International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1208

(01/2014)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cyberspace security – Cybersecurity

A cybersecurity indicator of risk to enhance confidence and security in the use of telecommunication/information and communication technologies

Recommendation ITU-T X.1208

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	**X.1200–X.1229**
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1208

A cybersecurity indicator of risk to enhance confidence and security in the use of telecommunication/information and communication technologies

Summary

Recommendation ITU-T X.1208 describes a methodology for organizations to use cybersecurity indicators when computing a risk measure and it provides a list of potential cybersecurity indicators.

Recommendation ITU-T X.1208 is intended to help organizations that implement or operate a portion of the global infrastructure of information and communication technologies to evaluate their own cybersecurity capability and risk. These guidelines are intended to facilitate the decision-making process within organizations on how to lower their risks and how to identify where they could/should invest resources to improve their cybersecurity capabilities.

Recommendation ITU-T X.1208 does not propose the use of an index or a single indicator to express the cybersecurity capabilities of an organization.

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T X.1208	2014-01-24	17	11.1002/1000/11950

Keywords

Cybersecurity indicator, cybersecurity indicator of risk

[*] To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T X.1208

A cybersecurity indicator of risk to enhance confidence and security in the use of telecommunication/information and communication technologies

1 Scope

This Recommendation provides a guideline to assist organizations in the development, selection and identification of the data to be captured (based on selected indicators) and shows how this information can be used to compute a cybersecurity indicator of risk (CSIR). Note that an organization may generate a cybersecurity indicator of risk with respect to a specific set of cybersecurity indicators (CSI) while departments within an organization may also generate a cybersecurity indicator of risk with respect to their specific set of cybersecurity indicators (CSI). The purpose of the cybersecurity indicator is to allow for the evaluation of the level of cybersecurity competency at a particular point in time of an organization and, when this process is repeated at other points in time, it allows the status of an organization's cybersecurity programme's progress over time to be determined.

This Recommendation also provides a list of potential indicators and describes a methodology to be used when these cybersecurity indicators are used to compute a cybersecurity indicator of risk.

This Recommendation is intended to help organizations that implement or operate a portion of the global infrastructure of information and communication technologies to evaluate their own cybersecurity capabilities and calculate their cybersecurity indicator of risk. These guidelines are intended to facilitate the decision-making process within organizations on how to improve cybersecurity and how to lower their cybersecurity risks. Furthermore, these guidelines provide an indication of where organizations could/should invest resources to improve their cybersecurity.

This Recommendation is not to be used to generate a cybersecurity indicator of risk on a country-level basis. Furthermore, this Recommendation does not propose the use of an index or a single indicator to express the cybersecurity capabilities of an organization (see clause 6.1).

NOTE 1 – Comparisons of the calculated cybersecurity indicator of risk between organizations should not be made. This is because each organization or community is supposed to select what they deem to be an appropriate set of cybersecurity indicators for their organization. Furthermore, they are expected to develop their own measurement methodology and criteria to address their risks and concerns. In some cases subjective information, as opposed to objective data, may be used. Consequently, it is recommended that a cybersecurity indicator of risk for one organization should never be compared to that of another organization, as it is highly context dependent.

NOTE 2 – The indicators described in this Recommendation may not be compatible with those developed by other industry sectors due to the different purposes of those industries.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 audit [b-ITU-T X.800]: An independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in control, policy and procedures.

3.1.2 bot [b-ITU-T X-Sup.8]: An automated software program used to carry out specific tasks designed for malicious purposes. It is interchangeable with a robot.

3.1.3 cybersecurity [b-ITU-T X.1205]: Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following:

– Availability

– Integrity, which may include authenticity and non-repudiation

– Confidentiality.

3.1. 4 measurement [b-ENISA]: The act or the process of measuring, where the value of a quantitative variable in comparison to a (standard) unit of measurement is determined.

3.1.5 metric [b-ENISA]: A system of related measuring enabling quantification of some characteristic of a system, component or process. A metric is composed of two or more measures.

3.1.6 patch [b-ITU-T X.1206]: A broadly released fix for a product-specific, security-related vulnerability. A method of updating a file that replaces only the parts being changed, rather than the entire file.

3.1.7 personally identifiable information (PII) [b-ITU-T X.1252]: Any information a) that identifies or can be used to identify, contact, or locate the person to whom such information pertains; b) from which identification or contact information of an individual person can be derived; or c) that is or can be linked to a natural person directly or indirectly.

3.1.8 risk [b-ISO/IEC 27000]: Effect of uncertainty on objectives.

3.1.9 risk management [b-ISO/IEC 27000]: Coordinated activities to direct and control an organization with regard to risk.

3.1.10 security certificate [b-ITU-T X.810]: A set of security-relevant data issued by a security authority or a trusted third party, together with security information which is used to provide the integrity and data origin authentication services for the data.

3.1.11 security controls [b-NIST FIPS 199]: The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

3.1.12 security incident [b-ITU-T E.409]: A security incident is any adverse event whereby some aspect of security could be threatened.

3.1.13 spam [b-ITU-T X.1242]: The electronic information delivered from senders to recipients by terminals such as computers, mobile phones, telephones, etc., which is usually unsolicited, unwanted, and harmful for recipients.

3.1.14 threat [b-ISO/IEC 27000]: Potential cause of an unwanted incident, which may result in harm to a system or organization.

3.1.15 vulnerability [b-ITU-T X.1500]: Any weakness that could be exploited to violate a system or the information it contains. (Aligned with Annex A of [b-ITU-T X.800].)

3.1.16 weakness [b-ITU-T X.1500]: A shortcoming or imperfection that, while not itself being recognized as a vulnerability, could, at some point become a vulnerability, or could contribute to the introduction of other vulnerabilities.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 cybersecurity indicator: Any one of a collection of indicators used to calculate or measure the risk status of a cybersecurity capability or competence for an organization or community.

NOTE − Selected cybersecurity indicators are indicators that are selected because they are relevant, i.e., they are related in some fashion to the risk concerns.

3.2.2 cybersecurity indicator of risk: The result from implementing a methodology that computes a cybersecurity indicator of risk.

3.2.3 cybersecurity indicator suite: A selected set of cybersecurity indicators that will be used to compute a cybersecurity indicator of risk.

NOTE – There is not one unique cybersecurity indicator suite.

3.2.4 indicator: It is interchangeable with metric in clause 3.1.5.

3.2.5 information security management system: Part of the overall management system, based on a business risk approach to establish, implement, operate, monitor, review, maintain and improve information security, see clause 3.2.1 of [b-ISO/IEC 27000].

NOTE − The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

3.2.6 programme: A series of coordinated activities aimed at achieving a clear business objective.

3.2.7 program: A set of coded instructions that enables a machine, especially a computer, to perform a desired sequence of operations.

3.2.8 threat source: It is either the intent and method which makes use of an intentional exploitation of a vulnerability or the situation and method that may accidentally trigger a vulnerability.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AS	Autonomous System
BSA	Business Software Alliance
C&A	Certified and Accredited
CIS	Center for Internet Security
CSI	Cybersecurity Indicator

CSIR	Cybersecurity Indicator of Risk
CVE	Common Vulnerabilities and Exposures
CYBEX	Cybersecurity information Exchange
DB	Database
DDoS	Distributed Denial-of-Service
DHCP	Dynamic Host Configuration Protocol
DoS	Denial-of-Service
DNS	Domain Name System
GDP	Gross Domestic Product
ICT	Information and Communication Technology
ID	Identifier
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
ISMS	Information Security Management System
IT	Information Technology
PCA	Principal Components Analysis
PII	Personally Identifiable Information
SSL	Secure Socket Layer
TLS	Transport Layer Security
TTP	Trusted Third Party

5 Conventions

In this Recommendation, the term organization is intended to be interpreted in a broad sense. It is to be understood that a community should be considered as being included in the term organization. However, organization should never be considered to be equivalent to country.

6 Cybersecurity indicator

6.1 Introduction

Numerous efforts have been made to measure information and communication technology (ICT) performance, track progress and evaluate the impact of the use of ICTs on governments, operators, researchers and industries. Examples of these sector-specific indicators include the Global Cloud Computing Scorecard [b-BSA] and the security metrics published by the Center for Internet Security [b-CIS]. The indicators in this Recommendation are focused on some aspects of cybersecurity.

The cybersecurity indicator of risk described in this Recommendation consists of multiple cybersecurity indicators combined into a risk measure describing the current risk posture of cybersecurity capabilities and their effectiveness, as well as the efficiency of the implementation of security controls for an organization or a community.

There are two separate conditions under which a cybersecurity indicator of risk measure could be calculated, a self-evaluation of its cybersecurity capabilities or the collection of indicators calculated by some external third party organization. This Recommendation is intended for use for self-evaluation by organizations.

The indicators in this Recommendation may be selected by taking into account International Standards on the information security management system [b-ISO/IEC 27001], [b-ISO/IEC 27002], [b-ISO/IEC 27003], network security [b-ISO/IEC 27033-1], [b-ISO/IEC 27033-2], [b-ISO/IEC 27033-4] and other specifications [b-NIST SP 800-27], [b-NIST SP 800-30], [b-NIST SP 800-53]. The management related international standards allow organizations to design, implement and maintain a coherent set of policies, processes and systems to manage risks to its information assets, thus ensuring acceptable levels of information security risk. The network security related international standards define and describe the concepts associated with, and provides management guidance on, network security. The other specifications provide the basic concept of controls to mitigate the risks for the information asset and how to manage the risks in the organizations' ICT environment.

The indicators may be grouped according to business functions: incident management, vulnerability management, patch management, application security, configuration management, and a financial category.

This Recommendation does not propose the use of an index or a single indicator to express the cybersecurity capabilities of an organization. This is because the security of an organization is only as good as its weakest link and the use of an index to express the organization cybersecurity capabilities does not properly identify the potential impacts resulting from the weakest link. If a cybersecurity indicator of risk is presented as a single number it can mislead those who are expected to use the number, it could also create false expectations in those who are expected to use this number in decision-making processes. Specifically, when a number of indicators are aggregated and normalized to a single number (i.e., index), the existence and significance of cybersecurity weaknesses of an organization are no longer obvious. Thus it would be inappropriate to use this index to either indicate that the cybersecurity capabilities of an organization are satisfactory or to consider using this cybersecurity index to compare the cybersecurity capabilities of different organizations.

6.2 General principles for cybersecurity indicators

This clause describes the general principles that should be considered when developing cybersecurity indicators.

- Preference should be given to the use of a globally agreed-upon set of indicators when calculating a cybersecurity indicator of risk.
- Cybersecurity indicators should be selected so that they can be used to measure the current status of cybersecurity competence against threats or to measure the progress of an information security programme for an organization or a community.
- Cybersecurity indicators should be selected that allow for accuracy and confidentiality of the raw data which is to be collected and used as a basis for the computation of the cybersecurity indicator of risk.
- Collection processes must retain the integrity of the raw data, which is to be used as a basis for the computation of the cybersecurity indicator of risk.

- Preference should also be given to the use of indicators that may help policy makers measure the performance of information security policy implementation and track the progress of a cybersecurity programme.
- New additional indicators should be developed or existing ones should be updated in a timely fashion in response to fast changing ICT services and technologies.

6.3 Guidelines for selecting cybersecurity indicators

When selecting indicators which are to be used to calculate a cybersecurity indicator of risk, it may be necessary for an organization to select indicators that facilitate meeting the goals and objectives of an organization. For example, organizations can select indicators based on the business functions of high priority.

In particular, a cybersecurity indicator should allow for:

- the measurement of the major impact on performance results;
- its use to address issues at the system level, the programme level and both levels, as appropriate;
- the measurement of the progress in implementing a cybersecurity programme, specific security controls and associated cybersecurity policies and procedures;
- the measurement of aspects which would allow for the identification of effectiveness and efficiency in a cybersecurity programme;
- the measurement of the positive or negative impact of a cybersecurity programme on an organization's mission;
- the measurement of the status of cybersecurity policy performance, with the ability to obtain results at the system level, the programme level or both levels;
- the measurement of the positive and negative impacts on the daily life of users.

Furthermore, a cybersecurity indicator should be selected which would allow for the collection of raw data in an accurate and reliable manner. In the entire measurement process, there is a need for ensuring that raw data can be made available, the integrity of the data being used and that privacy protection of the data is available.

6.4 Classification of indicators

There are three types of indicators according to the nature of indicators: implementation, effectiveness/efficiency and impact. Implementation indicators are used to demonstrate the progress in implementing an information security programme, specific security countermeasures and associated security policies and procedures. They can be grouped into two sub-types: programme-level implementation indicators and system-level indicators. Examples of implementation indicators related to the system level include the percentage of information systems security personnel who have received security training.

Effectiveness/efficiency indicators can used to check if programme-level processes and system-level security controls are implemented properly, whether they are operating as intended and if they satisfy the desired goals and objectives. They deal with two aspects of security control implementation results: effectiveness and efficiency of the result, i.e., effectiveness addresses robustness and efficiency addresses timeliness. Examples of the effectiveness indicator include the percentage of information security incidents caused by improperly configured access control; examples of the efficiency indicators include the percentage of system components that undergo maintenance on schedule.

Impact indicators can be used to specify the impact of information security on the mission of an organization. They can be used to quantify the cost saving produced by the information security programme or the costs incurred in addressing the information security incident, the degree of public trust obtained by the information security programme, or other mission-related impacts of information security. Examples of the impact indicators include the percentage of an organization's information security expenditure to the total information system expenditure.

In addition, indicators can be grouped according to business functions: incident management, vulnerability management, patch management, application security, configuration security, financial metrics, data and network security, etc.

7 Cybersecurity indicator development process

7.1 Introduction

The suite of cybersecurity indicators should be regarded as a key toolkit that can be used to evaluate the validity of enforcing the information security policy and to figure out the current status of information security in an organization.

7.2 Methodology for the construction of a cybersecurity indicator suite

The development of a cybersecurity indicator suite is a complex task and it needs to be undertaken by highly skilled professionals with knowledge of economics, cybersecurity and statistics. The development of the list of cybersecurity indicators needs to be based on the context of the organization and the different aspects of the risk(s) to be measured.

A developer of cybersecurity indicators should take into account that a given indicator may experience significant variability, unlike indicators with large samples, due to the scarce nature of samples being measured, e.g., incidents, which may be observed in a limited scale. Consequently, macroscopic analysis would have to be applied with extreme care.

The following steps can be used for the development of a cybersecurity indicator suite and to make the information ready for use:

- identification of the key indicators to be selected and used to compute the cybersecurity indicator of risk;
- identification of data sources;
- dealing with missing observations;
- making the indicators comparable to each other;
- converting the indicators into risk measurement values;
- leveraging a collection of the risk measurement values.

7.2.1 Selection of indicators to construct a risk measure

The selection of indicators to construct a risk measure is dependent on what is being measured, as well as the practicality of collecting the raw data.

NOTE – Although it may not be currently practical to make a measurement, an indicator may still be given serious consideration for selection. It is possible that this process can be used to identify a new work activity to allow for the capture of data so that risk can be properly evaluated.

The number of indicators may depend on the mission and objectives of the organization or the type of technologies being used by the organization. The use of a broad selection of indicators (for example, 10 to 30 indicators) to construct the risk measure of a cybersecurity indicator of risk is recommended. Mixing subjective indicators with objective measurements can influence the validity of the resultant computation. Therefore, avoiding the use of subjective indicators in the construction of a cybersecurity indicator of risk is recommended. However, in some areas of risk management a subjective indicator may be necessary, so the disciplined definition of how to define a subjective indicator is critical. Once the indicators are selected, it may be desirable to group them into different categories according to their business functions such as incident management, vulnerability management, patch management, etc. This makes the indicators more manageable and renders the comparison more meaningful.

The detailed development procedure is described in clause 7.3.

7.2.2 Data sources

The extent to which the data are available for cybersecurity indicators may determine the number and quality of indicators for the computation of a cybersecurity indicator of risk. Excessive dependence on a single data source may lead to errors and omissions. Therefore, it is essential for the data to be checked against different sources before applying it to the computation of a cybersecurity indicator of risk.

7.2.3 Dealing with missing data

While collecting the risk measurements for a cybersecurity indicator, cases may be encountered where data is missing or unavailable. In these cases, either the data can be left blank – in which case the organization will assign no value for that indicator – or extrapolation can be used to estimate the missing data. Leaving the data blank could lead to exclusion of aspects of a cybersecurity indicator. Extrapolation may amplify the value of the data thereby leading to inflated computational results. There is a trade-off between extrapolation and omission, such trade-offs should take into consideration the value of data or importance of indicators. Possibly a sensitivity test should be undertaken to determine how sensitive the computed results are to fluctuations in the extrapolated value or if the blank data is replaced with an estimated value.

7.2.4 Transformation of the data

The transformation stage involves two steps: converting from absolute into relative values and converting relative values of indicators into a cybersecurity indicator of risk. Absolute values are generally made comparable by dividing by the overall number of items. Many indicators may already be supplied in their transformed state so this step may not be necessary.

7.3 Cybersecurity indicators' development process

The cybersecurity indicator development process involves selecting the indicators that are appropriate for the organization or community mission and objectives. This process consists of five steps: stakeholder interest identification; goals and objectives definition; information security policies, guidelines, and procedures review; information security implementation review; and indicator selection.

Step 1. Stakeholder interest identification: This involves identifying the relevant stakeholders and their interest. The primary stakeholders include the organization head, the chief information officer, the chief security officer, the information system security officer, the programme manager, the network administrator, the security engineers and the information system support personnel. The outcome of this step includes all interests in the information security measurement. Each stakeholder may request a different set of indicators representing their view within their area of responsibility.

Step 2. Goals and objectives definition: This involves identifying the goals and objectives of the information security performance. They may be expressed as policies, requirements, guidelines, and guidance. The goals and objectives of the information security programme can be derived from high-level goals and objectives to support the organization's mission.

Step 3. Information security policies, guidelines and procedures review: This involves describing the details of how security controls should be implemented in organization-specific policies and procedures.

Step 4. Information security implementation review: This involves reviewing existing indicators and relevant data repositories that can be used to derive new indicators.

Step 5. Indicator selection: This involves selecting and developing as appropriate three types of indicators described in clause 6.4. This step involves selecting a suite of indicators that track process implementation, efficiency/effectiveness and mission impact, and if required, developing as appropriate new indicators.

8 Potential cybersecurity indicators

This clause describes various potential cybersecurity indicators that have been identified as key indicators and that are applicable for the construction of a suite of cybersecurity indicators for an organization. The indicators can be classified into three categories: base indicators, recommended indicators and optional indicators. In addition, the indicators can be classified into three categories according to the nature of the indicator: implementation indicators, effectiveness/efficiency indicators and impact indicators. This Recommendation does not define the requirement level associated with any indicator. It is expected that organizations will identify a requirement level of each indicator, according to the security policy of an organization that they propose to use. In addition, organizations may, and are invited to, develop further indicators to address their own situation.

The indicators in this clause, see Tables 8-1 to 8-30, are designated for use by an organization, however, they can be applicable to a community by aggregating the indicators from organizations which are a component of a community.

There are indicators where for some instances a larger value is more desirable, i.e., bigger-better, while for some instances a smaller value is more desirable, i.e., smaller-better and there are other instances where it is not intuitive as to whether larger or smaller is better.

Table 8-1 – Indicator 1: Vulnerability management (programme level, bigger-better)

Field	Data
Indicator ID	Percentage of mitigated high-impact vulnerabilities.
Goal	The organization should address known vulnerabilities on time.
Indicator	Percentage of high-impact vulnerabilities that have been mitigated within organization-defined time frame after discovery.
Formula	(Total number of high-impact vulnerabilities mitigated on time/Total number of high-impact vulnerabilities identified) × 100.
Raw data	• Number of identified vulnerabilities during the organization-specified time period. (Note the number of identified high-impact vulnerabilities during the organization-specified time period must be calculated from the raw data.) • Number of mitigated high-impact vulnerabilities during the time period.
Frequency	• Weekly, monthly, quarterly, annually.
Type	• Effectiveness/efficiency.
Requirement level	
Applicable to	Organizations, (a community by aggregation).

Table 8-1 – Indicator 1: Vulnerability management (programme level, bigger-better)

Field	Data
Reference from CYBEX techniques	Recommendation ITU-T X.1521, Common vulnerability scoring system, [b-ITU-T X.1521] and Recommendation ITU-T X.1520, Common vulnerabilities and exposures [b-ITU-T X.1520].

Table 8-2 – Indicator 2: Audit log maintenance (system level, bigger-better)

Field	Data
Indicator ID	Percentage of end-point devices for which an audit log is maintained.
Goal	The organization should maintain a system audit log to investigate the inappropriate activities of the end points.
Indicator	Percentage of end-point devices for which an audit log is maintained.
Formula	(Total number of end-point devices with audit log/Total number of end-point devices) × 100.
Raw data	• Number of end-user devices for which an audit log is maintained by a centralized log server or an end-point device. • Total number of end-point devices.
Frequency	• Weekly, monthly, quarterly, annually.
Type	• Effectiveness/efficiency.
Requirement level	
Applicable to	Organizations, (a community by aggregation).
Reference from CYBEX techniques	

Table 8-3 – Indicator 3: Incident response (system level and programme level, bigger-better)

Field	Data
Indicator ID	Incident response.
Goal	The organization should report incidents on time for every incident category.
Indicator	Percentage of incidents reported within the required time frame per applicable category.
Formula	(Number of incidents reported on time/Total number of reported incidents) × 100, for every category.
Raw data	• Number of incidents reported within the organization-defined time frame. • Total number of incidents reported.
Frequency	• Weekly, monthly, quarterly, annually.
Type	• Effectiveness/efficiency.
Requirement level	
Applicable to	Organizations, (a community by aggregation).
Reference from CYBEX techniques	Recommendation ITU-T X.1544, Common attack pattern enumeration and classification [b-ITU-T X.1544].

Table 8-4 – Indicator 4: Mean time to mitigate vulnerabilities (system level and programme level, smaller-better)

Field	Data
Indicator ID	Mean time to mitigate vulnerabilities.
Goal	The indicator is designed to indicate the performance of the organization in addressing identified vulnerabilities. The less time required to mitigate vulnerabilities, the more likely an organization can react effectively to reduce the risk of exploitation of vulnerabilities.
Indicator	Mean-time-to-mitigate-vulnerabilities quantifies the average time to mitigate vulnerabilities identified in an organization.
Formula	Sum (Date_of_Completion_Mitigation – Date_of_Detection)/Count (Mitigated_Vulnerabilities)
Raw data	• Date of detection of vulnerabilities. • Date of mitigation of vulnerabilities. • Total number of detected vulnerabilities. • Total number of reported mitigated vulnerabilities.
Frequency	• Weekly, monthly, quarterly, annually.
Type	• Effectiveness/efficiency.
Requirement level	
Applicable to	Organizations, (a community by aggregation).
Reference from CYBEX techniques	Recommendation ITU-T X.1521, Common vulnerability scoring system, [b-ITU-T X.1521] and Recommendation ITU-T X.1520, Common vulnerabilities and exposures/[b-ITU-T X.1520].

Table 8-5 – Indicator 5: Security patch program deployment (system level, bigger-better)

Field	Data
Indicator ID	Security patch program.
Goal	End-point devices should deploy a security patch program to mitigate the vulnerabilities.
Indicator	Percentage of end-point devices that deploy the patch management system.
Formula	(Total number of end-point devices employing a security patch program/Total number of end-point devices) × 100.
Raw data	• Total number of end-point devices deploying the security patch program. • Number of end-point devices.
Frequency	• Weekly, monthly, quarterly, annually.
Type	• Effectiveness/efficiency.
Requirement level	
Applicable to	Organizations, (a community by aggregation).
Reference from CYBEX techniques	

Table 8-6 – Indicator 6: Mean time to patch (system level and programme level, smaller-better)

Field	Data
Indicator ID	Mean time to patch.
Goal	Mean time to patch quantifies the average time taken to deploy a patch for the organization's systems. The more quickly patches can be deployed, the less the mean time to patch is, and the less time the organization operates systems in a state known to be vulnerable.
Indicator	Average time taken to deploy a patch for the organization's systems.
Formula	Sum (Date_of_Installation – Date_of_Availability)/Count (Completed_patches).
Raw data	• Date of installation. • Date of availabilities. • Total number of completed patches.
Frequency	• Weekly, monthly, quarterly, annually.
Type	• Effectiveness/efficiency.
Requirement level	
Applicable to	Organizations, (a community by aggregation).
Reference from CYBEX techniques	

Table 8-7 – Indicator 7: Mean time to complete a configuration change (system level and programme level, smaller-better)

Field	Data
Indicator ID	Mean time to complete a configuration change.
Goal	Mean time to complete a configuration change quantifies the average time taken to complete a change in the organization's systems. The more quickly the change can be deployed, the less the mean time to patch is, and the less time the organization deploys in systems in a state known to be unstable.
Indicator	The average time taken to complete a configuration change in the organization's systems.
Formula	Sum (Date_of_Completion – Date_of_Submission)/Count (Completed_changes)
Raw data	• Date of completion. • Date of submission. • Total number of completed changes.
Frequency	• Weekly, monthly, quarterly, annually.
Type	• Effectiveness/efficiency.
Requirement level	
Applicable to	Organizations, (a community by aggregation).
Reference from CYBEX techniques	

Table 8-8 – Indicator 8: Risk assessment coverage (system level and programme level, bigger-better)

Field	Data
Indicator ID	Risk assessment coverage.
Goal	The organization should conduct risk assessment as much as possible for applications in the organization's systems.
Indicator	The percentage of business applications that have been subject to a risk assessment at any time.
Formula	Count (Applications_undergone_risk_assessment)/Count (Applications) × 100.
Raw data	• Number of applications that have undergone risk assessment. • Number of applications.
Frequency	• Weekly, monthly, quarterly, annually.
Type	• Effectiveness/efficiency.
Requirement level	
Applicable to	Organizations, (a community by aggregation).
Reference from CYBEX techniques	

Table 8-9 – Indicator 9: Malware detection and treatment program coverage (system level, bigger-better)

Field	Data
Indicator ID	Malware detection and treatment program
Goal	End-user devices should deploy an antivirus program for mitigating malware including viruses residing in them.
Indicator	Percentage of end-point devices deploying a malware detection and treatment program.
Formula	(Total number of end-point devices deploying a malware detection and treatment program/Total number of end-point devices) × 100.
Raw data	• Total number of end-point devices deploying an antivirus program. • Number of end-point devices.
Frequency	• Weekly, monthly, quarterly, annually.
Type	• Effectiveness/efficiency.
Requirement level	
Applicable to	Organizations, (a community by aggregation).
Reference from CYBEX techniques	

Table 8-10 – Indicator 10: Contingency planning coverage (programme level, bigger-better)

Field	Data
Indicator ID	Contingency plan testing.
Goal	The organization should conduct contingency plan testing for information systems.
Indicator	Percentage of information systems for which contingency plan testing has been conducted.
Formula	(Number of end-point systems for which contingency plan testing has been conducted/Total number of end-point systems) × 100.
Raw data	• Number of information systems for which contingency plan testing has been conducted. • Number of end-point systems.
Frequency	• Weekly, monthly, quarterly, annually.
Type	• Effectiveness/efficiency.
Requirement level	
Applicable to	Organizations, (a community by aggregation).
Reference from CYBEX techniques	

Table 8-11 – Indicator 11: Security assessment (programme level, bigger-better)

Field	Data
Indicator ID	Percentage of information systems with security assessment approvals.
Goal	An organization's end-point system should be certified and accredited prior to deployment to ensure an environment of comprehensive security and accountability for personnel, facilities and products.
Indicator	Percentage of new end-point systems that have completed certification and accreditation prior to their deployment.
Formula	(Number of information systems that have completed C&A/Total number of information systems) × 100.
Raw data	• Number of new end-point systems that have completed certification and accreditation. • Number of end-point systems.
Frequency	• Weekly, monthly, quarterly, annually.
Type	• Effectiveness/efficiency.
Requirement level	
Applicable to	Organizations, (a community by aggregation).
Reference from CYBEX techniques	

Table 8-12 – Indicator 12: Security pledge (programme level, bigger-better)

Field	Data
Indicator ID	Security pledge or code of conduct.
Goal	Employees who are authorized to access information systems should sign a security pledge before accessing the end-point system of an organization.
Indicator	Percentage of information system security personnel who have signed the security pledge.
Formula	(Number of personnel who are granted system access signing the rules of behaviour/Total number of personnel who are authorized to access end-point system) × 100.
Raw data	• Number of employees who are granted system access after signing the security pledge. • Number of employees who are granted system access.
Frequency	• Weekly, monthly, quarterly, annually.
Type	• Implementation.
Requirement level	
Applicable to	Organizations, (a community by aggregation).
Reference from CYBEX techniques	

Table 8-13 – Indicator 13: Remote access control with security gateway (system/programme level, bigger-better)

Field	Data
Indicator ID	Protected remote access points.
Goal	The organization should deploy a security gateway to enable protected remote access to protect its internal assets.
Indicator	Percentage of protected remote access points.
Formula	(Number of remote access points that use a security gateway/Total number of remote access points in an organization) × 100.
Raw data	• Number of protected remote access points that use a security gateway. • Number of protected remote access points.
Frequency	• Weekly, monthly, quarterly, annually.
Type	• Effectiveness/efficiency.
Requirement level	
Applicable to	Organizations, (a community by aggregation).
Reference from CYBEX techniques	

Table 8-14 – Indicator 14: Remote access control with security function for intrusion prevention or intrusion detection (system/programme level, bigger-better)

Field	Data
Indicator ID	Protected remote access points.
Goal	The organization should implement a security function for intrusion detection or prevention to protect the organization's internal assets.
Indicator	Percentage of protected remote access points.
Formula	(Number of remote access points that implement the security function with intrusion detection and prevention/Total number of remote access points) × 100.
Raw data	• Number of protected remote access points that implement the security function for intrusion detection or prevention. • Number of remote access points.
Frequency	• Weekly, monthly, quarterly, annually.
Type	• Effectiveness/efficiency.
Requirement level	
Applicable to	Organizations, (a community by aggregation).
Reference from CYBEX techniques	

Table 8-15 – Indicator 15: Wireless access control (system/programme level, bigger-better)

Field	Data
Indicator ID	Protected wireless access points.
Goal	The organization should provide protected wireless access points to protect the internal network from unauthorized access.
Indicator	Percentage of protected wireless access points.
Formula	(Number of protected wireless access points/Total number of wireless access points) × 100.
Raw data	• Number of protected wireless access points. • Number of wireless access points.
Frequency	Weekly, monthly, quarterly, annually.
Type	Effectiveness/efficiency.
Requirement level	
Applicable to	Organizations, (a community by aggregation).
Reference from CYBEX techniques	

Table 8-16 – Indicator 16: Personnel security (system level/programme level, bigger-better)

Field	Data
Indicator ID	Personnel security screening.
Goal	The organization should permit access to end-point systems by authorized personnel.
Indicator	Percentage of individuals screened before being granted access to the organization's end-point systems.
Formula	(Number of individuals screened/Total number of individuals with access) × 100.
Raw data	• Number of individuals screened. • Number of individuals.
Frequency	• Weekly, monthly, quarterly, annually.
Type	Implementation.
Requirement level	
Applicable to	Organizations, (a community by aggregation).
Reference from CYBEX techniques	

Table 8-17 – Indicator 17: Personally identifiable information (PII) protection (system/programme level, bigger-better)

Field	Data
Indicator ID	Percentage of protected sensitive personally identifiable information.
Goal	The organization should protect the organization's sensitive personally identifiable information in an encrypted way.
Indicator	Percentage of protected sensitive personally identifiable information.
Formula	(Number of sensitive personally identifiable information encrypted/Total number of personally identifiable information) × 100
Raw data	• Number of protected personally identifiable pieces of information. • Total number of personally identifiable pieces of information.
Frequency	• Weekly, monthly, quarterly, annually.
Type	Effectiveness/efficiency and implementation.
Requirement level	
Applicable to	Organizations, (a community by aggregation).
Reference from CYBEX techniques	

Table 8-18 – Indicator 18: Back-up data protection (system/programme level, bigger-better)

Field	Data
Indicator ID	Rate of integrity inspection of back-up data.
Goal	The organization should provide integrity protection for back-up data.
Indicator	Percentages of integrity-protected back-up data.
Formula	(Amount of integrity-protected back-up data/Total amount of back-up data) × 100.
Raw data	• Amount of integrity-protected back-up data. • Total amount of back-up data.
Frequency	• Weekly, monthly, quarterly, annually.
Type	Effectiveness/efficiency and implementation.
Requirement level	
Applicable to	Organizations, (a community by aggregation).
Reference from CYBEX techniques	

Table 8-19 – Indicator 19: Certified security management system (e.g., ISMS) coverage (system/programme level, bigger-better)

Field	Data
Indicator ID	Management system coverage.
Goal	The organization's end point should be covered by certified security management system (e.g., ISMS).
Indicator	Percentage of end-point systems covered by the certified security management system.
Formula	(Number of end-point systems covered by certified security management system (e.g., ISMS)/Total number of end-point systems) × 100.
Raw data	• Number of end-point systems covered by certified security management system (e.g., ISMS). • Total number of end-point systems.
Frequency	Weekly, monthly, quarterly, annually.
Type	Effectiveness/efficiency and implementation.
Requirement level	
Applicable to	Organizations, (a community by aggregation).
Reference from CYBEX techniques	

Table 8-20 – Indicator 20: Secure server deployment (system level/programme level, bigger-better)

Field	Data
Indicator ID	Secure server deployment.
Goal	The organization's network services should exchange information by the use of a secure tunnel for remote access.
Indicator	Percentage of network services that use a secure tunnel, e.g., TLS, SSL, or secure shell.
Formula	(Number of network services that use a secure tunnel/Total number of network services) × 100.
Raw data	• Number of network services that use a secure channel. • Total number of network services.
Frequency	• Weekly, monthly, quarterly, annually.
Type	Effectiveness/efficiency and implementation.
Requirement level	
Applicable to	Organizations, (a community by aggregation).
Reference from CYBEX techniques	
NOTE – The secure server (referred to in the indicator title) may be implemented in many ways to provide a secure tunnel between end-points. It includes the servers protected with SSL/TLS and a secure shell.	

Table 8-21 – Indicator 21: Spam receipt ratio (programme, smaller-better)

Field	Data
Indicator ID	Spam receipt ratio
Goal	The organization should use the spam filter to block spam e-mails from reaching the employees.
Indicator	Percentage of employees that have received more than the organization-defined number of spam e-mails during the defined time frame.
Formula	(Number of employees who have received a certain number of spam e-mails/Total number of employees) × 100.
Raw data	• Number of employees who have received spam e-mails exceeding the organization-defined numbers during the defined time frame. • Number of employees.
Frequency	• Weekly, monthly, quarterly, annually.
Type	Effectiveness/efficiency and implementation.
Requirement level	
Applicable to	Organizations, (a community by aggregation).
Reference from CYBEX techniques	

Table 8-22 – Indicator 22: Organization's awareness programme (bigger-better)

Field	Data
Indicator ID	Organization's awareness programme.
Goal	Employees should have participated in an awareness programme.
Indicator	Percentage of employees who have participated in an awareness programme.
Formula	(Number of employees who have participated in an awareness programme/Total number of employees) × 100.
Raw data	• Number of employees who have participated in an awareness programme. • Number of employees.
Frequency	• Weekly, monthly, quarterly, annually.
Type	Effectiveness/efficiency and implementation.
Requirement level	
Applicable to	Organizations, (a community by aggregation).
Reference from CYBEX techniques	

Table 8-23 – Indicator 23: Security training and education (programme level, bigger-better)

Field	Data
Indicator ID	Security training and education.
Goal	The organization's employees should complete the security training and education to respond adequately to security incidents.
Indicator	Percentage of employees who have completed the security training and education during the organization-defined time frame.
Formula	(Number of employees who completed security training and education/Total number of employees) × 100.
Raw data	• Number of employees who have completed training and education. • Number of employees.
Frequency	• Weekly, monthly, quarterly, annually.
Type	Impact/implementation.
Requirement level	
Applicable to	Organizations, (a community by aggregation).
Reference from CYBEX techniques	

Table 8-24 – Indicator 24: Cybersecurity role and responsibility (programme level, bigger-better)

Field	Data
Indicator ID	Role and responsibility.
Goal	The organization should recruit and organize personnel related to cybersecurity activities.
Indicator	Percentage of personnel related to cybersecurity activities.
Formula	(Number of personnel related to cybersecurity activities/Total number of IT personnel) × 100.
Raw data	• Number of personnel that are related to cybersecurity activities. • Total number of IT personnel.
Frequency	• Weekly, monthly, quarterly, annually.
Type	Impact/implementation.
Requirement level	
Applicable to	Organizations, (a community by aggregation).
Reference from CYBEX techniques	

Table 8-25 – Indicator 25: Malware infection (programme level and system level, smaller-better)

Field	Data
Indicator ID	Malware-infected end-point devices.
Goal	Employees' end-point devices should be protected from various malware.
Indicator	Percentage of employees' computers infected with virus or malware or compromised by attackers using hacking technologies.
Formula	(Total number of end-point devices infected with malware/Total number of end-point devices) × 100.
Raw data	• Number of end-point devices infected with virus or malware or compromised by attackers using hacking technologies. • Total number of end-point devices in an organization.
Frequency	• Weekly, monthly, quarterly, annually.
Type	Impact and effectiveness.
Requirement level	
Applicable to	Organizations, (a community by aggregation).
Reference from CYBEX techniques	

Table 8-26 – Indicator 26: Personally identifiable information leakage (programme level)

Field	Data
Indicator ID	Personally identifiable information leakage.
Goal	The organization should protect personally identifiable information from being leaked to outside organizations.
Indicator	Percentage of personally identifiable information units that are leaked during a defined time frame in the reported PII incident. NOTE – Developers of this indicator should define their own unit of PII.
Formula	(Number of personally identifiable information units that are leaked within the organization-specified time frame in the reported PII incident/Total number of personally identifiable information units) × 100.
Raw data	• Number of personally identifiable information units leaked within the organization-specific time frame in the reported PII incident. • Total number of personally identifiable information units.
Frequency	• Weekly, monthly, quarterly, annually.
Type	Impact.
Requirement level	
Applicable to	Organizations, (a community by aggregation).
Reference from CYBEX techniques	

Table 8-27 – Indicator 27: Security budget as a percentage of ICT budget (programme level)

Field	Data
Indicator ID	Percentage of organization's cybersecurity budget to ICT budget.
Goal	The organization should provide a budget for cybersecurity within a given target.
Indicator	Percentage of the organization's cybersecurity budget to ICT budget, the security budget is assumed to be included in the IT budget.
Formula	(Cybersecurity budget/Total ICT budget) × 100.
Raw data	• Amount of cybersecurity budget. • Amount of total ICT budget.
Frequency	• Weekly, monthly, quarterly, annually.
Type	Impact.
Requirement level	
Applicable to	Organizations, (a community by aggregation).
Reference from CYBEX techniques	

Table 8-28 – Indicator 28: Ratio of authorized device (bigger-better)

Field	Data
Indicator ID	Ratio of organization's authorized devices to all devices.
Goal	The organization should track/control/prevent/correct network access by devices (computers, network components, printers, anything with IP addresses) based on an asset inventory of which devices are allowed to connect to the network.
Indicator	Ratio of the organization's authorized devices to all devices.
Formula	(Number of authorized devices/Number of devices) × 100.
Raw data	• Number of authorized devices. • Number of devices.
Frequency	• Weekly, monthly, quarterly, annually.
Type	Impact.
Requirement level	
Applicable to	Organizations, (a community by aggregation).
Reference from CYBEX techniques	

Table 8-29 – Indicator 29: Ratio of authorized software (bigger-better)

Field	Data
Indicator ID	Ratio of organization's authorized software assets to all software assets.
Goal	The organization should track/control/prevent/correct installation and execution of software on computers based on an asset inventory of approved software.
Indicator	Ratio of the organization's authorized software assets to all software assets.
Formula	(Number of authorized software assets/Total number of software assets) × 100.
Raw data	• Number of authorized software assets. • Total number of software assets.
Frequency	• Weekly, monthly, quarterly, annually.
Type	Impact.
Requirement level	
Applicable to	Organizations, (a community by aggregation).
Reference from CYBEX techniques	Recommendation ITU-T X.1528, Common platform enumeration, [b-ITU-T X.1528] and [ISO/IEC 19770-2], Information technology – Software asset management – Part 2: Software identification tag [b-ISO/IEC 19770-2].

Table 8-30 – Indicator 30: Application software security (bigger-better)

Field	Data
Indicator ID	Ratio of organization's application software that are protected from major application-level software attacks (e.g., CWE top 25) to all application software assets.
Goal	The organization should detect and block an application-level software attack, and generate an alert or send e-mail to enterprise administrative personnel within 24 hours of detection and blocking.
Indicator	Ratio of the organization's application software that are protected from major application-level software attacks to all application software assets.
Formula	(Number of application software that are protected from major application-level software attacks/Number of all application software assets) × 100.
Raw data	• Number of application software that are protected from major application-level software attacks. • Number of all application software assets.
Frequency	• Weekly, monthly, quarterly, annually.
Type	Impact.
Requirement level	
Applicable to	Organizations, (a community by aggregation).
Reference from CYBEX techniques	Recommendation ITU-T X.1524, Common weakness enumeration, [b-ITU-T X.1524] and Recommendation ITU-T X.1544, Common attack pattern enumeration and classification [b-ITU-T X.1544].

Appendix I

Examples of indicators of information security risk measures and metrics

(This appendix does not form an integral part of this Recommendation.)

This appendix gives two example sets of indicators of information security risk measures and metrics that could be used to compute a cybersecurity indicator.

[b-NIST SP 800-55] provides potential candidates of risk measurements of the system level and programme level which can be grouped as follows:

- System-level risk measures:
  - access control
  - audit and accountability
  - identification and authentication
  - maintenance
  - risk assessment.
- Programme-level risk measures:
  - security expenditure, vulnerability management
  - awareness and training
  - certification, accreditation, and security assessments
  - configuration management
  - contingency planning
  - physical environment.
- Programme-level and system-level risk measures:
  - incident response
  - media protection
  - planning
  - personal security
  - system and communication acquisition
  - system and information integrity.

In addition, [b-NRI] by the World Economic Forum (WEF) provides several indicators while [b-WEF] uses a specific vendor's secure socket layer (SSL) certificate or transport layer security (TLS) certificate.

Appendix II

Classifying indicators by nature

(This appendix does not form an integral part of this Recommendation.)

In order to obtain wider acceptance of this Recommendation across organizations, it would be useful to identify minimum measurements that can be obtained and used without incurring significant cost.

For instance, Indicator 24 (Cybersecurity role and responsibility) in clause 8 could be an easily implementable indicator to start with, as its measurement only involves head-counting. Some of the other indicators require further introduction of other tools and/or databases in order to make those indicators measurable. For instance, Indicator 1 (vulnerability management) requires that tools and associated databases for vulnerability management be in place. Thus, organizations that wish to use this indicator must consider the benefit of making an investment to make this information available versus the cost to do so. Likewise, Indicator 2 requires that an ICT asset management function is already effective in an organization. Another class of indicators requires certain capabilities within an organization, in order to make them measurable. For instance, Indicator 4 (Mean time to mitigate vulnerabilities) requires that the date of occurrence is known, which would be difficult without auditing and analysis capabilities.

This appendix describes a classification of indicators by their nature: those that are easily measurable, those measurable by using tools and/or databases that would normally exist in an organization and those measurable if the organization decided to implement enhanced measurement capabilities.

Table II.1 – Classification of indicators by nature

Nature of indicators	Indicator number	Indicator ID
Easily measurable indicators	Indicator 12: Security pledge	Security pledge or code of conduct
	Indicator 16: Personnel security	Personnel security screening
	Indicator 24: Cybersecurity role and responsibility	Cybersecurity role and responsibility
	Indicator 27: Security budget as a percentage of ICT budget	Percentage of organization's information security budget to ICT budget
Indicators that can be measured with the deployment of measurement tools and/or databases that would normally exist in an organization	Indicator 1: Vulnerability management	Percentage of mitigated high vulnerabilities
	Indicator 2: Audit log maintenance	Percentage of end-point devices for which an audit log is maintained
	Indicator 3: Incident response	Incident response
	Indicator 8: Risk assessment coverage	Risk assessment coverage
	Indicator 9: Malware detection and treatment program coverage	Malware detection and treatment program coverage
	Indicator 21: Spam receipt ratio	Spam receipt ratio
	Indicator 22: Organization's	Organization's awareness programme

Table II.1 – Classification of indicators by nature

Nature of indicators	Indicator number	Indicator ID
	awareness programme	
	Indicator 23: Security training and education	Security training and education
	Indicator 28: Ratio of authorized device	Ratio of organization's authorized devices to all devices
	Indicator 29: Ratio of authorized software	Ratio of organization's authorized software assets to all software assets
	Indicator 30: Application software security	Ratio of organization's application software that are protected from major application-level software attacks (e.g., CWE top 25) to all application software assets
Indicators that probably require further development of measurement capabilities within an organization	Indicator 4: Mean time to mitigate vulnerabilities	Mean time to mitigate vulnerabilities
	Indicator 5: Security patch program deployment	Security patch program
	Indicator 6: Mean time to patch	Mean time to patch
	Indicator 7: Mean time to complete a configuration change	Mean time to complete a configuration change
	Indicator 10: Contingency planning coverage	Contingency plan testing
	Indicator 11: Security assessment	Percentage of information systems with security assessment approvals
	Indicator 13: Remote access control with security gateway	Protected remote access points
	Indicator 14: Remote access control with security function for intrusion prevention or intrusion detection	Protected remote access points
	Indicator 15: Wireless access control	Protected wireless access points
	Indicator 17: Personally identifiable information (PII) protection	Percentage of protected sensitive personally identifiable information
	Indicator 18: Back-up data protection	Rate of integrity inspection of back-up data
	Indicator 19: Certified security management system coverage	Management system coverage
	Indicator 20: Secure server deployment	Secure server deployment
	Indicator 25: Malware infection	Malware-infected end-point devices

Table II.1 – Classification of indicators by nature

Nature of indicators	Indicator number	Indicator ID
	Indicator 26: Personally identifiable information leakage	Personally identifiable information leakage

Appendix III

Experimental indicators

(This appendix does not form an integral part of this Recommendation.)

This appendix describes a number of experimental indicators, (see Tables III.1 to III.6) which may be applicable for use by organizations.

Table III.1 – Indicator III-1: Mean time to incident discovery (system level and programme level, smaller-better)

Field	Data
Indicator ID	Mean time to incident discovery.
Goal	The organization should detect incidents as soon as they happen and measure the mean-time-to-incident-discovery to prove effectiveness of the organization in detecting security incidents. In general, the faster an organization can detect an incident, the less damage it is likely to incur.
Indicator	Average amount of time, in hours, that elapsed between the occurrence time and discovery time for a given set of incidents.
Formula	Sum (Time_of_Discovery – Time_of_Occurence)/Count (incidents).
Raw data	Discovery time of incidents, for every incident. Total number of reported incidents.
Frequency	Weekly, monthly, quarterly, annually.
Type	Effectiveness/efficiency.
Requirement level	
Applicable to	Organizations, (a community by aggregation).
Reference from CYBEX techniques	

Table III.2 – Indicator III-2: Link redundancy (system, bigger-better)

Field	Data
Indicator ID	Percentage of network links with redundancy.
Goal	The organization should construct a redundancy of links within the main network to guarantee the availability and continuity of the organization's services.
Indicator	Percentage of network links with redundancy.
Formula	(Number of links with redundancy/Total number of network links) × 100.
Raw data	Number of redundancy links for routers, domain name system (DNS), dynamic host configuration protocol (DHCP), firewall, or database (DB). Number of links without redundancy.
Frequency	Weekly, monthly, quarterly, annually.
Type	Effectiveness/efficiency.

Field	Data
Requirement level	
Applicable to	Organizations, (a community by aggregation).
Reference from CYBEX techniques	

Table III.3 – Indicator III-3: Bot infection (system level, smaller-better)

Field	Data
Indicator ID	Percentage of end-point devices infected with bot.
Goal	The organization should reduce the presence of bots in the network of an organization.
Indicator	Percentage of end-point devices infected with known bots in an organization. The organization is assumed to employ the bot infection detection system.
Formula	(Total number of end-point devices infected with known bots/Total number of end-point devices) × 100.
Raw data	Number of end-point devices infected with bots.
Frequency	Weekly, monthly, quarterly, annually.
Type	Effectiveness/efficiency.
Requirement level	
Applicable to	Organizations, (a community by aggregation).
Reference from CYBEX techniques	

Table III.4 – Indicator III-4: Distributed denial-of-service (DDoS) measures (system level, smaller-better)

Field	Data
Indicator ID	DDoS measures.
Goal	The organization should protect its end-point systems against DDoS (or denial-of-service (DoS)) attacks for the organization-defined time frame.
Indicator	Percentage of organization's systems that are unavailable for a specified time duration due to DDoS (DoS) attacks.
Formula	(Number of organization's systems that are unavailable for a specified time duration due to DDoS attacks during the organization-specified period/Total number of websites that an organization has) × 100.
Raw data	Number of websites that are unavailable for a specified time duration due to DDoS attacks within the organization-defined time frame. Total number of websites.
Frequency	Weekly, monthly, quarterly, annually.

Table III.4 – Indicator III-4: Distributed denial-of-service (DDoS) measures (system level, smaller-better)

Field	Data
Type	Effectiveness/efficiency.
Requirement level	
Applicable to	Organizations, (a community by aggregation).
Reference from CYBEX techniques	

Table III.5 – Indicator III-5: Audit log performance (system level and programme level, bigger-better)

Field	Data
Indicator ID	Percentage of computer security incidents for which an audit log has captured observable traces.
Goal	The organization should assess the effectiveness of audit logs.
Indicator	Percentage of computer security incidents for which an audit log has captured observable traces.
Formula	(Reported incidents that left observable traces in logs/Total number of reported incidents) × 100.
Raw data	Number of reported incidents for which observable traces have been found in audit logs. (Either centralized log or logs aggregated from end-points) Total number of reported incidents.
Frequency	Weekly, monthly, quarterly, annually.
Type	Effectiveness/efficiency.
Requirement level	
Applicable to	Organizations, (a community by aggregation).
Reference from CYBEX techniques	

Table III.6 – Indicator III-6: Incident mitigation performance (system level and programme level, bigger-better)

Field	Data
Indicator ID	Percentage computer security incidents located within C&A systems (end-points or groups of end-points).
Goal	The organization should assess the effectiveness of C&A procedures.
Indicator	Percentage of computer security incidents located within C&A systems.
Formula	(Reported incidents located within C&A systems/Total number of reported incidents) × 100.
Raw data	Number of reported incidents that were located in C&A systems Total number of reported incidents.
Frequency	Weekly, monthly, quarterly, annually.
Type	Effectiveness/efficiency.
Requirement level	
Applicable to	Organizations, (a community by aggregation).
Reference from CYBEX techniques	

Bibliography

[b-ITU-T E.409] Recommendation ITU-T E.409 (2004), *Incident organization and security incident handling: Guidelines for telecommunication organizations*.

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991) | ISO/IEC 7498-2 (1989), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.810] Recommendation ITU-T X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.

[b-ITU-T X.1205] Recommendation ITU-T X.1205 (2008), *Overview of cybersecurity.*

[b-ITU-T X.1206] Recommendation ITU-T X.1206 (2008), *A vendor-neutral framework for automatic notification of security related information and dissemination of updates*.

[b-ITU-T X.1242] Recommendation ITU-T X.1242 (2009), *Short message service (SMS) spam filtering system based on user-specified rules*.

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions*.

[b-ITU-T X.1500] Recommendation ITU-T X.1500 (2011), *Overview of cybersecurity information exchange*.

[b-ITU-T X.1520] Recommendation ITU-T X.1520 (2011), *Common vulnerabilities and exposures*.

[b-ITU-T X.1521] Recommendation ITU-T X.1521 (2011), *Common vulnerability scoring system*.

[b-ITU-T X.1524] Recommendation ITU-T X.1524 (2012), *Common weakness enumeration*.

[b-ITU-T X.1528] Recommendation ITU-T X.1528 (2012), *Common platform enumeration*.

[b-ITU-T X.1544] Recommendation ITU-T X.1544 (2013), *Common attack pattern enumeration and classification*.

[b-ITU-T X-Sup.8] ITU-T X-series Recommendations − Supplement 8 (2010), *ITU-T X.1205 − Supplement on best practices against botnet threats*.

[b-ISO/IEC 19770-2] ISO/IEC 19770-2:2009, *Information technology – Software asset management – Part 2: Software identification tag*.

[b-ISO/IEC 27000] ISO/IEC 27000:2012, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/IEC 27001] ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management systems – Requirements*.

[b-ISO/IEC 27002] ISO/IEC 27002:2005, *Information technology – Security techniques – Code of practice for information security management*.

[b-ISO/IEC 27003] ISO/IEC 27003:2010, *Information technology – Security techniques – Information security management system implementation guidance*.

[b-ISO/IEC 27033-1] ISO/IEC 27033-1:2009, *Information technology – Security techniques – Network security – Part 1: Overview and concepts*.

[b-ISO/IEC 27033-2] ISO/IEC 27033-2:2012, *Information technology – Security techniques – Network security – Part 2: Guidelines for the design and implementation of network security*.

[b-ISO/IEC 27033-4] ISO/IEC 27033-4: 2014, *Information technology – Security techniques – Network security – Part 4: Securing communications between networks using security gateways*.

[b-NIST SP 800-27] NIST SP 800-27 Revision A (2004), *Engineering Principles for IT Security (A Baseline for Achieving Security), Revision A*.

[b-NIST SP 800-30] NIST SP 800-30 Revision 1 (2012), *Guide for Conducting Risk Assessments*.

[b-NIST SP 800-53] NIST SP 800-53 Revision 4 (2013), *Security and Privacy Controls for Federal Information Systems and Organizations*.

[b-NIST SP 800-55] NIST SP 800-55 Revision 1 (2008), *Performance Measurement Guide for Information Security*.

[b-NIST FIPS 199] NIST FIPS PUB 199 (2004), *Standards for Security Categorization of Federal Information and Information Systems*.

[b-ENISA] ENISA (V6_2, 2011), *Measurement Frameworks and Metrics for Resilient Networks and Services: technical report.*

[b-NRI] World Economic Forum (2013), *Networked Readiness Index*.

[b-WEF] World Economic Forum (2013), *Secure Internet servers*. (Sources: The World Bank, World Development Indicators Online; national sources).

[b-CIS] Center for Internet Security (2010), *The CIS security metrics*.

[b-Nelson] Nelson, C. E. (2010), *Security metrics: An overview,* ISSA Journal, Vol.8, No. 8.

[b-BSA] BSA (2013), *BSA Global Cloud Computing Scorecard*. http://cloudscorecard.bsa.org/2013/

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2014