ICS 35.040
L 80

# 中华人民共和国国家标准

GB/T 32923—2016/ISO/IEC 27014:2013

# 信息技术　安全技术　信息安全治理

**Information technology—Security techniques—Governance of information security**

(ISO/IEC 27014:2013,IDT)

2016-08-29 发布　　2017-03-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

# 目　　次

# 前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准使用翻译法等同采用 ISO/IEC 27014:2013《信息技术　安全技术　信息安全治理》。

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这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:中电长城网际系统应用有限公司、中国信息安全测评中心、中国电子技术标准化研究院、中国信息安全研究院有限公司。

本标准主要起草人:闵京华、张晓菲、上官晓丽、许玉娜、李斌、罗锋盈、王惠莅、左晓栋、周亚超、刘恒、张兴、李刚、陈洪波、张春明、张劲、刘作康、王琰、王新杰。

# 引　言

本标准提供关于信息安全治理的指南。

信息安全已成为组织的关键问题。不仅法规要求日益增加，而且组织的信息安全措施失效会直接影响其声誉。

因此，组织治理者越来越需要承担起治理责任中的信息安全监督职责，以确保组织目标的实现。

此外，在组织的治理者、执行管理者和负责实现与运行信息安全管理体系人员之间，信息安全治理提供了强有力的纽带。

信息安全治理为在整个组织内推动信息安全行动倡议提供了必不可少的基础。

再者，信息安全的有效治理确保治理者收到在业务语境下形成的信息安全相关活动的报告，从而能够对信息安全问题作出恰当和及时的决策来支持组织的战略目标。

# 信息技术　安全技术　信息安全治理

## 1　范围

本标准就信息安全治理的概念和原则提供指南，通过本标准，组织可以对其范围内的信息安全相关活动进行评价、指导、监视和沟通。

本标准适用于所有类型和规模的组织。

## 2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 29246—2012　信息技术　安全技术　信息安全管理体系　概述和词汇(ISO/IEC 27000：2009，IDT)

## 3　术语和定义

GB/T 29246—2012 界定的以及下列术语和定义适用于本文件。

3.1

**执行管理者　executive management**

为达成组织意图，承担由组织治理者委派的战略和策略实现责任的个人或一组人。

注 1：执行管理者构成最高管理层的一部分。为明晰角色，本标准在最高管理层内区分两组人员：治理者和执行管理者。

注 2：执行管理者可包括首席执行官/行政总裁(CEO)、政府机构领导、首席财务官/财务总监(CFO)、首席运营官/运营总监(COO)、首席信息官/信息总监(CIO)、首席信息安全官/信息安全总监(CISO)和类似的角色。

3.2

**治理者　governing body**

对组织的绩效和合规负有责任的个人或一组人。

注：治理者构成最高管理层的一部分。为明晰角色，本标准在最高管理层内区分两组人员：治理者和执行管理者。

3.3

**信息安全治理　governance of information security**

指导和控制组织信息安全活动的体系。

3.4

**利益相关者　stakeholder**

对于组织活动能够产生影响、受到影响或感觉受到影响的任何个人或组织。

注：决策者可以是利益相关者。

## 4　概念

### 4.1　总则

信息安全治理需要使信息安全目标和战略与业务目标和战略一致，并要求符合法律、法规、规章和