ICS 35.030
CCS L 80

中 华 人 民 共 和 国 国 家 标 准

GB/T 31497—2024/ISO/IEC 27004:2016
代替 GB/T31497—2015

信息技术　安全技术　信息安全管理 监视、测量、分析和评价

Information technology—Securitytechniques—Information security management—Monitoring,measurement,analysisand evaluation

(ISO/IEC 27004:2016,IDT)

2024-03-15发布 2024-10-01实施

国家市场监督管理总局
国家标准化管理委员会 发布

目　　次

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则　第 1部分 :标准化文件的结构和起草规则》的规定起草。

本文件代替 GB/T 31497—2015《信息技术　安全技术　信息安全管理　测量》,与 GB/T 31497—2015相比 ,除结构调整和编辑性改动外 ,主要技术变化如下 :

a) 更改了 “范围” 的表述(见第 1章 ,2015年版的第 1章) ;

b) 更改了第 5章的标题和内容 ,标题由 “信息安全测量概述” 修改为 “基本原理” ,删掉了 “信息安全测量模型” 相关内容(见第 5章 ,2015年版的第 5章) ;

c) 删除了 “管理职责” (见 2015年版的第 6章) ;

d) 增加了 “特征” (见第 6章) ;

e) 更改了测度的类型 ,将 “基本测度” 和 “导出测度” 更改为 “实施进度的测度” 和 “有效性测度” (见第 7章 ,2015年版的第 5章) ;

f) 更改了信息安全管理　监视、测量、分析和评价的过程(见第 8章 ,2015年版的第 8章、第 9章和第 10章) 。

本文件等同采用 ISO/IEC 27004:2016《信息技术　安全技术　信息安全管理　监视、测量、分析和评价》。

本文件做了下列最小限度的编辑性改动 :

a) 增加了有利于理解本文件的注(见第 4章 ,5.2) ;

b) 增加了资料性附录 NA,给出了 GB/T 22081—2016与 ISO/IEC 27002:2022 中控制的对应关系(见附录 NA) 。

请注意本文件的某些内容可能涉及专利 。本文件的发布机构不承担识别专利的责任。

本文件由全国网络安全标准化技术委员会(SAC/TC260)提出并归 口 。

本文件起草单位 :中国电子技术标准化研究院 、中国合格评定国家认可中心 、北京赛西认证有限责任公司 、杭州安恒信息技术股份有限公司 、北京邮电大学 、上海三零卫士信息安全有限公司 、道普信息技术有限公司 、中电长城网际系统应用有限公司 、北京航空航天大学 、华为技术有限公司 、中国科学院信息工程研究所 、西安电子科技大学 、重庆邮电大学 、中国网络安全审查技术与认证中心 、国家工业信息安全发展研究中心 、北京中关村实验室 、上海观安信息技术股份有限公司 、北京天融信网络安全技术有限公司 、国家计算机网络应急技术处理协调中心 、公安部第三研究所 、山东正中信息技术股份有限公司 、重庆市信息通信咨询设计院有限公司 、启明星辰信息技术集团股份有限公司 、西安交大捷普网络技术有限公司 、国网新疆电力有限公司电力科学研究院 、广东省信息安全测评中心 、长扬科技(北京)股份有限公司 、

北京源堡科技有限公司 、云智慧(北京)科技有限公司 、远江盛邦(北京)网络安全科技股份有限公司 、新 华三技术有限公司 。

本文件主要起草人 :上官晓丽、王惠莅、付志高、许玉娜、王东滨、周亚超、赵丽华、闵京华、伍前红、史文征、张东举、干露、邵萌、刘俊荣、谢江、马文平、黄永洪、魏立茹、陈雪鸿、杨光、陆月明、张静、崔牧凡、郭峰、吕明、陈长松、张晓琴、陈星佑、何建锋、邹振婉、叶劲宏、赵华、梁露露、戚依军、王晶、权晓文、万晓兰、陈纪旸。

本文件及其所代替文件的历次版本发布情况为：

—2015年首次发布为 GB/T 31497—2015;

—本次为第一次修订 。

引　言

本文件旨在帮助组织评价信息安全绩效和信息安全管理体系的有效性，以满足 GB/T 22080—2016中 9.1“监视、测量、分析和评价”的要求。

信息安全管理体系(ISMS)的监视和测量结果会对 ISMS的治理、管理、有效运行和持续改进有关的决策提供支持。

与其余 ISO/IEC 27000系列标准一样，组织根据自身实际情况和需要考虑、解释和调整本文件的内容。本文件中的概念和方法是广泛适用的，但任何特定组织所需的具体测度取决于在实践中差异很大的环境因素(如其规模、行业、成熟度、信息安全风险、合规义务和管理风格)。

依据 GB/T 22080实施 ISMS的组织使用本文件。但本文件没有为符合 GB/T 22080 的 ISMS提出任何新的要求，也没有要求组织一定要遵守本文件提出的指南。

按照 GB/T 22080—2016中 9.1 的要求对标准文本进行了重新编写，前言中仅列出了主要的技术变动，详细变动见本文件具体内容。

信息技术　安全技术　信息安全管理
监视、测量、分析和评价

1　范围

本文件提供了旨在协助组织评价信息安全绩效和ISMS(信息安全管理体系)有效性,以满足GB/T 22080—2016中9.1要求的指南。本文件规定了:

a)　信息安全绩效的监视和测量;

b)　ISMS(包括其过程和控制)有效性的监视和测量;

c)　监视和测量结果的分析和评价。

本文件适用于各种类型和规模的组织。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 22080—2016　信息技术　安全技术　信息安全管理体系　要求(ISO/IEC 27001:2013,IDT)

ISO/IEC 27000　信息技术　安全技术　信息安全管理体系　概述和词汇(Information technology—Security techniques—Information security managementsystems—Overview and vocabulary)

注:GB/T 29246—2023　信息安全技术　信息安全管理体系　概述和词汇(ISO/IEC 27000:2018,IDT)

3　术语和定义

ISO/IEC 27000界定的术语和定义适用于本文件。

4　结构和概述

本文件的结构如下：

a) 基本原理(第 5章)；

b) 特征(第 6章)；

c) 测度的类型(第 7章)；

d) 过程(第 8章)。

这几章的排序旨在帮助理解并与 GB/T 22080—2016中 9.1 的要求形成如图 1所示的对应关系。

组织首先识别满足要求所需的信息(称之为 “信息需求”)，然后确定用于满足信息需求的测度。监视和测量过程产生了随后要被分析的数据，用分析结果来评价是否满足组织的信息需求。

注：测量是确定一个值的过程，测度是作为测量结果赋值的变量。

此外，附录 A描述了信息安全测量模型，包括测量模型的组成部分与 GB/T 22080—2016中 9.1 的要求之间的关系。

附录 B提供了一系列的示例。这些示例旨在就组织如何监视、测量、分析和评价其所选择的ISMS过程和信息安全绩效领域提供实际指导。附录 B 中的示例使用了表 1 中给出的建议模板,附件 C则提供了使用另一种基于自由文本格式的示例。

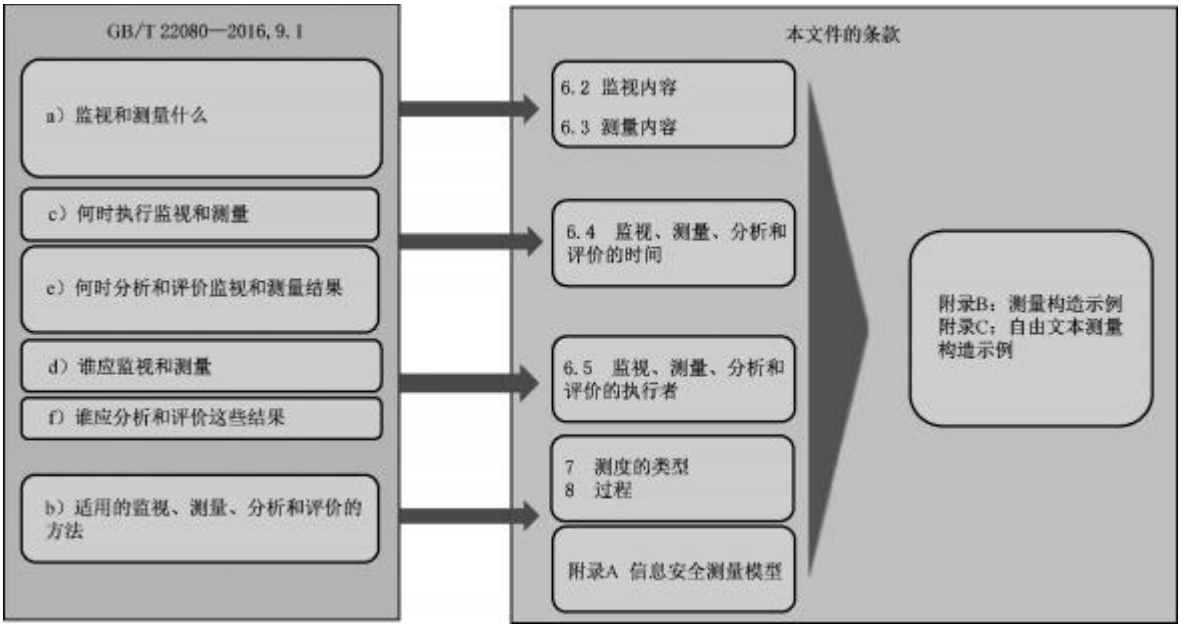

图 1 与 GB/T22080—2016,9.1 的对应

5 基本原理

5.1 测量的必要性

ISMS的总体目标是在其范围内保持信息的保密性、完整性和可用性,通过 ISMS活动制定实现该目标的计划以及这些计划的实施。但是,仅这些活动本身并不能保证完成这些计划就能达到信息安全目标。因此,在 GB/T 22080规定的 ISMS中,有多处要求组织评价计划和活动是否确保实现了信息安全目标。

5.2 满足 GB/T22080的要求

GB/T 22080—2016的 9.1要求组织评价信息安全绩效和 ISMS有效性,在第 7章给出了能够满足这些要求的测度类型。

GB/T 22080—2016的 9.1还要求组织确定:

a) 需要被监视和测量的内容,包括信息安全过程和控制;

b) 适用的监视、测量、分析和评价的方法,以确保得到有效的结果;

注:所选的方法产生可比较和可再现的有效结果。

c) 何时应执行监视和测量;

d) 谁应监视和测量;

e) 何时应分析和评价监视和测量的结果；

f) 谁应分析和评价这些结果 。

图 1提供了本文件与这些要求的对应 。

最后 ,GB/T 22080—2016的 9.1要求组织保留适当的文件作为监视和测量结果的证据(见 8.9) 。

GB/T 22080—2016的 9.1还指出,所选择的方法宜产生可比较和可再现的结果,以便确认它们是有效的(见 6.4)。

5.3 结果的有效性

GB/T 22080—2016的 9.1 b)要求组织选择测量、监视、分析和评价的方法,以确保有效的结果。该条款指出:为了获得有效的结果,结果宜是可比较的和可再现的。为实现这一目标,组织宜考虑以下几个方面来收集、分析和报告测度。

a) 为了从基于不同时间点的监视中获得测度的可比较结果,确保 ISMS 的范围及其环境没有变化是很重要的。

b) 测量和监视的方法或技术发生改变时,一般不会产生可比较的结果。为了保持可比性,可以要求进行特定的测试,比如同时分别使用原方法和变化后的方法。

c) 如果测量和监视所用方法或技术包括主观要素,则需要采取特定的步骤以获得可再现的结果。例如,宜对照设定的准则来评价问卷调查结果。

d) 在某些情况下,只能在特定情况下才会产生再现性。例如,有些情况下,结果是不可再现的,但在将其汇总后,结果是有效的。

5.4 益处

实现 ISMS过程与控制并确保信息安全实施,能产生大量的组织效益和经济效益。主要效益可能包括如下内容。

a) 强化责任:监视、测量、分析和评价能通过帮助识别未正确实施的、未实施的或无效的特定信息安全过程或控制,来强化对信息安全的责任。

b) 改进信息安全绩效和 ISMS过程:监视、测量、分析和评价能使组织量化其在 ISMS范围内保护信息方面的改进,并证实其在实现组织信息安全目标方面可量化的进展。

c) 提供满足要求的证据:监视、测量、分析和评价可提供文件化的证据,有助于证明组织符合 GB/T 22080(及其他标准)以及适用的法律、法规和规章制度。

d) 支持决策:监视、测量、分析和评价能通过向风险管理过程提供可量化的信息来支持风险指引决策。它能使组织衡量以往的和当前的信息安全投资的成败,并能提供可量化的数据,以支持未来投资的资源分配。

6 特征

6.1 概述

监视和测量是评价信息安全绩效和 ISMS有效性的第一步。

面对大量信息安全相关实体的各种各样的可测量属性,并不是非常明确宜测量哪些属性。这是一个重要的问题,因为测量太多的或错误的属性是不切实际的、代价高昂的和适得其反的。对众多的属性进行测量、分析和报告,除了会产生明显的成本之外,倘若没有合适的测度,还很有可能出现关键问题被淹没于大量信息中或者完全被遗漏掉。

为了确定要监视和测量的内容,组织宜首先考虑在评价信息安全实施和 ISMS有效性方面希望实现的目标,这可使组织确定其信息需求。

组织接下来宜决定需要采取哪些测度来支持每一种不同的信息需求,以及需要哪些数据以生成所需的测度。 因此,测量宜始终与组织的信息需求相对应。

6.2 监视内容

监视是确定系统、过程或活动的状态,以满足特定的信息需求。

能被监视的系统、过程和活动包括但不限于:

a) ISMS过程的实施;

b) 事件管理;

c) 脆弱性管理;

d) 配置管理;

e) 安全意识和培训;

f) 访问控制、防火墙和其他事件日志;

g) 审核;

h) 风险评估过程;

i) 风险处置过程;

j) 第三方风险管理;

k) 业务连续性管理;

l) 物理和环境安全管理;

m) 系统监视。

这些监视活动产生的数据(事件日志、用户访谈、培训统计、事件信息等),能用于支持其他测度。在定义被测量的属性的过程中,能要求实施额外的监视,以提供支持性信息。

需要注意的是,监视能使组织确定风险是否已经发生,从而提示组织能采取什么措施来处置该风险。还需要注意的是,某些类型的信息安全控制具有明确的监视目的。在使用这些控制的输出来支持测量时,组织宜确保测量过程考虑了所用的数据是在采取任何处置措施之前还是之后获得的。

6.3 测量内容

测量是指为确定实施进度或有效性的值、状态或趋势的活动,以帮助识别潜在的改进需求。测量能应用于任何 ISMS过程、活动、控制和控制组。

例如,GB/T 22080—2016的 7.2 c)要求组织适用时采取行动以获得必要的能力。组织能确定是否所有需要培训的人员都已经接受了培训,以及培训是否按计划进行,这能用接受过培训的人数或百分比来测量。组织还能确定接受过培训的人员是否实际获得了并持续拥有必要的能力(能用培训后的问卷来测量)。

关于 ISMS过程,组织宜注意到 GB/T 22080 中有一些条款明确要求确定某些活动的有效性。例如,GB/T 22080—2016的 10.1 d)要求组织“评审任何所采取的纠正措施的有效性”。为了实施该评审,组织首先宜根据某种规定的测度形式来确定纠正措施的有效性。为了做到这一点,组织宜首先定义适当的信息需求和能满足信息需求的一个或多个测度。第8章中阐述了这一过程。

可作为测量对象的 ISMS过程和活动包括：

a) 规划；

b) 领导；

c) 风险管理；

d) 方针管理；

e) 资源管理；

f) 沟通；

g) 管理评审;

h) 文件化;

i) 审核。

关于信息安全实施,最明显的候选对象是组织的信息安全控制或这类控制的组合(甚至是整个风险处置计划)。这些控制是通过风险处置过程确定的并在 GB/T 22080 中被称为必要的控制。它们能是 GB/T 22080—2016附录 A 中的控制、特定行业的控制(例如 ISO/IEC 27010等标准所规定的)、其他标准规定的控制和由组织设计的控制。由于控制的目的是改变风险,因此有很多能被测量的属性,例如:

j) 控制措施降低事件发生的可能性的程度;

k) 控制措施减轻事件后果的程度;

l) 控制措施在发生故障前对事态进行处理的频次;

m) 控制措施在事态发生后多长时间内检测到事态。

6.4 监视、测量、分析和评价的时间

组织宜根据单个信息需求、所需的测度和支持单个测度的全生命周期的数据,定义实施监视、测量、分析和评价的具体时间表。对支持测度所需数据的收集频次,可高于分析测度和向利益相关方报告该测度的频次。例如,虽然能连续收集安全事件的数据,但向外部利益相关方报告此类数据宜基于特定要求,如严重性(如发生应报告的违规时,可能需要立即告知)或累计值(如发现和阻止企图入侵的情况)。

组织宜注意,为了满足某些信息需求,在进行分析和评价之前需要收集适当数量的数据,为评估和比较提供重要基础(例如:进行统计分析时)。此外,监视、测量、分析和评价的过程可能需要测试和微调,然后所形成的测度才可能对组织有用。因此,组织宜确定任何微调的时限(以便持续推进真正的目标:测量 ISMS),以及在开始分析和评价之前,监视和收集宜持续多长时间。

组织可能在更新其测量活动时调整其测量的时间表,以应对 8.2 中列出的具体环境变化。例如,如果组织正在从手动数据源过渡到自动数据源,则可能需要改变收集的频率。此外,需要一个基线来比较在不同时间点实施的、可能使用不同方法但都是为了满足同一信息需求的两组测度。

组织能选择将其监视、测量、分析和评价活动写到一个测量方案中。但是,GB/T 22080没有要求组织要有这样一个方案。

6.5 监视、测量、分析和评价的执行者

组织(考虑到 GB/T 22080—2016中 5.3和 9.1的要求)宜规定负责实施监视、测量、分析和评价的个人或角色。监视、测量、分析和评价可以使用手动或自动的方式进行。无论测量是手动还是自动实施,组织都能规定以下与测量相关的角色和职责。

a) 测量的客户:要求或需要关于 ISMS、控制或控制组的有效性相关的信息的管理层和其他利益相关方。

b) 测量策划者:将可测量属性关联到特定信息需求并完成测量构造的人或部门。

c) 测量评审者:确认已制定的测量构造是否适合于评价信息安全绩效和 ISMS、控制或控制组有效性的人或部门。