ETSI GS ISI 003 V1.2.1 (2018-01)

Information Security Indicators (ISI); Key Performance Security Indicators (KPSI) to evaluate the maturity of security event detection

Disclaimer

The present 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-003rev_2

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

Intellectual Property Rights

Essential patents

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 (https://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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

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

The present document is included in a series of 9 ISI specifications. These 9 specifications are the following (see figure 1 summarizing the various concepts involved in event detection and interactions between all specifications):

- ETSI GS ISI 001-1 [1]: addressing (together with its associated guide ETSI GS ISI 001-2 [2]) information security indicators, meant to measure application and effectiveness of preventative measures.
- ETSI GS ISI 002 [3]: addressing the underlying event classification model and the associated taxonomy.
- **ETSI GS ISI 003: addressing the key issue of assessing an organization's maturity level regarding overall event detection (technology/process/ people) and to evaluate event detection results.**
- ETSI GS ISI 004 [4]: 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.1]: addressing ways to produce security events and to test the effectiveness of existing detection means within an organization. More detailed and more a case by case approach than the present document and therefore complementary.
- ETSI GS ISI 006 [i.2]: addressing another engineering part of the series, complementing ISI-004 and focusing on the design of a cybersecurity language to model threat intelligence information and enable detection tools interoperability.
- ETSI GS ISI 007 [i.3]: addressing comprehensive guidelines to build and operate a secured SOC, especially regarding the architectural aspects, in a context where SOCs are often real control towers within organizations.
- ETSI GS ISI 008 [i.4]: addressing and explaining how to make SIEM a whole approach, which is truly integrated within an overall organization-wide and not only IT-oriented cyber defence.

Figure 1 summarizes the various concepts involved in event detection and the interactions between the specifications.

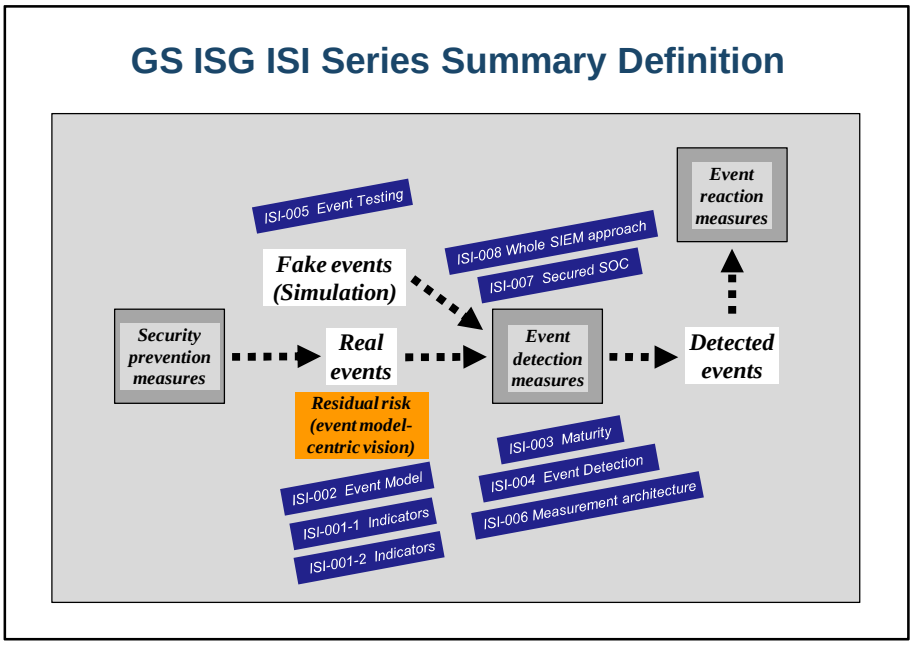

Figure 1: Positioning the 9 GS ISI against the 3 main security measures

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

The present document addresses the event detection aspects of the information security processes in an organization. The maturity level assessed during event detection can be considered as a good approximation of the overall Cyber Defence and SIEM maturity level of an organization.

1 Scope

The present document defines and describes a set of Key Performance Security Indicators (KPSI) to be used for the evaluation of the performance, the maturity levels of the detection tools and processes used within organizations for security assurance. The response is not included in the scope of the present document.

In particular, the purpose of the present document is to enable organizations to:

- assess the overall maturity level of the security event detection;
- provide a reckoning formula to assess detection levels of major security events as summarized in ETSI GS ISI 001-1 [1];
- evaluate the results of measurements.

This work is mainly based on the CIS® Controls [5].

The target groups of the present document are Head of detection, reaction teams, Cyber defence team and head of security governance.

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 referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://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] 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".

[2] 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".

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

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

[5] CIS® Controls V6.1.

NOTE: Available at https://www.cisecurity.org/controls/ for an up-to-date version.

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

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 referenced 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] ETSI GS ISI 005: "Information Security Indicators (ISI); Guidelines for security event detection testing and assessment of detection effectiveness".

[i.2] ETSI GS ISI 006: "ISI An ISI-compliant Measurement and Event Management Architecture for Cyber Security and Safety".

[i.3] ETSI GS ISI 007: "ISI Guidelines for building and operating a secured SOC".

[i.4] ETSI GS ISI 008: "Information Security Indicators (ISI); Description of a whole organization-wide SIEM approach".

[i.5] The Capability Maturity Model Integration CMMI® V1.3 (Software Engineering Institute/Carnegie Mellon University, 2001).

NOTE: Available at https://resources.sei.cmu.edu/asset_files/presentation/2011_017_001_23331.pdf.

[i.6] OGC PSM3® V2.1: "Portfolio, Programme and Project Management Maturity Model (2008).

NOTE: Available at http://miroslawdabrowski.com/downloads/P3M3/OGC%20branded/P3M3_v2.1_Introduction_and_Guide.pdf.

3 Definitions, symbols and abbreviations

3.1 Definitions

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

3.2 Symbols

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

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GS ISI 001-2 [2] and the following apply:

CC	Critical Control
CMMI	Capability Maturity Model Integration
CSIRT	Computer Security Incident Response Team
KPI	Key Performance Indicators
KPSI	Key Performance Security Indicators
MSSP	Managed security service provider
SOC	Security Operation Centre

4 Background

4.1 Key Performance Indicators

Key Performance Indicators (KPIs) are quantifiable variables which can measure the performance of an organization, evaluate the success of specific activities and support decision making processes. KPIs are metrics that allow to measure progress and deficiency. The metrics have to be well-defined and quantifiable to be useful.

KPIs can be used to assess the performance of IT services. Examples of IT KPIs are the availability of IT systems and services, the Service Level Agreements (SLAs), the Mean Time Between Failures (MTBF) and the Mean Time To Recover (MTTR), and Mean-Time-Between-System-Incidents (MTBSI).

The usage of KPI in the field of Information Assurance is at its early stage. Defining KPIs for the Security Assurance processes is difficult because of the complexity of regulations, certifications, technical and organizational issues, and budget constraints. Hence it is a complex task to quantify clear Security Assurance objectives and performance in terms of KPIs.

4.2 Key Performance Security Indicators

Key Performance Security Indicators (KPSIs) can measure the maturity level of the information security processes (detection and detection-related processes).

A Maturity Model to measure the performance in the Security Assurance field can be based on the five level maturity framework adapted from The Capability Maturity Model Integration CMMI® (Software Engineering Institute, 2001) [i.5] and Portfolio, Programme and Project Management Maturity Model P3M3® (OGC, 2008) [i.6]. Organizations using these models, can assess the maturity level of their performance management practices in the five dimensions of the model:

1) **Initial:** Processes are managed ad hoc. No measure of the performance is requested.
2) **Managed:** Processes characterized for projects and are often reactive.
3) **Defined:** Processes are tailored for the organization and are proactive.
4) **Quantitatively Managed:** Processes are measured and controlled.
5) **Optimizing:** Continuous Process Improvement.

To adapt these models to security event detection and detection-related reactions, a simplified 3-level scale is proposed:

- The present document, level 1 corresponding to CMMI® levels 1 and 2.
- The present document, level 2 corresponding to CMMI® levels 3 and 4.
- The present document, level 3 corresponding to CMMI® level 5.

The three levels can be defined as follows:

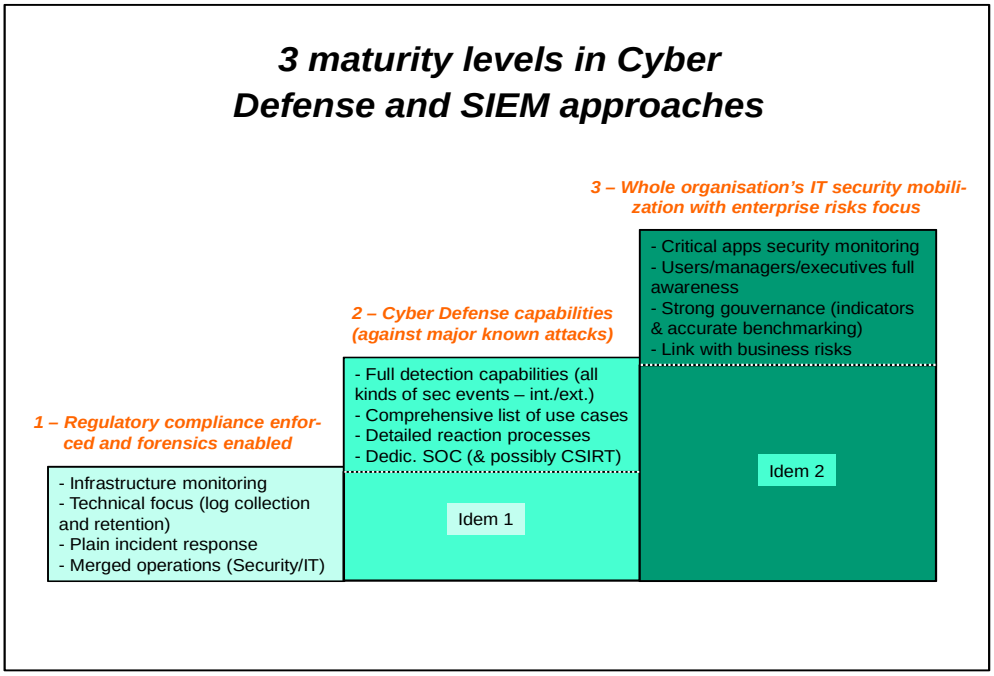

Figure 2: 3 majority levels in Cyber Defence and SIEM approaches

4.3 SANS CAG

The CIS Controls [5] is a compliance standard that specifies 20 "control points" that have been identified through a consensus of security professionals from the federal and private industry. The aim is to begin the process of establishing a prioritized baseline of information security measures and controls that can be applied across organizations to help improving their defences.

The 20 Critical Controls subject to collection, measurement, and validation currently defined are:

1) Inventory of Authorized and Unauthorized Devices.
2) Inventory of Authorized and Unauthorized Software.
3) Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers.
4) Continuous Vulnerability Assessment and Remediation.
5) Malware Defences.
6) Application Software Security.
7) Wireless Device Control.
8) Data Recovery Capability (validated manually).
9) Security Skills Assessment and Appropriate Training to Fill Gaps (validated manually).
10) Secure Configurations for Network Devices such as Firewalls, Routers and Switches.
11) Limitation and Control of Network Ports, Protocols and Services.
12) Controlled Use of Administrative Privileges.
13) Boundary Defence.
14) Maintenance, Monitoring, and Analysis of Security Audit Logs.

15) Controlled Access Based on the Need to Know.

16) Account Monitoring and Control.

17) Data Loss Prevention.

18) Incident Response Capability (validated manually).

19) Secure Network Engineering (validated manually).

20) Penetration Tests and Red Team Exercises (validated manually).

Each Critical Control (CC) is described in detail, is subject to continuous monitoring and checking and has gained a broad consensus as regards their relevancy and effectiveness.

The KPSIs defined within the present document are based on the CC list concerning detection, with adaptation and extension whenever needed to cover the scope of the ETSI ISG ISI series.

5 Key Performance Security Indicators

5.1 How to use KPSIs to assess the organization's overall maturity level in security event detection and response posture

The first purpose of KPSIs is to assess the organization's overall maturity level of security event detection and response posture. The way to do it is to reckon the average of all KPSIs in order to get the unique level for the whole organization, which can then be compared to the best in the industry.

5.2 How to use KPSIs as a first step to evaluate the detection levels of security events

The second purpose of KPSIs is to enable an organization to assess the actual detection levels of security events as summarized in ETSI GS ISI 001-1 [1] information security indicators and to evaluate the results of the measurements.

The formula to reckon the actual detection level of events is by making an indicator from the following: state-of-the-art detection level (see ETSI GS ISI 001-1 [1]) x organization KPSI/state-of-the-art KPSI.

To apply this formula, it is of course required to know which KPSI(s) is (are) applicable to the given indicator. This requirement is met below in clause 5.4 for each indicator (see the row "Core ISI 001 mapping" [1] for a minimal indicators mapping, and "Additional ISI 001 mapping" [1] for a full mapping of the indicators over the KPSIs). When an indicator has several KPSIs assigned, it is proposed to take the average of all of them to get a unique and finalized KPSI.

All data necessary to use the formula are given for each KPSI in clause 5.4 with a recap in annex A.

5.3 KPSIs description table

Table 1 skeleton defines the KPSIs covering major detection issues. Each KPSI has been described by using table 1.

Table 1

Name	Full title/name of the KPSI		
KPSI Index	Index number of the KPSI within this GS		
CIS Control(s)	References to the CIS Control(s) [5]		
Description/rationale	Extended description of the KPSI and/or rationale for this KPSI		
(Core) ISI 001Indicator mapping [1]	Core mapping to the ISI 001 security indicators [1] and [2] Minimal set of indicators to be mapped to this specific KPSI		
Additional ISI 001 Indicator mapping [1]	Additional mapping to the ISI 001 indicators [1] and [2]. Full set of indicators to be mapped to this specific KPSI		
State of the Art figure	This field gives the state-of-the-art figure (which level for the best ones within the security community) related to this specific KPSI. The figures have been estimated by ETSI ISG ISI		
Level 0	**Level 1 (see note)**	**Level 2 (see note)**	**Level 3 (see note)**
This box contains the description of the organization's maturity level about detection mechanisms (tools, people, processes) corresponding to level 0, which corresponds to no processes, tools, people dedicated to detection.	This box contains the description of the organization's maturity level about detection mechanisms (tools, people, processes) corresponding to level 1, which is "**basic and just compliance-oriented**".	This box contains the description of the organization's maturity level about detection mechanisms (tools, people, processes) corresponding to level 2, which is "**mature and integrated**".	This box contains the description of the organization's maturity level about detection mechanisms (tools, people, processes) corresponding to level 3, which is "**advanced and business integrated**".
NOTE: See clause 4.2 for more explanations.			

5.4 Description of the relevant KPSIs

The list of relevant KPSIs has been identified amongst the list of the 20 CIS critical controls, which concerns detection and response issues.

Table 2

Name	**Inventory of software or devices**		
KPSI Index	1		
CIS Control(s)	1, 2		
Description/rationale	This KPSI reflects the concept that asset inventory is at the basis of every ISMS. 70 % of all incidents are not registered or not managed devices.		
Core ISI 001 mapping [1]	IWH_UNA.1, VTC_NRG.1		
Additional ISI 001 mapping [1]	IWH_VNP.1 to 3, IWH_VCN.1, IWH_UNA.1, VTC_WFI.1, VTC_NRG.1		
State of the Art figure	2		
Level 0	**Level 1**	**Level 2**	**Level 3**
No policy, no process, no tools	Processes characterized for the organization but often reactive (reset after incidents). No tools	Processes systematically implemented. Tools usage	Processes continuously checked with the level of application and effectiveness evaluated (indicators, with well-defined periodic reporting processes toward upper levels)

Table 3

Name	Configuration monitoring and remediation		
KPSI Index	2		
CIS Control(s)	3,10		
Description/rationale	The less tackled issue regarding all kinds of vulnerabilities (regarding mobile devices, laptops, workstations and servers). More mature IT security issue regarding network devices (such as firewalls, routers and switches). 30 % of all security incidents are made possible by exploitation of configuration vulnerability.		
Core ISI 001 mapping [1]	VOR_VNR.1, VCF_FWR.1, VCF_ARN.1, VCF_TRF.1, VBH_WTI.1 to 6, VBH_PSW.1 to 3, VBH_PRC.5, IWH_VCN.1		
Additional ISI 001 mapping [1]	IWH_VCN.1, VOR_VNR.1, all VCF indicators, VBH_PRC.1 to 6, VBH_IAC.2, VBH_FTR.1 to 3, VBH_WTI.1 to 6, VBH_PSW.1 to 3, VBH_RGH.1, IWH_VCN.1, VTC_IDS.1, VTC_MOF.1, VTC_NRG.1, VTC_PHY.1		
State of the Art figure	2		
Level 0	**Level 1**	**Level 2**	**Level 3**
No process, no tools	Processes characterized for the organization but often reactive (reset after incidents). No tools	Processes systematically implemented. Tools used (to identify all deviations from technical policies)	Processes continuously checked with level of application and effectiveness evaluated (indicators, with well-defined periodic reporting processes toward upper levels)

Table 4

Name	Continuous software vulnerability assessment and remediation		
KPSI Index	3		
CIS Control(s)	4		
Description/rationale	Another mandatory issue in detection and response, complementary to the previous KPSI (20 to 30 % of all security incidents are made possible by exploitation of software vulnerability).		
Core ISI 001 mapping [1]	IEX_MLW.3 to 4, IWH_VNP.1 to 3, VSW_WSR.1, VSW_OSW.1, VSW_WBR.1, VOR_VNP.1 to 2		
Additional ISI 001 mapping [1]	IEX_MLW.3 to 4, IWH_VNP.1 to 3, all VSW indicators, VOR_VNP.1 to 2		
State of the Art figure	2		
Level 0	**Level 1**	**Level 2**	**Level 3**
No policy, no process, no tools	Processes characterized for the organization but often reactive (reset after incidents). No tools. Possible external watch and alerts collection	Processes systematically implemented. Tools used (vulnerability scanning, risk ranking, patch management, workaround application)	Processes continuously checked with level of application and effectiveness evaluated (indicators, with well-defined periodic reporting processes toward upper levels)

Table 5

Name	User access and account monitoring		
KPSI Index	4		
CIS Control(s)	12,16		
Description/rationale	As regards administrative privileges, their unwanted use is one of the most frequent paths to critical incidents.		
Core ISI 001 mapping [1]	IEX_MLW.1 to 4, IDB_UID.1, IDB_RGH.1 to 7, IDB_IDB.1, IDB_MIS.1, IDB_LOG.1, VBH_PRC.1, VCF_UAC.1 to 5, VTC_RAP.1		
Additional ISI 001 mapping [1]	IEX_MLW.1 to 4, all IDB indicators, VBH_PRC.1, VBH_RGH.1, VCF_UAC.1 to 5, VTC_RAP.1		
State of the Art figure	2		
Level 0	**Level 1**	**Level 2**	**Level 3**
No policy, no charter, no process, no tools	Processes characterized for the organization but often reactive (reset after incidents)	Processes systematically implemented. Tools used (to identify all deviations from technical policies and deviant behaviours - especially for administrators)	Processes continuously checked with level of application and effectiveness evaluated (indicators, with well-defined periodic reporting processes toward upper levels)

Table 6

Name	Log collection, analysis and archiving		
KPSI Index	5		
CIS Control(s)	14		
Description/rationale	This issue is one of the main pieces at the heart of SIEM approaches.		
Core ISI 001 mapping [1]	IEX_INT.2, IEX_MLW.3 to 4, IMF_TRF.1 to 3, IDB_UID.1, IDB_IAC.1, IDB_LOG.1, VBH_PRC.1 to 6, VBH_IAC.1 to 2, VBH_FTR.1 to 3, VBH_WTI.3		
Additional ISI 001 mapping [1]	IEX_INT.2, IEX_MIS.1, IEX_DOS.1, IEX_MLW.3 to 4, IMF_TRF.1 to 3, IDB_UID.1, IDB_IAC.1, IDB_LOG.1, VBH_PRC.1 to 6, VBH_IAC.1 to 2, VBH_FTR.1 to 3, VBH_WTI.3, VCF_ARN.1, VCF_UAC.3, VCF_UAC.5		
State of the Art figure	3		
Level 0	**Level 1**	**Level 2**	**Level 3**
No policy (log tracking, collection and analysis), no charter, no process, no tools	Processes characterized for some IT areas only. SIEM tools used with technical focus (log collection only). Log collection and centralization tools used. Well-defined whole organization structure for monitoring checking and archiving (Possible dedicated SOC or MSSP detection service)	Processes systematically implemented (organization-wide and continuous monitoring). Knowledge sharing on security incident monitoring best practices. Tools used (SIEM solutions with Use Cases development through dedicated correlation rules - cf. genuine threat intelligence). Tools capacity/performance monitoring. Always dedicated SOC (more rarely MSSP)	Processes continuously checked with level of application and effectiveness evaluated (indicators, with well-defined periodic reporting processes toward upper levels)

Table 7

Name	Security Skills Assessment and Appropriate Training		
KPSI Index	6		
CIS Control(s)	9		
Description/rationale	Security skills assessment and training are especially important in SOC and CSIRT to detect security incidents through technical symptoms that often need to be qualified by seasoned teams. This requirement also applies to incident response.		
Core ISI-001 mapping [1]	All IEX indicators, all IDB indicators, all VBH indicators, all VCF indicators		
Additional ISI-001 mapping [1]	All IEX indicators, IMF_LOM.1, IMF_TRF.1 to 3, all IDB indicators, IWH_VNP.1 to 3, IWH_VCN.1, IWH_UKN.1. all VBH indicators, all VSW indicators, all VCF indicators, VTC_PHY.1		
State of the Art figure	2		
Level 0	**Level 1**	**Level 2**	**Level 3**
No policy, no process	Processes characterized for the organization but often reactive (reset after incidents and poor incident management)	Processes systematically implemented (skills assessment during employment, periodic and/or relevant training)	Processes continuously checked with level of application evaluated (indicators, with well-defined periodic reporting processes toward upper levels)

Table 8

Name	Cyber stress drills		
KPSI Index	7		
CIS Control(s)	20		
Description/rationale	This issue complements the previous KPSI and is important to get effective operational security teams.		
Core ISI 001 mapping [1]	All IEX indicators, all IDB indicators, all VBH indicators, all VCF indicators		
Additional ISI 001 mapping [1]	All IEX indicators, all IDB indicators, IWH_UKN.1, all VBH indicators, all VCF indicators		
State of the Art figure	2		
Level 0	**Level 1**	**Level 2**	**Level 3**
No policy, no process	Processes characterized for some IT areas only	Processes systematically implemented (Periodic and/or relevant drills)	Processes continuously checked with level of application evaluated (indicators, with well-defined periodic reporting processes toward upper levels)

Table 9

Name	Data loss prevention (real-time part, excluding initial implementation)		
KPSI Index	8		
CIS Control(s)	17		
Description/rationale	In this document, the relevant issue is the real-time and detection part of data loss prevention.		
Core ISI 001mapping [1]	IEX_INT.2, IEX_MLW.1 to 4, IMF_LOM.1, IDB_UID.1, IDB_RGH.1 to 7, IDB_IDB.1		
Additional ISI 001mapping [1]	IEX_INT.2, IEX_MLW.1 to 4, IMF_LOM.1, IDB_UID.1, IDB_RGH.1 to 7, IDB_IDB.1, VBH_PRC.1 to 6		
State of the Art figure	2		
Level 0	**Level 1**	**Level 2**	**Level 3**
No policy, no process	Processes characterized for the organization but often reactive (reset after incidents). No tools	Processes systematically implemented. Tools used (to detect all critical leaks)	Processes continuously checked with level of application and effectiveness evaluated (indicators, with well-defined periodic reporting processes toward upper levels)

Annex A (normative): Recap of available KPSIs

Table A.1

KPSI index	Name	CIS Controls references	Core ISI 001 Indicator mapping	Additional ISI 001 Indicator mapping	State-of-the-art
1	**Inventory of software or devices**	1,2	IWH_UNA.1, VTC_NRG.1	IWH_VNP.1 to 3, IWH_VCN.1, IWH_UNA.1, VTC_WFI.1, VTC_NRG.1	2
2	**Configuration monitoring and remediation**	3,10	VOR_VNR.1, VCF_FWR.1, VCF_ARN.1, VCF_TRF.1, VBH_WTI.1 to 6, VBH_PSW.1 to 3, VBH_PRC.5, IWH_VCN.1	IWH_VCN.1, VOR_VNR.1, all VCF indicators, VBH_PRC.1 to 6, VBH_IAC.2, VBH_FTR.1 to 3, VBH_WTI.1 to 6, VBH_PSW.1 to 3, VBH_RGH.1, IWH_VCN.1, VTC_IDS.1, VTC_MOF.1, VTC_NRG.1, VTC_PHY.1	2
3	**Continuous software vulnerability assessment and remediation**	4	IEX_MLW.3 to 4, IWH_VNP.1 to 3, VSW_WSR.1, VSW_OSW.1, VSW_WBR.1, VOR_VNP.1 to 2	IEX_MLW.3 to 4, IWH_VNP.1 to 3, all VSW indicators, VOR_VNP.1 to 2	2
4	**User access and account monitoring**	12,16	IEX_MLW.1 to 4, IDB_UID.1, IDB_RGH.1 to 7, IDB_IDB.1, IDB_MIS.1, IDB_LOG.1, VBH_PRC.1, VCF_UAC.1 to 5, VTC_RAP.1	IEX_MLW.1 to 4, all IDB indicators, VBH_PRC.1, VBH_RGH.1, VCF_UAC.1 to 5, VTC_RAP.1	2
5	**Log collection, analysis and archiving**	14	IEX_INT.2, IEX_MLW.3 to 4, IMF_TRF.1 to 3, IDB_UID.1, IDB_IAC.1, IDB_LOG.1, VBH_PRC.1 to 6, VBH_IAC.1 to 2, VBH_FTR.1 to 3, VBH_WTI.3	IEX_INT.2, IEX_MIS.1, IEX_DOS.1, IEX_MLW.3 to 4, IMF_TRF.1 to 3, IDB_UID.1, IDB_IAC.1, IDB_LOG.1, VBH_PRC.1 to 6, VBH_IAC.1 to 2, VBH_FTR.1 to 3, VBH_WTI.3, VCF_ARN.1, VCF_UAC.3, VCF_UAC.5	3
6	**Security Skills Assessment and Appropriate Training**	9	All IEX indicators, all IDB indicators, all VBH indicators, all VCF indicators	All IEX indicators, IMF_LOM.1, IMF_TRF.1 to 3, all IDB indicators, IWH_VNP.1 to 3, IWH_VCN.1, IWH_UKN.1. all VBH indicators, all VSW indicators, all VCF indicators, VTC_PHY.1	2

KPSI index	Name	CIS Controls references	Core ISI 001 Indicator mapping	Additional ISI 001 Indicator mapping	State-of-the-art
7	**Cyber stress drills**	20	All IEX indicators, all IDB indicators, all VBH indicators, all VCF indicators	All IEX indicators, all IDB indicators, IWH_UKN.1, all VBH indicators, all VCF indicators	2
8	**Data loss prevention (real-time part, excluding initial implementation)**	17	IEX_INT.2, IEX_MLW.1 to 4, IMF_LOM.1, IDB_UID.1, IDB_RGH.1 to 7, IDB_IDB.1	IEX_INT.2, IEX_MLW.1 to 4, IMF_LOM.1, IDB_UID.1, IDB_RGH.1 to 7, IDB_IDB.1, VBH_PRC.1 to 6	2

Annex B (informative): SOC example

The following table B.1 describes for the 8 areas of maturity assessment (and related KPSIs), how the present document can be refined and implemented for SOCs and more globally for a whole organization.

Each upper level is described by enhanced requirements against the lower level. In bold are given the possible areas of application to SOCs.

Table B.1

KPSIs	Levels (1 to 3)	Process/ People/ Tools	Applicable to the monitored perimeter of the whole organization	Applicable to SOC
1 **Inventory of devices or software**	**1**	Process	• Regulatory compliance • Perform regular scanning for unauthorized devices and software on the whole perimeter (against a continuously updated official list)	• Idem (applicable to the whole organization's perimeter asset inventory discovery)
		People	• Training on the importance to use only registered and managed devices and software (Cf. 70 % of all incidents due to not abiding by this basic rule), and to fight shadow-IT	• Idem (applicable to the SOC team)
		Tools	• Tools integrated to network and system management tools	• Idem (applicable to the whole organization's perimeter asset inventory discovery)
	2	Process	• Idem level 1	• Idem level 1
		People	• Idem level 1	• Idem level 1
		Tools	• Asset inventory discovery tools (active or passive - Cf. for example some IPS analyzing forbidden traffic) • Software inventory tools or file integrity checking tools to validate the list of authorized software (and version and patch level) has not been modified (applicable to each type of system, including servers, workstations, and laptops)	• Idem (applicable to the whole organization's perimeter asset inventory discovery)
	3	Process	• Idem level 1	• Idem level 1
		People	• Tie critical incidents and related vulnerabilities (likely if not managed) to their business impact (for example by building Information Protection Plans) to enhance users' concern and motivation	• Not applicable
		Tools	• Dynamic host configuration protocol (DHCP) server logging, and use of a system to improve the asset inventory and help detect unknown systems through this DHCP information	• Idem (applicable to the whole organization's perimeter asset inventory discovery)

KPSIs	Levels (1 to 3)	Process/ People/ Tools	Applicable to the monitored perimeter of the whole organization	Applicable to SOC
2 **Configu-ration monitor-ring**	**1**	Process	• Regulatory compliance • Periodic checking of the presence of configuration non-conformities • Target of some types of assets only (sensitive Web site, Web browser, firewall)	• Idem (applicable to the whole SOC information system + to the whole organization's perimeter technical compliance checking)
		People	• Training of IT people (Developers, administrators) to use of technical compliance services and to related regulations	• Idem (applicable to the SOC team)
		Tools	• Use of external technical compliance services (usually based on standard security baselines for some types of software or devices)	• **Idem (applicable to the whole SOC information system + to the whole organization's perimeter technical compliance checking)**
	2	Process	• Broad continuous checking of a large set of types of assets • Measurement through possibly related ETSI ISI-001 VCF and VBH indicators (if relevant)	• **- Idem (applicable to the whole SOC information system** + to the whole organization's perimeter technical compliance checking) • On-boarding management • Change management • Release management • ISO/IEC 27002 [6] compliant
		People	• Training of IT people (Administrators) to internal use of technical compliance checking tools	• Idem (applicable to the SOC team)
		Tools	• Periodic and frequent use of technical compliance checking tools on a large set of assets	• Idem (applicable to the whole SOC information system + to the whole organization's perimeter technical compliance checking)
	3	Process	• Benchmarking against statistical state-of-the rat figures	• Not applicable
		People	• Tie non-conformities and possibly related incidents to their business impact (for example by relying on existing Information Protection Plans) to enhance IT People concern and motivation	• Idem (applicable to the SOC team)
		Tools	• Advanced scanning and simulation tools • (Sky-Box-like, etc.)	• Idem (applicable to the whole organization's perimeter technical compliance checking)

KPSIs	Levels (1 to 3)	Process/ People/ Tools	Applicable to the monitored perimeter of the whole organization	Applicable to SOC
3 **Conti-nuous software vulnera-bility assess-ment**	**1**	Process	• Regulatory compliance • External watch and alerts collection • Periodic checking of the presence of known software vulnerabilities • Target of critical assets only	• Idem (applicable to the whole SOC information system + to the whole organization's perimeter scanning)
		People	• Training of IT people (Developers, administrators) to use of scanning services and to related regulations	• Idem (applicable to the SOC team)
		Tools	• Use of external scanning services	• Idem (applicable to the whole SOC information system + to the whole organization's perimeter scanning)
	2	Process	• Calculate vulnerability criticality (through a better link to asset sensitivity – Cf. CVSS score) • Measurement through possibly related ETSI GS ISI 001 VSW indicators (if relevant)	• Idem (applicable to the whole SOC information system + to the whole organization's perimeter scanning) • Change management • Release management • ISO/IEC 27002 [6] compliant
		People	• Training of IT people (Developers, administrators) to internal use of scanning tools, and calculation of CVSS score	• Idem (applicable to the SOC team)
		Tools	• Periodic and frequent use of VDS tools on a large set of assets (with accurate calculation of vulnerability criticality – Cf. CVSS score)	• Idem (applicable to the whole SOC information system + to the whole organization's perimeter scanning)
	3	Process	• Idem level 2	• Idem level 2
		People	• Tie critical vulnerabilities and possibly related incidents to their business impact (for example by relying on existing Information Protection Plans) to enhance IT People concern and motivation	• Idem (applicable to the SOC team)
		Tools	• Advanced scanning and simulation tools (Sky-Box-like, etc.)	• Idem (applicable to the whole organization's perimeter scanning)

KPSIs	Levels (1 to 3)	Process/ People/ Tools	Applicable to the monitored perimeter of the whole organization	Applicable to SOC
4 **User access and account moni-toring**	**1**	Process	• Regulatory compliance • Periodic review of accounts (least privilege) See especially administrative privileges • Periodic review of authentication devices • Periodic review of accounts without owners • Periodic review of inactive or dormant accounts	• Idem (applicable to the whole SOC information system)
		People	• Training on account usage (admin and others), i.e. logging-off, change of position, passwords, etc.	• **Idem (applicable to the SOC team)**
		Tools	• Logging of all connections • Cleaned logs	• **Idem (applicable to the whole SOC information system)**
	2	Process	• Use of ETSI GS ISI 001 [1], [2] and ETSI GS ISI 002 [3] standards (security event classification, indicators, notification)	• Idem (applicable to the whole SOC information system) • ISO/IEC 27002 [6] compliant
		People	• Training to ETSI GS ISI 00x standards • Make them aware of their behaviour through ad hoc sessions (based on accurate figures) • Human detection (spear-phishing, etc.)	• **Idem (applicable to the SOC team)**
		Tools	• Various tools (including SIEM) used to detect all deviant behaviours and non-conformities (measurement through related IDB and VBH indicators) • Calculate incident criticality (incident severity x asset sensitivity) through a link to asset sensitivity	• **Idem (applicable to the whole SOC information system** + to the whole organization's perimeter monitoring)
	3	Process	• Strong threat intelligence processes (use case management through exchanges between Governance or CSIRT and various detection units - Cf. exchanges of statistical state-of-the-art and benchmarking against these figures)	• Idem (applicable especially to the SOC team for tweaking its monitoring tools)
		People	• Tie critical incidents and related vulnerabilities to their business impact (for example by building Information Protection Plans) to enhance users' concern and motivation	• Not applicable
		Tools	• Advanced tools (Big Data, Cyber Ark-like for administrative privileges management, etc.)	• Idem (applicable to the whole organization's perimeter monitoring)

KPSIs	Levels (1 to 3)	Process/ People/ Tools	Applicable to the monitored perimeter of the whole organization	Applicable to SOC
5 **Log collection analysis and archiving**	**1**	Process	• Regulatory compliance • Periodic review of logs • Process to produce, store and handle raw logs in a controlled and compliant way (to be used in forensics)	• **Idem (applicable to the whole SOC information system+ to the organization's perimeter log retention)**
		People	• Training of IT people (Developers, administrators) to log production and to related regulations	• **Idem (applicable to the SOC team)**
		Tools	• Log production • Cleaned logs • Log storage, retention and archiving during a defined period of time (filtered logs, raw logs with guaranteed integrity and usable for forensics) • Automatic detection of log production and/or retention malfunction	• **Idem (applicable to the whole SOC information system + to the organization's perimeter log retention)**
	2	Process	• Use of ETSI GS ISI 001 [1], [2] and ETSI GS ISI 002 [3] standards (security event classification, indicators, notification)	• **Idem (applicable to the whole SOC information system+ to the organization's perimeter log retention)** • **On-boarding management** • **Change management** • **Release management** • **ISO/IEC 27002** [6] **compliant**
		People	• Training of IT people to ETSI GS ISI 00x standards • Training for use case technical creation and management (IT Security experts and analysts involved in detection)	• **Idem (applicable to the SOC team)**
		Tools	• Broad scope of ISI security events detected • Various tools (including SIEM) used to detect all possible security incidents or events (measurement through all related indicators) • Calculate incident criticality (incident severity x asset sensitivity) through a link to asset sensitivity	• **Idem (applicable to the whole SOC information system + to the whole organization's perimeter monitoring)**
	3	Process	• Strong threat intelligence processes (collection of IoCs or use case management through exchanges between Governance or CSIRT and various detection units - Cf. exchanges of statistical state-of-the-art and benchmarking against these figures)	• **Idem (applicable especially to the SOC team for tweaking its monitoring tools)**
		People	• Tie critical incidents and related vulnerabilities to their business impact (for example by building Information Protection Plans) to enhance users' concern and motivation	• Not applicable
		Tools	• Advanced tools (Big Data, SkyBox-like, etc.) • Use of IoC (stemming from possibly Government Information Security agencies, or other sources)	• Idem (applicable to the whole organization's perimeter monitoring)

KPSIs	Levels (1 to 3)	Process/ People/ Tools	Applicable to the monitored perimeter of the whole organization	Applicable to SOC
6 **Security skills assess-ment and appro-priate training**	**1**	Process	• Training process to make employees aware of cyber risks, company security policy and main existing security measures (with focus on detection) • Check periodically the level of knowledge and perform gap analysis (with focus on detection, and especially human detection)	• **Idem (applicable to the SOC team)**
		People	• Periodic training as defined above	• **Idem (applicable to the SOC team)**
		Tools	• No tools	• **Idem**
	2	Process	• Check periodically the level of security policy application regarding human practices (hygiene and compliant human behaviour) • Measurement through possibly related ETSI GS ISI 001 [1], [2] relevant IDB and VBH indicators (to assess training and awareness effectiveness)	• **Idem (applicable to the SOC team for improving his detection skills)**
		People	• Training to ETSI GS ISI 00x standards • Make them aware of their behaviour through ad hoc sessions (based on accurate figures) • Human detection (spear-phishing, etc.)	• **Idem (applicable especially to the SOC team for improving his detection skills)**
		Tools	• See KPSI 5 (Continuous monitoring of human behaviours as regards cyber security)	• **Idem (applicable to the whole organization's perimeter monitoring)**
	3	Process	• Benchmarking against statistical state-of-the rat figures (to assess training and awareness effectiveness)	• **Idem (applicable to the SOC team for improving his detection skills)**
		People	• Tie critical incidents and related vulnerabilities to their business impact (for example by building Information Protection Plans) to enhance users' concern and motivation	• **Not applicable**
		Tools	• See KPSI 5 (Continuous monitoring of human behaviours as regards cyber security)	• **Idem (applicable to the whole organization's perimeter monitoring)**

KPSIs	Levels (1 to 3)	Process/ People/ Tools	Applicable to the monitored perimeter of the whole organization	Applicable to SOC
7 Cyber stress drills	**1**	Process	• Regulatory compliance • Requirement to organize periodically cyber stress drills, involving users and IT people (for example, spear-phishing)	• **Idem (applicable to the SOC team)**
		People	• Perform exercises to test organizational readiness to identify attacks (users & IT people)	• **Idem (applicable to the SOC team)**
		Tools	• No tools	• **No tools**
	2	Process	• Requirement to test the effectiveness of detection means (for example, by resting on ETSI GS ISI 005 [i.1])	• **Idem (applicable to the SOC team for assessing the effectiveness of its monitoring tools)**
		People	• Perform testing campaigns on various detection means and IT people (administrators, SOC, etc.)	• **Idem (applicable especially to the SOC team for assessing his detection skills)**
		Tools	• Specific tools simulating attacks in order to stimulate technical detection means	• **Idem (applicable to the SOC team for assessing the effectiveness of its monitoring tools)**
	3	Process	• Benchmarking against statistical state-of-the rat figures (to assess training and awareness effectiveness)	• **Idem (applicable to the SOC team for assessing the effectiveness of its monitoring tools)**
		People	• Tie critical incidents and related vulnerabilities to their business impact (for example by building Information Protection Plans) to focus the cyber stress drills on some special populations and to rationalize them	• **Not applicable**
		Tools	• See KPSI 5 (Continuous monitoring of human behaviours as regards cyber security)	• **Idem (applicable to the SOC team for assessing the effectiveness of its monitoring tools)**
8 Data loss preven-tion	**1**	Process	• Regulatory compliance	• Not applicable
		People	• Training on how to identify and classify his/her own sensitive information	• **Idem (applicable to the SOC team)**
		Tools	• No tools	• No tools
	2	Process	• Use of ETSI GS ISI 001 [1], [2] and ETSI GS ISI 002 [3] standards (security event classification, indicators, notification) to help identify all possible ways of data leak	• **Idem (applicable to the whole SOC information system)**
		People	• Training to ETSI GS ISI-00x standards • Make them aware o • f their behaviour through ad hoc sessions • (based on accurate figures) • Human detection (spear-phishing, etc.)	• **Idem (applicable to the SOC team)**
		Tools	• Various tools (including especially DLP) used to detect all possible ways of data leak (measurement through related IEX, IMF and IDB indicators) • Calculate incident criticality (incident severity x asset sensitivity) through a link to asset sensitivity	• **Idem (applicable to the whole SOC information system)**

KPSIs	Levels (1 to 3)	Process/ People/ Tools	Applicable to the monitored perimeter of the whole organization	Applicable to SOC
	3	Process	• Strong threat intelligence processes (use case management through exchanges between Governance or CSIRT and various detection units - Cf. exchanges of statistical state-of-the-art and benchmarking against these figures)	• Not applicable
		People	• Tie critical incidents and related vulnerabilities to their business impact (for example by building Information Protection Plans) to enhance users' concern and motivation about risks of data leak	• Not applicable
		Tools	• Not applicable	• Not applicable

Annex C (informative): Authors & contributors

The following people have contributed to the present document:

Rapporteur:
Paolo De Lutiis, Telecom Italia

Other contributors:
Gerard Gaudin, G²C, Chairman of ISG ISI

Herve Debar, Institut Telecom, Vice-Chairman of ISG ISI

Arnaud Fillette, Nokia, Secretary of ISG ISI

And in alphabetical order:

Christophe Blad, Oppida

Jan deMeer, SmartSpaceLabs.eu

Stephane Lemée, Airbus

Axel Rennoch, Fraunhofer Fokus

Philippe Saadé, ESI-Group

Julien Saugeot, BNP Paribas

History

Document history		
V1.1.1	May 2014	Publication
V1.1.2	June 2014	Publication
V1.2.1	January 2018	Publication