF_LOG.1 to 3 IDB_RGH.3 to 5 IDB_RGH.7 IDB_MIS.1 IDB_LOG.1	VCF_WTI.1 to 2 VCF_LOG.1 VCF_ARN.1 VCF_UAC.3 VTC_BKP.1 VOR_VNP.1 to 2 VOR_VNR.1 VOR_DSC.1	
A13	IMF_LOG.1 to 3 IMF_MDL.1 IDB_LOG.1	VBH_FTR.1 VCF_LOG.1 VCF_FWR.1 VTC_WFI.1	
A14		WSW_WSR.1 WSW_OSW.1 WSW_WBR.1 VOR_VNP.1 to 2 VOR_VNR.1	Marginal topic for continuous checking
A15	IDB_RGH.1	VBH_PSW.1 to 3 VOR_VNR.1	
A16	IEX_PHI.2 IEX_INT.1 to 3 IEX_DFC.1 IEX_MIS.1 IEX_DOS.1 IEX_MLW.1 to 4 IWH_VNP.1 to 3 IWH_VCN.1 IWH_UKN.1	VCF_UAC.2 VOR_RCT.1 to 2	
A17	IMF_BRE.1 to 4		Not central topic for a SIEM approach

ISO/IEC 27002 [1] control categories	Incident type indicators	Vulnerability (behavioural, software, configuration, general security) type indicators	Comments
A18	IMF_LOG.2 to 3 IMF_MDL.1	VBH_IAC.2 VBH_WTI.1 to 2 VBH_WTI.4 to 6 VBH_RGH.1 VCF_DIS.1 VCF_LOG.1 VCF_FWR.1 VCF_ARN.1 VCF_UAC.1 to 3 VCF_WTI.1 to 2 VTC_IDS.1	Focus on configuration vulnerabilities or non-conformities
NOTE: Indicators IEX_FGY.1, IEX_FGY.2, IEX_SPM.1, IEX_PHI.1, VOR_PRT.1, VOR_PRT.2, IMP_COS.1, IMP_TIM.1, IMP_TIM.2 and IMP_TIM.3 have no correspondence here.			

Annex B (informative): Position the proposed operational indicators against COBIT V4.1 DS5 Control Objectives (Summary table)

Table B.1

COBIT V4.1 [3] Control Objective	Incident type indicators	Vulnerability (behavioural, software, configuration, general security) type indicators	Comments
DS5.1 Management of IT Security	IEX_PHI.2 IEX_DFC.1 IEX_DOS.1 IMF_LOM.1 IMF_MDL.1 IWH_UKN.1 IMP_COS.1	VBH_FTR.1 to 3 VBH_WTI.1 to 6 VBH_HUW.1 to 2 VCF_WTI.1 to 2 VTC_NRG.1	Social engineering more and more part of attacks (Information security awareness, education and **training** therefore more and more important)
DS5.2 IT Security Plan	IEX_INT.2 to 3 IMF_BRE.1 to 4	VCF_LOG.1 VTC_BKP.1 VOR_VNP.1 to 3 VOR_PRT.1 to 3	Translation of business risk and compliance requirements into security in IT projects and into IT security processes
DS5.3 Identity Management	IDB_UID.1 IDB_RGH.1 to 7 IDB_MIS.1 IDB_IAC.1 IDB_LOG.1	VBH_WTI.1 VBH_RGH.1 VTC_RAP.1	Identification of all users and their activity
DS5.4 User Account Management	IDB_UID.1 IDB_RGH.1 to 7	VBH_PSW.1 to 3 VCF_UAC.1 to 5 VTC_RAP.1	Management of user accounts and access privileges
DS5.5 Security Testing, Surveillance and Monitoring	IMF_LOG.1 to 3 IWH_VNP.1 to 3 IWH_VCN.1 IWH_UKN.1 IWH_UNA.1	VBH_PRC.1 to 6 VBH_FTR.1 to 3 VBH_WTI.1 to 6 VBH_PSW.1 to 3 VBH_RGH.1 VSW_WSR.1 VSW_OSW.1 VSW_WBR.1 VCF_DIS.1 VCF_FWR.1 VCF_WTI.1 to 2 VCF_UAC.1 to 5 VOR_DSC.1	
DS5.6 Security Incident Definition	IMP_COS.1 IMP_TIM.1 to 3	VOR_RCT.1 to 2	
DS5.7 Protection of Security Technology	IEX_PHY.1 IDB_LOG.1	VBH_IAC.1 to 2 VBH_WTI.4 VBH_PSW.1 to 3 VCF_UAC.2 VCF_WTI.1 to 2 VOR_VNP.1 to 2 VOR_VNR.1	
DS5.8 Cryptographic Key Management			No indicators due to the low likelihood of such security events

COBIT V4.1 [3] Control Objective	Incident type indicators	Vulnerability (behavioural, software, configuration, general security) type indicators	Comments
DS5.9 Malicious Software Prevention, Detection and Correction	IEX_MLW.1 to 4	VCF_WTI.1	Link to be made with **DS5.5** (regarding vulnerability management for patch application)
DS5.10 Network Security	IEX_INT.2 to 3	VBH_WTI.3 VCF_FWR.1 VTC_IDS.1 VTC_WFI.1	
DS5.11 Exchange of Sensitive Data		VBH_FTR.2 to 3 VBH_WTI.4	Focus to be made on deviant behaviours
NOTE: Indicators IEX_FGY.1 and 2, IEX_SPM.1, IEX_PHI.1, IEX_MIS.1 and VTC_PHY.1 have no correspondence.			

Annex C (informative): Position the proposed operational indicators against CAG V4.0 framework 20 Critical Controls (Summary table)

Table C.1

CAG [4] Critical Controls	Incident type indicators	Vulnerability (behavioural, software, configuration, general security) type indicators	Comments
CC 1 Inventory of Authorized & Unauthorized Devices	IEX_PHY.1 IWH_UNA.1	VTC_NRG.1	Cf. 70 % of all incidents due to not registered or not managed devices
CC 2 Inventory of Authorized & Unauthorized Software	IWH_VNP.1 to 3 IWH_UNA.1		The most difficult control to apply
CC 3 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers		VBH_PRC.5 VBH_WTI.1 to 6 VBH_PSW.1 to 3 VCF_LOG.1 VCF_WTI.2 VOR_VNR.1	The less tackled issue regarding all kinds of vulnerabilities
CC 4 Continuous Vulnerability Assessment and Remediation	IEX_MLW.3 to 4 IWH_VNP.1 to 3 IWH_VCN.1	WSW_WSR.1 VSW_OSW.1 VSW_WBR.1 VOR_VNP.1 to 2	Scoring of vulnerabilities is key
CC 5 Malware Defences	IEX_MLW.1 to 4	VCF_WTI.1	Antivirus today insufficient
CC 6 Application Software Security	IEX_INT.1 to 3	VSW_WSR.1 VOR_PRT.1 to 3	Not continuous checking
CC 7 Wireless Device Control		VTC_WFI.1	Marginal topic for a SIEM approach
CC 8 Data Recovery Capability		VTC_BKP.1	Marginal topic for a SIEM approach
CC 9 Security Skills Assessment and Appropriate Training to Fill Gaps	IEX_DOS.1 IMF_LOM.1 IMF_MDL.1 IDB_IAC.1 IWH_UKN.1 IEX_PHI.2	VBH_FTR.1 to 3 VBH_WTI.1 to 6 VBH_PSW.1 to 3 VBH_HUW.1 to 2	Social engineering more and more part of attacks
CC 10 Secure Configurations for Network Devices such as Firewalls, Routers and Switches		VCF_FWR.1 VOR_VNR.1	The most mature IT security issue within organizations
CC 11 Limitation and Control of Network Ports, Protocols and Services	IEX_INT.2 to 3 IEX_MIS.1 IDB_IAC.1	VBH_PRC.1 to 3 VBH_PRC.6 VCF_DIS.1	
CC 12 Controlled Use of Administrative Privileges	IEX_MLW.3 to 4 IDB_RGH.3 IDB_RGH.5 IDB_MIS.1 IDB_LOG.1	VBH_PRC.1	One of the most frequent way to critical incidents
CC 13 Boundary Defense		VBH_PRC.4 VBH_IAC.1 to 2	Issue generally well dealt with
CC 14 Maintenance, Monitoring and Analysis of Audit Logs	IMF_LOG.1 to 3 IDB_LOG.1		At the heart of SIEM approaches

CAG [4] Critical Controls	Incident type indicators	Vulnerability (behavioural, software, configuration, general security) type indicators	Comments
CC 15 Controlled Access Based on the Need to Know	IDB_RGH.1 to 7	VBH_WTI.1 VBH_RGH.1 VCF_UAC.1 to 5	Focus to be applied on this matter too much neglected
CC 16 Account Monitoring and Control	IDB_UID.1 IDB_RGH.1 to 7 IDB_LOG.1	VCF_UAC.1 to 5 VTC_RAP.1	
CC 17 Data Loss Prevention	IEX_MLW.3 to 4		Many security devices required
CC 18 Incident Response and Management		VOR_DSC.1 VOR_RCT.1 to 2 IMP_COS.1 IMP_TIM.1 to 3	Be prepared is key
CC 19 Secure Network Engineering		VTC_IDS.1 VOR_PRT.1 to 3	Not continuous checking
CC 20 Penetration Tests and Red Team Exercises			More and more important to get truly efficient teams
NOTE: Indicators IEX_FGY.1 and 2, IEX_SPM.1, IEX_PHI.1, IEX_DFC.1, IMF_BRE.1 to 4 and VTC_PHY.1 have no correspondence.			

Annex D (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 E (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.

ISO/IEC 27035:2011: "Information technology - Security techniques - Information security incident management".

History

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