国 际 电 信 联 盟

ITU-T

X.1208

(01/2014)

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

网络空间安全 – 网络安全

增强使用电信/信息通信技术的信心和安全性的网络安全风险指标

ITU-T X.1208 建议书

国际电信联盟

ITU-T X 系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
报文处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定安全	X.1080–X.1099
安全应用和服务	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
网页安全	X.1140–X.1149
安全协议	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
网络安全	**X.1200–X.1229**
反垃圾信息	
身份管理	X.1250–X.1279
安全应用和服务	X.1230–X.1249
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1339
网络安全信息交换	
网络安全概述	X.1500–X.1519
脆弱性/状态信息交换	X.1520–X.1539
事件/事故/探索法信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
探索法和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589
云计算安全	
云计算安全概述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和导则	X.1640–X.1659
云计算安全的部署	X.1660–X.1679
其他云计算安全	X.1680–X.1699

欲了解更详细信息，请查阅 ITU-T建议书目录。

ITU-T X.1208 建议书

增强使用电信/信息通信技术的信心和安全性的网络安全风险指标

摘要

ITU-T X.1208建议书为机构介绍了一种网络安全指标的使用方法，以帮助后者量化网络风险，并就潜在的网络安全指标提供了一份清单。

ITU-T X.1208建议书旨在帮助实施或操作部分信息通信技术全球基础设施的各类机构评估其自身的网络安全能力和风险。这些导则旨在促进机构内部在以下方面的决策流程：如何降低风险以及为加强网络安全可/应在何处投入资源等。

ITU-T X.1208建议书不建议使用一个指数或一项单一指标来表达机构的网络安全能力。

历史

版本	建议书	批准	研究组	唯一ID*
1.0	ITU-T X.1208	2014-01-24	17	11.1002/1000/11950

关键词

网络安全指标、网络安全风险指标

* 要访问该建议书，请在网页浏览器的地址栏输入URL http://handle.itu.int/，然后输入建议书的唯一ID。例如，http://handle.itu.int/11.1002/1000/11830-en.

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定 ITU-T 各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA 第 1 号决议规定了批准建议书须遵循的程序。

属 ITU-T 研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其他一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其他机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T X.1208 建议书

增强使用电信/信息通信技术的信心和安全性的网络安全风险指标

1 范围

本建议书提供的导则有助于机构制定、选择和确定需要捕获的数据（根据选定的指标），并说明了利用此类信息来计算网络安全风险指标（CSIR）的方法。请注意，机构可可能会针对一组特定的网络安全指标（CSI）来产生一项网络安全风险指标，而机构内的部门也可能会针对一组特定的网络安全指标（CSI）来产生一项网络安全风险指标，网络安全指标旨在对机构在特定时间点的网络安全能力水平进行评估，当在其他时间点重复此过程时，它允许随着时间的推移来确定机构的网络安全项目的进展状况。

本建议书还提供了一系列潜在指标的清单，并介绍了当这些网络安全指标被用于计算网络安全风险指标时可采用的一种方法。

本建议书旨在帮助实施或运行部分全球信息通信技术基础设施的机构评估其自身网络安全能力及计算其网络安全风险指标。本建议所述导则则旨在方便机构就如何改善网络安全及如何降低其网络安全风险做出决策。此外，这些导则亦可说明机构可/应在哪些环节投入资源，以提高其网络安全。

不应使用本建议书在国家层面产生网络安全风险指标。此外，本建议书不建议使用一个指数或一项单一指标来表达机构的网络安全能力（见第6.1段）。

注1 – 不应在机构之间就网络安全风险指标的计算结果进行比较，原因是每一机构或社区均应选择其认为适合所在机构的一组网络安全指标。此外，机构应自行开发测量方法和标准，以解决其风险隐忧。在某些情况下，亦可使用相对于目标数据的主观信息。因此，不建议将某一机构的网络安全风险指标与其他机构进行比较，原因是该指标与环境高度相关。

注2 – 本建议书所述指标可能与其他行业确定的指标不相兼容，原因是这些行业各有其不同目标。

2 参考资料

无。

3 术语

3.1 他处定义的术语

本建议书使用了下列它处定义的术语：

3.1.1 审计[b-ITU-T X.800]：为测试系统控制适用性而对系统记录和活动进行的独立审查与检验，以确保符合既定的政策和运作程序，检查安全违规现象并就提出的控制、政策和程序修改提出建议。

3.1.2 机器人（bot）[b-ITU-T X-Sup.8]：一种用于执行具体的恶意任务的自动软件程序。它可与机器人（robot）一词互换使用。

3.1.3 网络安全[b-ITU-T X.1205]：网络安全涉及用以保护网络环境和机构及用户资产的各种工具、政策、安全理念、安全保障、导则、风险管理方式、行动、培训、最佳做法、保证和技术。机构和用户的资产包括相互连接的计算装置、人员、基础设施、应用、服务、电信系统以及在网络环境中全部传送和/或存储的信息。网络安全工作旨在确保防范网络环境中的各种安全风险，实现并维护机构和用户资产的安全特性。网络安全的总体目标包括下列各个方面：

– 可用性
– 完整性（其中可以包括真实性和不可否认性）
– 机密性。

3.1.4 测量[b-ENISA]：测定与衡量单位（标准）对比的量化变量值的测量行为或过程。

3.1.5 度量表[b-ENISA]：能够对某些方法、组件或程序的特性进行量化的相关测量方法。度量表由两种或更多测量标准构成。

3.1.6 补丁[b-ITU-T X.1206]：为特定产品和安全漏洞而广泛发布的修正软件。一种仅对发生变化的部分进行替换而非替换整个文件的方法。

3.1.7 个人可识别信息（PII）[b-ITU-T X.1252]：任何信息a) 识别或能用于识别、联系或定位与该信息相关的个人；b) 从这些信息能够获得某个人的识别或联系信息；或c) 该信息能够直接或间接与一个自然人相关联。

3.1.8 风险[b-ISO/IEC 27000]：不确定性对目标的影响。

3.1.9 风险管理[b-ISO/IEC 27000]：指导与控制机构风险的协调行动。

3.1.10 安全证书[b-ITU-T X.810] ：安全机构或可信第三方发布的一系列与安全相关的数据，并附带用于为数据提供完整性和数据来源认证服务的安全信息。

3.1.11 安全控制[b-FIPS 199]：供信息系统保护系统及其信息保密性、完整性和可用性使用的管理、运行和技术控制（如防护措施或对策）。

3.1.12 安全事件[b-ITU-T E.409]：安全事件是所有使安全的某个方面受到威胁的有害事件。

3.1.13 垃圾信息[b-ITU-T X.1242]：通过计算机、移动电话、电话等终端由发送方向接收方发送的电子信息，该信息对接收方来说通常是未经请求、无用和有害的。

3.1.14 威胁[b-ISO/IEC 27000]：可能对系统或机构造成伤害的有害事件的潜在起因。

3.1.15 漏洞[b-ITU-T X.1500]：所有可能被用来破坏系统或它所含信息的缺陷。

3.1.16 缺陷[b-ITU-T X.1500]：虽然缺点或缺陷本身并不被视为漏洞，但它们可以在某个时候成为一个漏洞或可能诱发其他漏洞。

3.2 本建议书定义的术语

本建议书定义了下列术语：

3.2.1 网络安全指标：用于计算或衡量机构、社区网络安全能力状况的一系列指标。

注 – 被选定的网络安全指标是因具有相关性而被选定的指标，即它们均以某种方式涉及到风险隐忧。

3.2.2 网络安全风险指标：因实施计算网络安全风险指标的方法而产生的结果。

3.2.3 网络安全指标组：被用来计算网络安全风险指标的一组被选定的网络安全指标。
注 – 不存在唯一的网络安全指示组。

3.2.4 指标：可与第3.1.6段中的度量表互换使用。

3.2.5 信息安全管理系统：整个管理系统的一部分，基于业务风险方法来建立、实施、运行、监控、审查、维护和改进信息安全，见[b-ISO/IEC 27000]的第3.2.1段。
注 – 管理系统包括组织结构、政策、规划活动、职责、惯例、程序、过程和资源。

3.2.6 项目：实现明确商业目标的系列协调行动。

3.2.7 程序：能够使机器，尤其是计算机，执行既定运作顺序的一套加密指令。

3.2.8 威胁来源：一种有意利用漏洞的企图和方法，或可不慎触发漏洞的情况和方法。

4 缩写词和首字母缩略语

本建议书使用以下缩写词和首字母缩略语：

AS 自主系统
BSA 商业软件联盟
C&A 认证与认可
CIS 互联网安全中心
CSI 网络安全指标

CSIR 网络安全风险指标

CVE 常见弱点与漏洞

CYBEX 网络安全信息交换

DB 数据库

DDoS 分布式拒绝服务

DHCP 动态主机设置协议

DoS 拒绝服务

DNS 动态名称系统

GDP 国内生产总值

ICT 信息通信技术

ID 标识符

IDS 入侵检测系统

IP 互联网协议

IPS 入侵防范系统

ISMS 信息安全管理系统

IT 信息技术

PCA 主要组件分析

PII 个人可识别信息

SSL 安全套接层协议

TLS 传输层安全

TTP 可信的第三方

5 惯例

在本建议书中，术语“机构”的内涵为广义。“社区”应被视为包括在术语“机构”中。但是，“机构”不应被视为等同于国家。

6 网络安全指标

6.1 引言

为衡量信息通信技术（ICT）的效果、跟踪进展和评估ICT的使用对政府、运营商、研究人员和行业的影响，人们做出了巨大努力。这些针对行业的示例包括全球云计算记分卡[b-BSA]和互联网安全中心发布的安全度量表[b-CIS]。本建议书所述指标侧重于网络安全的某些方面。

本建议书所述的网络安全风险指标包括合并为一个风险指标的多种网络安全指标，旨在说明一个机构或社区的网络安全风险能力及其有效性，以及实施安全控制的效率。

计算网络安全风险指标有两个互不相关的条件：对自身网络安全能力的自我评估，或由一些外部第三方机构算得的一系列指标。本建议书由机构在做自我评估时加以使用。

在选择本建议书所述指标时，可考虑到以下有关信息安全管理系统的国际标准：[b-ISO/IEC 27001]、[b-ISO/IEC 27002]、[b-ISO/IEC 27003]；有关网络安全的国际标准：[b-ISO/IEC 27033-1]、[b-ISO/IEC 27033-2]、[b-ISO/IEC FDIS 27033-4]，以及其他规范：[b-SP 800-27]、[b-SP 800-30]、[b-SP 800-53]。与管理相关的国际标准有助于机构设计、实施和维护一系列连贯一致的政策、程序和系统，以管理其信息资产面临的风险，从而确保信息安全风险处于可令人接受的程度。与网络安全相关的国际标准确定并阐述与网络安全相关的理念，同时提供有关网络安全的管理指南。其他规范提供的基础性监控理念有助于降低信息资产风险，并说明在机构的信息通信技术环境中如何对风险加以管理。

可根据事件管理、漏洞管理、补丁管理、应用安全、配置管理和财务类别等业务职能划分指标。

本建议书不建议使用指数或单一指标来说明机构的网络安全能力，原因是机构的安全性强弱取决于其最薄弱环节，使用指数来说明机构的网络安全能力将无法如实确定最薄弱环节所产生的潜在影响。如仅以数字来表示网络安全风险指标，则它或会误导此类数字的预期使用者，也可能会在后者的决策过程中引发不实错觉。具体而言，当多个指标被归一成一个数字（即指数）时，机构的网络安全缺陷便不再具有明显的存在意义。因此，不宜使用指数来说明机构在网络安全能力方面的满意度，亦不宜使用此类网络安全指数来在不同机构的网络安全能力之间加以比较。

6.2 网络安全指标的一般原则

本段介绍了在制定网络安全指标时应考虑的一般原则。

- 在计算网络安全风险指标时，应优先采用全球认可的指标；
- 应选择网络安全指标，以将其用于测量机构或社区应对威胁的网络安全能力现状或信息安全项目的进展情况；
- 所选择的网络安全指标应确保原始数据的准确性和保密性，所采集的原始数据是计算网络安全风险指标的基础；
- 采集过程必须保留原始数据的完整性，此类数据是网络风险指标的基础；

- 同时，亦应优先采用可能有助于决策者衡量信息安全政策落实和跟踪网络安全项目进展的指标；
- 针对快速变化的ICT服务和技术，应及时制定新的附加指标或更新现有指标。

6.3 选择网络安全风险指标的导则

在选择用于计算网络安全风险的指标时，可能需要一个机构选择有助于实现机构宗旨和目标的指标。例如，各机构可根据高度优先的业务职能选择指标。

须特别指出，网络安全指标应能够：

- 测量对效果的重大影响；
- 用指标在系统级、程序级及酌情在两者结合级来解决问题；
- 测量网络安全项目、具体安全控制和相关安全政策和程序的落实进展；
- 测量网络安全项目中可确定效能和效率的各方面情况；
- 测量网络安全项目对机构使命带来的积极或消极影响；
- 测量网络安全政策效果的状态，以便在系统级、项目级或两者结合级取得成果；
- 测量对用户日常生活带来的积极和消极影响。

此外，在选择网络安全指标时，应确保原始数据的采集过程准确而可靠。在整个测量过程中，需要确保能够提供原始数据，所使用的原始数据应确保完整，并对数据隐私提供相应的保护。

6.4 指标的分类

指标可根据其性质分为三类：实施、效能/效率和影响。实施指标被用于显示实施信息安全项目、具体安全对策和相关安全策略及程序的进展。它们又可分为两个子类型：计划及实施指标和系统级指标。涉及系统级实施指标的示例包括接受安全培训的信息系统安全人员的比例。

效能/效率指标可用于检查是否妥善实施了项目级程序和系统级安全控制，它们是否按计划运行，并是否达到了既定的目标和目的。它们涉及两个方面的安全控制实施结果：结果的效能和效率，效能涉及强健性，而效率涉及及时性。有效性指标的示例包括不良配置接入控制引发的信息安全事件的比例；效率指标的示例包括得到及时维护的系统组件的百分比。

影响指标可被用于说明信息安全对一机构或社区使命的影响。它们可被用于量化信息安全项目带来的成本节约，或解决信息安全事件生成的费用，信息安全项目获得的公众信任，或其他与任务相关的信息安全影响。影响指标的示例包括机构信息安全支出占信息系统总支出的百分比。

此外，指标可按事件管理、漏洞管理、补丁管理、应用安全、配置安全、财务度量表、数据和网络安全等进行业务职能划分。

7 网络安全指标制定程序

7.1 引言

网络安全指标套件可被视为一重要的工具包，用于强化信息安全策略的有效性，并了解一机构的信息安全现状。

7.2 网络安全指标套件的构建方法

构建网络安全指标套件是一项复杂工作，需要具有经济、网络安全和统计数据知识的高级专业技术人员承办。制定一系列网络安全指标需以机构所处环境为基础，并对不同风险方面做出衡量。

网络安全指标的开发人员应考虑到一个给定指标可能会出现显著的变化，这不同于具有大样本的指标，原因是所测样本（如事件）具有稀缺性，此类样本可能要在一个有限范围内进行观察。因此，必须以极其审慎的态度进行宏观分析。

可通过下列步骤构建网络安全指标套件及提供相关信息：

- 选择并确定可用于计算一系列网络安全风险指标的关键指标；
- 确定数据源；
- 解决观察缺失问题；
- 使指标具有互比性；
- 将指标转换为风险衡量值；
- 充分利用一系列风险衡量值。

7.2.1 对构建风险衡量标准的指标的选择

对构建风险衡量标准的指标的选择，取决于测量的内容以及原始数据采集的现实性。

注 – 虽然在目前进行测量可能仍不现实，但在选择时仍需对指标加以认真考虑。此过程或可被用来确定一项新的工作活动，以实现对数据的捕获，如此便可对风险进行适当评估。

指标的数量可能取决于机构的使命和目标，或机构正在使用的技术。建议采用多项指标（如10至30项）构建网络安全风险指标的风险衡量标准。将主观指标与客观测量相结合，可影响到最终计算结果的有效性。因此，建议在构建网络安全风险指标时避免采用主观指标，但是，在某些风险管理领域中，可能需要采用主观指标，因此，如何严格定义主观指标至关

重要。指标一旦选定，即应根据事件管理、漏洞管理、补丁管理等业务职能分为不同类型，使指标更易于管理，也使比较更具意义。

详细的指标制定程序见第7.3段。

7.2.2 数据源

用于计算网络安全风险指标的指标数量和质量取决于网络安全指标数据的可用程度。过分依赖单一数据源可能导致错误与失误。因此，必须在将数据用于计算网络安全风险指标之前对照不同来源进行检查。

7.2.3 解决数据缺失问题

在为网络安全指标收集风险衡量标准时，可能会遇到数据缺失或无法提供数据的情况。在这种情况下，可将数据项空置（在这种情况下，机构将不对该指标赋值），或利用推断法估计出缺失的数据。将数据项空置可能导致网络安全的某些方面被排除在外。外推法可能会夸大数据值，因此导致计算结果虚高。要在外推法和省略法之间做出权衡，这种权衡应考虑数据值或指标的重要性。为此，可能应进行敏感试验，以确定计算结果对外推值波动的敏感程度，或是否以估值替换空白数据。

7.2.4 数据转换

转换包括两个阶段：从绝对值转换为相对值，以及从指标的相对值转换为网络安全风险指标。绝对值通常通过除以各项的总数获得可比性。许多指标可能已通过其转换状态提供，因此或许无需这一步骤。

7.3 网络安全指标的制定过程

网络安全指标制定过程包括选择适用于机构或社区任务和目标的指标。这一过程包括五个步骤：利益攸关方利益的确认、目标和目的的定义、信息安全政策、导则和程序的审核、信息安全实施的审核和指标选择。

步骤1，利益攸关方利益的确定包括确定相关利益攸关方及其利益。主要利益攸关方包括机构首脑、首席信息官、首席安全官、信息系统安全官、程序管理员、网络管理员、安全工程师和信息系统支持人员。这一步骤的成果包括信息安全测量中的所有利益。各利益攸关方都可能要求一套不同的指标，以表达他们在其职责领域的意见。

步骤2，目标和目的定义包括信息安全效果的目标和目的的确定，它们可能体现为政策、要求、导则和指示。信息安全项目的目标和目的可源自支持机构使命的高层目标和目的。

步骤3，信息安全政策、导则和程序的审核，这包括有关在针对机构的政策和程序中实施安全控制的详细说明。

步骤4，信息安全实施的审核，这包括审核现有指标和可用于求出新指标的相关数据存储库。

步骤5，指标的选择，这包括第6.4段提及的三类指标的酌情选择和制定。此步骤包括选择一组指标，以追踪程序实施、效率/效能和任务的影响，并视需要酌情制定新指标。

8 潜在的网络安全指标

本节介绍了已被确定为关键指标的各种潜在的网络安全指标，此类指标适用于为机构构建网络安全指标套件。这些指标可分为三类：基本指标、推荐指标和可选指标。此外，还可根据指标的性质，即实施指标、效能/效率指标和影响指标，将它们分为三类。本建议书没有确定与各项指标相关的要求等级。预计机构将根据机构其建议使用的安全政策来确定各项指标的要求等级。此外，机构可制定进一步指标（我们亦鼓励它们这样做），以应对其各自面临的情况。

本节中的指标（见8-1至8-30）被确定用于一个机构，但是，通过将构成一社区的机构的指标加以汇总，也可将它们用于社区。

就指标而言，在某些情况下，可能需要采用更大数值的指标（即：更大 - 最好）；而在另外一些情况下，最好采用更大还是更小数值的指标通过直观判断可能无法确定。

表8-1 – 指标1：漏洞管理（项目级，更大 – 更好）

域	数据
指标ID	经缓解的高危漏洞的百分比。
目标	机构应及时解决已知的漏洞。
指标	在机构确定的时限内缓解发现的高危漏洞的百分比。
公式	（及时缓解的高危漏洞总量/发现的高危漏洞的总量）× 100。
原始数据	• 在机构确定的时限内发现的漏洞数量。（注：必须通过原始数据来算得在机构确定的时限内发现的高危漏洞数量。） • 在时限内缓解的高危漏洞的数量。
频率	• 每周、每月、每季度、每年。
类型	• 效能/效率。
要求等级	
适用于	机构（汇总社区）。

表8-1 – 指标1：漏洞管理（项目级，更大 – 更好）

域	数据
参考自CYBEX技术	ITU-T X.1521建议书 – 常见漏洞评分系统，[b-ITU-T X.1521]和ITU-T X.1520建议书 – 常见漏洞和风险，[b-ITU-T X.1520].

表8-2 – 指标2：审计记录的保有（系统级、更大 – 更好）

域	数据
指标ID	保有审计记录的端点装置的百分比。
目标	机构应保有系统审计记录，以调查端点的不当活动。
指标	保有审计记录的端点装置的百分比。
公式	（具有审计记录的端点装置的总量/端点装置的总量）× 100。
原始数据	• 由中央记录服务器或端点装置保有审计记录的端点装置的数量。 • 端点装置总量。
频率	• 每周、每月、每季度、每年。
类型	• 效能/效率。
要求等级	
适用于	机构（汇总社区）。
参考自CYBEX技术	

表8-3 - 指标3：事件响应（系统级和项目级、更大 -更好）

域	数据
指标ID	事件响应。
目标	机构应针对每个事件类型及时报告事件。
指标	按适用类型在要求的时限内报告的事件的百分比。
公式	每个类别（及时报告的事件的数量/报告的事件的总量）× 100。
原始数据	• 机构确定的时限内报告的事件数量。 • 报告的事件的总量。
频率	• 每周、每月、每季度、每年。
类型	• 效能/效率。
要求等级	
适用于	机构（汇总社区）。
参考自CYBEX技术	ITU-T X.1544建议书 – 常见攻击模式列举和分类[b-ITU-T X.1544]。

表8-4 - 指标4：缓解漏洞平均时间（系统级和项目级、更小 – 更好）

域	数据
指标ID	缓解漏洞平均时间。
目标	这一指标旨在说明机构在解决发现的漏洞方面的表现。缓解漏洞所需的时间越短，机构就越能进行有效处理，以降低漏洞被利用的风险。
指标	缓解漏洞平均时间量化的是缓解机构发现的漏洞的平均时间。
公式	和（完成缓解日期 – 发现日期）/计算（缓解_漏洞）。
原始数据	• 漏洞发现日期。 • 漏洞缓解日期。 • 检测到的漏洞总量。 • 报告的经缓解的漏洞的总量。
频率	• 每周、每月、每季度、每年。
类型	• 效能/效率。
要求等级	
适用于	机构（汇总社区）。
参考自CYBEX技术	ITU-T X.1521建议书 – 常见漏洞评分系统，[b-ITU-T X.1521]和ITU-T X.1520建议书 – 常见漏洞和风险/[b-ITU-T X.1520].

表8-5 - 指标5：安全补丁程序的部署（系统级、更大 – 更好）

域	数据
指标ID	安全补丁程序。
目标	端点装置应采用安全补丁程序，以缓解用户个人电脑的漏洞。
指标	采用补丁管理系统的端点装置的百分比。
公式	（采用安全补丁程序的端点装置的总量/端点装置总量）× 100。
原始数据	• 采用安全补丁程序的端点装置的总量。 • 端点装置数量。
频率	• 每周、每月、每季度、每年。
类型	• 效能/效率。
要求等级	
适用于	机构（汇总社区）。
参考自CYBEX技术	

表8-6 - 指标6：补丁平均时间（系统级和项目级、更小 – 更好）

域	数据
指标ID	补丁平均时间。
目标	补丁平均时间量化的是为机构系统部署补丁所用的平均时间。补丁部署得越迅速，补丁平均时间越短，机构在已知脆弱状态运行系统的时间就越短。
指标	为机构系统部署补丁所用的平均时间。
公式	和（安装日期 – 可用日期）/计算（完成补丁）。
原始数据	• 安装日期。 • 投用日期。 • 完成补丁总量。
频率	• 每周、每月、每季度、每年。
类型	• 效能/效率。
要求等级	
适用于	机构（汇总社区）。
参考自 CYBEX 技术	

表8-7 - 指标7：完成配置修改的平均时间（系统级和项目级、更小 – 更好）

域	数据
指标ID	完成配置修改平均时间。
目标	完成配置修改平均时间旨在量化完成机构系统修改所用的平均时间。修改进程越快，补丁平均时间越短，机构将系统置于不稳定状态的时间就越短。
指标	完成机构系统配置修改所用的平均时间。
公式	和（完成日期 – 提交日期）/计算（完成修改）。
原始数据	• 完成日期。 • 提交日期。 • 完成修改总量。
频率	• 每周、每月、每季度、每年。
类型	• 效能/效率。
要求等级	
适用于	机构（汇总社区）。
参考自 CYBEX 技术	

表8-8 - 指标8：风险评估范围（系统级和项目级、更大 – 更好）

域	数据
指标ID	系统评估范围。
目标	机构应尽可能多地为机构系统应用进行风险评估。
指标	在任一时间接受风险评估的业务应用的百分比。
公式	计算（接受风险评估的应用）/计算（应用）× 100。
原始数据	• 接受风险评估的应用的数量。 • 应用数量。
频率	• 每周、每月、每季度、每年。
类型	• 效能/效率。
要求等级	
适用于	机构（汇总社区）。
参考自CYBEX技术	

表8-9 - 指标9：恶意软件发现和处理项目的覆盖范围（系统级、更大 – 更好）

域	数据
ID指标	恶意软件发现和处理项目。
目标	端点装置应实施反病毒项目，以减缓恶意软件，包括寄生在装置上的病毒。
指标	实施恶意软件发现和处理项目的端点装置百分比。
公式	（实施恶意软件发现和处理项目的端点装置总数/端点装置总数）× 100。
原始数据	• 实施反病毒项目的端点装置总数。 • 端点装置数量。
频率	• 每周、每月、每季度、每年。
类型	• 效能/效率。
要求等级	
适用于	机构（汇总社区）。
参考自CYBEX技术	

表8-10 - 指标10：应急规划范围（项目级、更大 – 更好）

域	数据
指标ID	应急规划测试
目标	机构因为信息系统进行应急规划测试。
指标	已进行应急规划测试的信息系统的百分比。
公式	（已进行应急规划测试的端点系统数量/端点系统总量）× 100。
原始数据	• 已进行应急规划测试的信息系统数量。
频率	• 每周、每月、每季度、每年。
类型	• 效能/效率。
要求等级	
适用于	机构（汇总社区）。
参考自 CYBEX 技术	

表8-11 - 指标11：安全评估（项目级、更大 – 更好）

域	数据
指标ID	获得安全评估批准的信息系统的百分比。
目标	机构的端点系统应在部署前得到认证和认可，以确保向人员、设施和产品提供具有全面安全保障的环境。
指标	已在部署前完成认证和认可的新端点系统的百分比。
公式	（已完成认证和认可的信息系统数量/信息系统总量）× 100。
原始数据	• 已完成认证和认可的新端点系统的数量。
频率	• 每周、每月、每季度、每年。
类型	• 效能/效率。
要求等级	
适用于	机构（汇总社区）。
参考自 CYBEX 技术	

表8-12 - 指标12：安全承诺（项目级、更大 – 更好）

域	数据
指标ID	安全承诺或行为准则。
目标	获准接入端点系统的雇员应在接入机构的信息系统前签署安全承诺。
指标	签署安全承诺的信息系统安全人员的百分比。
公式	（获准接入系统并签署行为规范的人员的数量/获准接入端点系统的人员总量）× 100。
原始数据	• 在签署安全承诺后获准接入系统的雇员的数量。
频率	• 每周、每月、每季度、每年。
类型	• 实施。
要求等级	
适用于	机构（汇总社区）。
参考自 CYBEX 技术	

表8-13 - 指标13：配备安全网关的远程接入控制（系统/项目级、更大 – 更好）

域	数据
指标ID	受保护的远程接入点。
目标	机构应部署安全网关，以实现保护其内部资产的受保护远程接入。
指标	受保护远程接入点的百分比。
公式	（采用安全网关的远程接入点数量/机构远程接入点总量）× 100。
原始数据	• 采用安全网关的受保护远程接入点的数量。
频率	• 每周、每月、每季度、每年。
类型	• 效能/效率。
要求等级	
适用于	机构（汇总社区）。
参考自 CYBEX 技术	

表8-14 - 指标14：带有入侵预防和发现安全功能的远程访问控制（系统/项目级、更大 – 更好）

域	数据
指标ID	受保护的远程接入点。
目标	机构应部署入侵发现和预防安全功能，以保护机构的内部资产。
指标	受保护远程接入点的百分比。
公式	（实施带有入侵发现和预防安全功能的远程接入点数量/远程接入点总数）× 100。
原始数据	• 实施带有入侵发现和预防安全功能、受保护的远程接入点数量。
频率	• 每周、每月、每季度、每年。
类型	• 效能/效率。
要求等级	
适用于	机构（汇总社区）。
参考自CYBEX技术	

表8-15 - 指标15：无线接入控制（系统/项目级、更大 – 更好）

域	数据
指标ID	受保护的无线接入点。
目标	机构应提供受保护的无线接入点，以保护内部网络免受擅自接入。
指标	受保护无线接入点的百分比。
公式	（受保护无线接入点数量/无线接入点总量）× 100。
原始数据	• 受保护无线接入点数量。 • 无线接入点数量。
频率	每周、每月、每季度、每年。
类型	效能/效率。
要求等级	
适用于	机构（汇总社区）。
参考自CYBEX技术	

表8-16 - 指标16：个人安全（系统级/项目级、更大 – 更好）

域	数据
指标ID	个人安全筛查。
目标	机构应允许被授权的个人接入端点系统。
指标	在获准接入机构的端点系统前接受筛查的个人的百分比。
公式	（经筛查的个人的数量/获准接入的个人的总量）× 100。
原始数据	• 经筛查的个人数量。 • 个人数量。
频率	• 每周、每月、每季度、每年。
类型	实施。
要求等级	
适用于	机构（汇总社区）。
参考自 CYBEX 技术	

表8-17 - 指标17：个人可识别信息（PII）的保护（系统/项目级、更大 – 更好）

域	数据
指标ID	受保护的敏感个人可识别信息的百分比。
目标	机构应以加密形式保护其敏感的个人可识别信息。
指标	受保护的敏感个人可识别信息的百分比。
公式	（加密的敏感个人可识别信息数量/个人可识别信息总量）× 100。
原始数据	• 受保护的个人可识别信息数量。 • 个人可识别信息总量。
频率	• 每周、每月、每季度、每年。
类型	效能/效率和实施。
要求等级	
适用于	机构（汇总社区）。
参考自 CYBEX 技术	

表8-18 - 指标18：备份数据保护（系统/项目级、更大 – 更好）

域	数据
指标ID	备份数据完整性检查率。
目标	机构应为备份数据提供完整性保护。
指标	完整性受保护的备份数据的百分比。
公式	（完整性受保护的备份数据数量/备份数据总量）× 100。
原始数据	• 完整性受保护的备份数据的数量。 • 备份数据总量。
频率	• 每周、每月、每季度、每年。
类型	效能/效率和实施。
要求等级	
适用于	机构（汇总社区）。
参考自CYBEX技术	

表8-19 - 指标19：经认证的安全管理系统（如ISMS）的范围（系统/项目级、更大 – 更好）

域	数据
指标ID	管理系统的范围。
目标	机构的端点应由获认证的安全管理系统（如，ISMS）涵盖。
指标	获认证的安全管理系统保护的端点系统的百分比。
公式	（获认证的安全管理系统（如ISMS）保护的端点系统的数量/端点系统总量）× 100。
原始数据	• 获认证的安全管理系统（如ISMS）保护的端点系统的数量。 • 端点系统总量。
频率	每周、每月、每季度、每年。
类型	效能/效率和实施。
要求等级	
适用于	机构（汇总社区）。
参考自CYBEX技术	

表8-20 - 指标20：安全服务器的部署（系统级/项目级、更大 – 更好）

域	数据
指标ID	安全服务器的部署。
目标	机构的网络业务应通过对远程接入采用安全隧道交换信息。
指标	采用TLS、SSL或安全壳等安全隧道的网络业务的百分比。
公式	（采用安全隧道的网络业务的数量/网络业务总量）× 100。
原始数据	• 采用安全隧道的网络业务的数量。 • 网络业务总量。
频率	• 每周、每月、每季度、每年。
类型	效能/效率和实施。
要求等级	
适用于	机构（汇总社区）。
参考自CYBEX技术	
注 -（在指标一项中所指的）安全服务器可以多种方式来实现，以在端点之间提供安全隧道，其中包括使用SSL/TLS和安全外壳保护的服务器。	

表8-21 - 指标21：垃圾信息接收率（项目、更小 – 更好）

域	数据
指标ID	垃圾信息接收率。
目标	机构应采用垃圾信息过滤器以防止垃圾信息电子邮件流向雇员。
指标	在规定时限内超出机构所定数量收到垃圾信息电子邮件的雇员的百分比。
公式	（收到一定数量垃圾信息电子邮件的雇员的数量/雇员总量）× 100。
原始数据	• 在规定时限内超出机构所定数量收到垃圾信息电子邮件的雇员的数量。 • 雇员的数量。
频率	• 每周、每月、每季度、每年。
类型	效能/效率和实施。
要求等级	
适用于	机构（汇总社区）。
参考自CYBEX技术	

表8-22 - 指标22：机构的意识项目（更大 – 更好）

域	数据
指标ID	机构的意识提高项目。
目标	雇员应具有意识提高项目。
指标	参与意识提高项目的雇员的百分比。
公式	（已参与意识提高项目的雇员的数量/雇员总量）× 100。
原始数据	• 已参与意识提高项目的雇员的数量。 • 雇员的数量。
频率	• 每周、每月、每季度、每年。
类型	效能/效率和实施。
要求等级	
适用于	机构（汇总社区）。
参考自CYBEX技术	

表8-23 - 指标23：安全培训和教育（项目级、更大 – 更好）

域	数据
指标ID	安全培训和教育。
目标	机构雇员应完成安全培训和教育课程，以便妥善的应对安全事件。
指标	在机构规定的时限内完成安全培训和教育课程的雇员的百分比。
公式	（完成安全培训和教育课程的雇员的数量/雇员总量）× 100。
原始数据	• 完成培训和教育课程的雇员的数量。 • 雇员的数量。
频率	• 每周、每月、每季度、每年。
类型	影响/实施。
要求等级	
适用于	机构（汇总社区）。
参考自CYBEX技术	

表8-24 - 指标24：网络安全的作用和职责（项目级、更大 - 更好）

域	数据
指标ID	作用与职责。
目标	机构应招聘一个网络安全响应团队。
指标	与信息安全相关人员的百分比。
公式	（参与网络任务的人员的数量/IT人员总量）× 100。
原始数据	• 与网络安全活动相关人员的数量。 • IT人员总量。
频率	• 每周、每月、每季度、每年。
类型	影响/实施。
要求等级	
适用于	机构（汇总社区）。
参考自CYBEX技术	

表8-25 - 指标25：恶意软件的感染（项目级和系统级、更小 – 更好）

域	数据
指标ID	受恶意软件感染的端点装置。
目标	雇员的端点装置应具有对各类恶意软件的防范能力。
指标	雇员的计算机受到病毒或恶意软件感染或受到利用黑客技术的攻击者危害的百分比。
公式	（受恶意软件感染的端点装置的总量/端点装置总量）× 100。
原始数据	• 受病毒或为软件感染或受利用黑客技术攻击而受损的端点装置的数量。 • 机构的端点装置的总量。
频率	• 每周、每月、每季度、每年。
类型	影响和效能。
要求等级	
适用于	机构（汇总社区）。
参考自CYBEX技术	

表8-26 - 指标26：个人可识别信息的泄漏（项目级）

域	数据
指标ID	个人可识别信息的泄漏。
目标	机构应避免向外界机构泄漏个人可识别信息。
指标	所报告个人可识别信息事件特定时间段内被泄漏的个人可识别信息单位的百分比。 注 - 该指标的开发人员应定义其自身的PII单位。
公式	（所报告PII事件中机构确定的时段内被泄漏的个人可识别信息单位数量/个人可识别信息单位总量）× 100。
原始数据	• 所报告个人可识别信息（PII）事件中机构确定的时段内被泄漏的PII单位数量。 • 个人可识别信息单位的总量。
频率	• 每周、每月、每季度、每年。
类型	影响。
要求等级	
适用于	机构（汇总社区）。
参考自CYBEX技术	

表8-27 - 指标27：安全预算占ICT预算的百分比（项目级）

域	数据
指标ID	机构的信息安全预算占ICT预算的百分比。
目标	机构应为网络安全提供预算。
指标	机构的网络安全预算占ICT预算的百分比；假设安全预算被纳入IT预算。
公式	（网络安全预算/ICT总预算）× 100。
原始数据	• 网络安全预算额。 • ICT预算总额。
频率	• 每周、每月、每季度、每年。
类型	影响。
要求等级	
适用于	机构（汇总社区）。
参考自CYBEX技术	

表8-28 - 指标28：得到授权的装置比（更大 – 更好）

域	数据
指标ID	机构中得到授权的装置与所有装置之比。
目标	机构应在资产库存（允许接入网络的装置）基础上对装置（计算机、网络组成成分、打印机、与IP地址有关的任何装置）进行跟踪/控制/防止访问网络/纠正网络访问。
指标	机构中得到授权的装置与所有装置之比。
公式	（得到授权的装置数/装置数）× 100。
原始数据	• 得到授权的装置数量。 • 装置数量。
频率	• 每周、每月、每季度、每年。
类型	影响。
要求等级	
适用于	机构（汇总社区）。
参考自CYBEX技术	

表8-29 - 指标29：得到授权的软件比（更大 – 更好）

域	数据
指标ID	机构中得到授权的软件资产与总软件资产之比。
目标	机构应根据得到授权的软件资产库存，对软件进行跟踪/控制/防止/纠正在计算机上的安装和运行。
指标	机构中得到授权的软件资产与总软件资产之比。
公式	（得到授权的软件资产数/软件总资产数）× 100。
原始数据	• 得到授权的软件资产数量。 • 软件资产总数。
频率	• 每周、每月、每季度、每年。
类型	影响。
要求等级	
适用于	机构（汇总社区）。
参考自CYBEX技术	ITU-T X.1528建议书 – 常见平台列举，[b-ITU-T X.1528]和ISO/IEC 19770-2 – 信息技术 – 软件资产管理 – 第2部分：软件识别标签[b-ISO/IEC 19770-2]。

表8-30 - 指标30：应用软件的安全性（更大 – 更好）

域	数据
指标ID	机构中得到保护、防止受到重大应用级软件攻击（如前25 CWE）的应用软件与所有应用软件资产之比。
目标	机构应发现并阻止应用级软件攻击，并在发现和阻止的24小时内向企业行政管理人员发出了警示或电子邮件。
指标	机构中得到保护、防止受到重大应用级软件攻击的应用软件与所有应用软件资产之比。
公式	（机构中得到保护、防止受到重大应用级软件攻击的应用软件/应用软件总资产数）× 100。
原始数据	• 得到保护、免受重大应用级软件攻击影响的应用软件数。 • 应用软件资产总数。
频率	每周、每月、每季度、每年。
类型	影响。
要求等级	
适用于	机构（汇总社区）。
参考自CYBEX技术	ITU-T X.1524建议书 – 常见缺陷列举，[b-ITU-T X.1524]和ITU-T X.1544建议书 – 常见攻击模式列举和分类[b-ITU-T X.1544]。

附录I

信息安全风险衡量标准指标和度量表的示例

（本附录不构成本建议书的组成部分）

本附录具体说明了可用于计算网络安全指标的信息安全风险衡量标准指标和度量表示例。

[b-NIST SP 800-55]提供了系统级和项目级的潜在候选风险衡量标准，可分为以下三个等级：

- 系统级风险衡量标准：
  - 接入控制；
  - 审计和问责制；
  - 确定和认证；
  - 维护；
  - 风险评估。
- 项目级风险衡量标准：
  - 安全开支，漏洞管理；
  - 认识与培训；
  - 认证、鉴定和安全评估；
  - 配制管理；
  - 应急规划；
  - 物理环境。
- 项目级和系统级风险衡量标准：
  - 事件响应；
  - 媒体保护；
  - 规划；
  - 个人安全；
  - 系统和通信采购；
  - 系统和信息完整性。

此外，由世界经济论坛（WEF）制定的[b-NRI]亦提供若干指标，而[b-WEF]则使用具体厂商的安全套接层（SSL）证书和传输层安全（TLS）证书。

附录II

指标的按性质分类

（本附录不构成本建议书的组成部分）

为使机构更广泛地接受本建议书，有必要在不生成巨额费用的情况下确定可达到且可用的最低衡量标准。

例如，第8节的指标24（网络安全的作用和职责）是易于首先实施的指标，因为它的测量内容仅涉及人员统计。一些其他指标需要进一步采用其他工具和/或数据库，以便使这些指标具有可测量性。例如，指标1（漏洞管理）要求漏洞管理工具和相关数据库已经就位。因此，希望使用该指标的机构必须考虑进行投资的效益所在，以在提供此信息时亦公开其相关成本。同样，指标2要求ICT资产管理功能已在机构实行。另一指标等级要求一机构内部具有某种能力，以便使它们可被测量。例如，指标4（减缓漏洞的平均时间）则要求已知事件发生日期，如果没有审计和分析能力，将很难做到这一点。

本附录介绍了根据性质的指标划分：即易于利用机构中常见的工具和/或数据库测量的指标，以及在机构决定强化其测量能力后可测量的指标。

表II.1 – 按性质的指标分类

指标性质	指标数量	指标 ID
易于测量的指标	指标12：安全保证书	安全保证书或行为准则
	指标16：个人安全	个人安全审查
	指标24：网络安全作用和职责	网络安全的作用和职责
	指标27：安全预算占ICT预算的百分比	机构的信息安全预算占ICT预算的百分比
利用机构中常见的测量工具和/或数据库可以测量的指标	指标1：漏洞管理	缓解的高危漏洞的百分比
	指标2：审计记录保存	保有审计记录的端点装置的百分比
	指标3：事件响应	事件响应
	指标8：风险评估范围	风险评估范围
	指标9：恶意软件发现和处理程序的覆盖范围	恶意软件发现和处理程序的覆盖范围
	指标21：垃圾信息接收率	垃圾信息接收率
	指标22：机构的意识提高项目	机构的意识提高项目

表II.1 – 按性质的指标分类

指标性质	指标数量	指标 ID
	指标23：安全培训与教育	安全培训与教育
	指标28：获授权装置率	机构的获授权装置在全部装置中所占的比率
	指标29：获授权软件率	机构的获授权软件资产在全部软件资产中所占的比率
	指标30：应用软件安全	机构中通过保护而免收大型应用级攻击（如CWE前25名）的应用软件在全部应用软件资产中所占的比率
可能需要在机构内进一步开展测量能力建设的指标	指标4：缓解漏洞平均时间	缓解漏洞平均时间
	指标5：安全补丁程序的部署	安全补丁程序
	指标6：补丁平均时间	补丁平均时间
	指标7：完成配置修改平均时间	完成配置修改平均时间
	指标10：应急规划范围	应急规划测试
	指标11：安全评估	获得安全评估批准的信息系统的百分比
	指标12：带有安全网关的远程接入控制	受保护的远程接入点
	指标13：带有入侵发现或入侵预防安全功能的远程接入控制	受保护的远程接入点
	指标14：无线接入控制	受保护的无线接入点
	指标17：个人可识别信息（PII）的保护	受保护的敏感个人可识别信息的百分比
	指标18：备份数据保护	备份数据完整性检查率
	指标19：经认证的安全管理系统的覆盖范围	管理系统的覆盖范围
	指标20：安全服务器的部署	安全服务器的部署

表II.1 – 按性质的指标分类

指标性质	指标数量	指标 ID
	指标25：恶意软件感染	受恶意软件感染的端点装置
	指标26：个人可识别信息的泄露	个人可识别信息的泄露

附录III

实验性指标

（本附录不构成本建议书的组成部分）

本附录介绍了可能适合机构使用的一些实验性指标（见表III.1至 III.6）。

表III.1 – 指标III-1：事件发现的平均时间
（系统级和项目级、更小 – 更好）

域	数据
指标ID	事件发现的平均时间。
目标	机构应在出现事件时立即发现并测量事件发现平均时间，以证明机构在发现安全事件方面的效能。总之，机构发现事件越快，造成的损失可能越小。
指标	特定一系列事件发生和发现之间以小时计算的流失时间。
公式	和（发现时间 – 发生时间）/数量（事件）。
原始数据	发现每个事件所用的时间。 报告的事件的总量。
频率	每周、每月、每季度、每年。
类型	效能/效率。
要求等级	
适用于	机构（汇总社区）。
参考自 CYBEX 技术	

表III.2 – 指标III-2：链路冗余（系统级、更大 – 更好）

域	数据
指标ID	拥有冗余的网络链路的百分比。
目标	机构应在主要网络中构建一条冗余链路，以确保机构服务的可用性和连续性。
指标	配备冗余的网络链路的百分比。
公式	（冗余链路数量/网络链路总量）× 100。
原始数据	用于路由器、域名系统（DNS）、动态主机配置协议（DHCP）、防火墙或据库（DB）。 无冗余链路数。
频率	每周、每月、每季度、每年。
类型	效能/效率。

表III.2 – 指标III-2：链路冗余（系统级、更大 – 更好）

域	数据
要求等级	
适用于	机构（汇总社区）。
参考自CYBEX技术	

表III.3 – 指标III-3：机器人的感染（系统级、更小 – 更好）

域	数据
指标ID	受机器人感染的端点装置的百分比。
目标	机构应减少机器人在机构网络上的存在。
指标	受一机构已知机器人感染的端点装置的百分比。假设该机构采用机器人感染检测系统。
公式	（受已知机器人感染的端点装置的总量/端点装置总量）× 100。
原始数据	受机器人感染的端点装置的数量。
频率	每周、每月、每季度、每年。
类型	效能/效率。
要求等级	
适用于	机构（汇总社区）。
参考自CYBEX技术	

表III.4 – 指标III-4：分布式拒绝服务（DDoS）衡量指标（系统级、更小 – 更好）

域	数据
指标ID	DDoS衡量标准。
目标	机构应在其规定的时段内保护其信息系统免受DDoS（或拒绝服务（DoS））攻击。
指标	因DDoS（DoS）攻击而在特定时段内无法使用的系统的百分比。
公式	（在机构规定的时段内因DDoS攻击而在特定时间段无法使用的机构系统的数量/系统拥有的网站的总量）× 100。
原始数据	在机构规定的时段内因DDoS攻击而在特定时间段无法使用的网站的数量。 网站的总量
频率	每周、每月、每季度、每年。

表III.4 – 指标III-4：分布式拒绝服务（DDoS）衡量指标（系统级、更小 – 更好）

域	数据
类型	效能/效率。
要求等级	
适用于	机构（汇总社区）。
参考自 CYBEX 技术	

表III.5 – 指标III-5：审计记录的执行（系统级和项目级，更大 – 更好）

域	数据
指标ID	审计记录已捕获其可察觉踪迹的计算机安全事件百分比。.
目标	机构应评估审计记录的有效性。
指标	审计记录已捕获其可察觉踪迹的计算机安全事件百分比。
公式	（在记录中留下可察觉踪迹的被记录事件数/报告总数）× 100。
原始数据	在审计记录中已发现可察觉踪迹的得到报告的事件数。（集中记录或从端点汇总的记录）。 报告事件总数。
频率	每周、每月、每季度、每年。
类型	效能/效率。
要求等级	
适用于	机构（汇总社区）。
参考自 CYBEX 技术	

表III.6 – 指标III-6：事件减缓措施的执行（系统级和项目级，更大 – 更好）

域	数据
指标ID	C&A系统中得到定位的计算机安全事件百分比（端点或一组端点）。
目标	机构应评估C&A程序的有效性。
指标	C&A系统中得到定位的计算机安全事件百分比。
公式	（C&A系统中定位的报告事件数/报告事件总数）× 100。
原始数据	C&A系统中定位的报告事件数。 报告事件总数。
频率	每周、每月、每季度、每年。
类型	效能/效率。
要求等级	
适用于	机构（汇总社区）。
参考自CYBEX技术	

参考资料

[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/

ITU-T 系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	视听及多媒体系统
I系列	综合业务数字网
J系列	有线网络和电视、声音节目及其它多媒体信号的传输
K系列	干扰的防护
L系列	电缆和外部设备其它组件的结构、安装和保护
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备的技术规范
P系列	电话传输质量、电话设施及本地线路网络
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	**数据网、开放系统通信和安全性**
Y系列	全球信息基础设施、互联网协议问题和下一代网络
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2014年，日内瓦