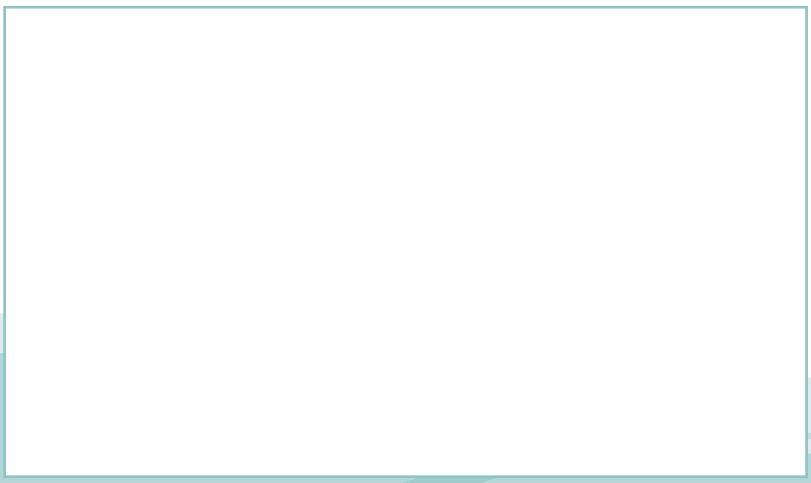
SVENSK STANDARD
SS-ISO/IEC 27011:2018

Fastställd/Approved: 2018-03-13
Publicerad/Published: 2018-03-14
Utgåva/Edition: 1
Språk/Language: engelska/English
ICS: 03.100.70; 35.030

SWEDISH STANDARDS INSTITUTE

Informationsteknik – Säkerhetstekniker – Riktlinjer för informationssäkerhetsåtgärder, baserad på ISO/IEC 27002, för telekomsektorn (ISO/IEC 27011:2016, IDT)

Information technology – Security techniques – Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations (ISO/IEC 27011:2016, IDT)



Standarder får världen att fungera

SIS (Swedish Standards Institute) är en fristående ideell förening med medlemmar från både privat och offentlig sektor. Vi är en del av det europeiska och globala nätverk som utarbetar internationella standarder. Standarder är dokumenterad kunskap utvecklad av framstående aktörer inom industri, näringsliv och samhälle och befrämjar handel över gränser, bidrar till att processer och produkter blir säkrare samt effektiviserar din verksamhet.

Delta och påverka
Som medlem i SIS har du möjlighet att påverka framtida standarder inom ditt område på nationell, europeisk och global nivå. Du får samtidigt tillgång till tidig information om utvecklingen inom din bransch.

Ta del av det färdiga arbetet
Vi erbjuder våra kunder allt som rör standarder och deras tillämpning. Hos oss kan du köpa alla publikationer du behöver – allt från enskilda standarder, tekniska rapporter och standard-paket till handböcker och onlinetjänster. Genom vår webbtjänst e-nav får du tillgång till ett lättnavigerat bibliotek där alla standarder som är aktuella för ditt företag finns tillgängliga. Standarder och handböcker är källor till kunskap. Vi säljer dem.

Utveckla din kompetens och lyckas bättre i ditt arbete
Hos SIS kan du gå öppna eller företagsinterna utbildningar kring innehåll och tillämpning av standarder. Genom vår närhet till den internationella utvecklingen och ISO får du rätt kunskap i rätt tid, direkt från källan. Med vår kunskap om standarders möjligheter hjälper vi våra kunder att skapa verklig nytta och lönsamhet i sina verksamheter.

Vill du veta mer om SIS eller hur standarder kan effektivisera din verksamhet är du välkommen in på www.sis.se eller ta kontakt med oss på tel 08-555 523 00.

Standards make the world go round

SIS (Swedish Standards Institute) is an independent non-profit organisation with members from both the private and public sectors. We are part of the European and global network that draws up international standards. Standards consist of documented knowledge developed by prominent actors within the industry, business world and society. They promote cross-border trade, they help to make processes and products safer and they streamline your organisation.

Take part and have influence
As a member of SIS you will have the possibility to participate in standardization activities on national, European and global level. The membership in SIS will give you the opportunity to influence future standards and gain access to early stage information about developments within your field.

Get to know the finished work
We offer our customers everything in connection with standards and their application. You can purchase all the publications you need from us - everything from individual standards, technical reports and standard packages through to manuals and online services. Our web service e-nav gives you access to an easy-to-navigate library where all standards that are relevant to your company are available. Standards and manuals are sources of knowledge. We sell them.

Increase understanding and improve perception
With SIS you can undergo either shared or in-house training in the content and application of standards. Thanks to our proximity to international development and ISO you receive the right knowledge at the right time, direct from the source. With our knowledge about the potential of standards, we assist our customers in creating tangible benefit and profitability in their organisations.

If you want to know more about SIS, or how standards can streamline your organisation, please visit www.sis.se or contact us on phone +46 (0)8-555 523 00

Den internationella standarden ISO/IEC 27011:2016 gäller som svensk standard. Detta dokument innehåller den officiella engelska versionen av ISO/IEC 27011:2016.

The International Standard ISO/IEC 27011:2016 has the status of a Swedish Standard. This document contains the official version of ISO/IEC 27011:2016.

Upplysningar om sakinnehållet i standarden lämnas av SIS, Swedish Standards Institute, telefon 08-555 520 00. Standarder kan beställas hos SIS som även lämnar allmänna upplysningar om svensk och utländsk standard.

Information about the content of the standard is available from the Swedish Standards Institute (SIS), telephone +46 8 555 520 00. Standards may be ordered from SIS, who can also provide general information about Swedish and foreign standards.

Denna standard är framtagen av kommittén för LIS, SIS/TK 318/AG 11.

Har du synpunkter på innehållet i den här standarden, vill du delta i ett kommande revideringsarbete eller vara med och ta fram andra standarder inom området? Gå in på www.sis.se - där hittar du mer information.

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

This second edition cancels and replaces firs edition of ISO/IEC 27011:2008 which has been technically revised.

ISO/IEC 27011 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27*, IT Security techniques,* in collaboration with ITU-T. The identical text is published as Rec. ITU-T X.1051.

CONTENTS

Introduction

This Recommendation | International Standard provides interpretation guidelines for the implementation and management of information security controls in telecommunications organizations based on ISO/IEC 27002.

Telecommunications organizations provide telecommunications services by facilitating the communications of customers through their infrastructure. In order to provide telecommunications services, telecommunications organizations need to interconnect and/or share their services and facilities and/or use the services and facilities of other telecommunications organizations. Furthermore, the site location, such as radio sites, antenna locations, ground cables and utility provision (power, water), may be accessed not only by the organization's staff, but also by contractors and providers external to the organization.

Therefore, the management of information security in telecommunications organizations is complex, potentially:

- depending on external parties;
- having to cover all areas of network infrastructure, services applications and other facilities;
- including a range of telecommunications technologies (e.g., wired, wireless or broadband);
- supporting a wide range of operational scales, service areas and service types.

In addition to the application of security objectives and controls described in ISO/IEC 27002, telecommunications organizations may need to implement extra controls to ensure confidentiality, integrity, availability and any other security property of telecommunications in order to manage security risk in an adequate fashion.

1) *Confidentiality*

   Protecting confidentiality of information related to telecommunications from unauthorized disclosure. This implies non-disclosure of communications in terms of the existence, the content, the source, the destination and the date and time of communicated information.

   It is critical that telecommunications organizations ensure that the non-disclosure of communications being handled by them is not breached. This includes ensuring that persons engaged by the telecommunications organization maintain the confidentiality of any information regarding others that may have come to be known during their work duties.

   NOTE – The term "secrecy of communications" is used in some countries in the context of "non-disclosure of communications".

2) *Integrity*

   Protecting the integrity of telecommunications information includes controlling the installation and use of telecommunications facilities to ensure the authenticity, accuracy and completeness of information transmitted, relayed or received by wire, radio or any other method.

3) *Availability*

   Availability of telecommunications information includes ensuring that access to facilities and the medium used for the provision of communication services is authorized, regardless of whether communications is provided by wire, radio or any other method. Typically, telecommunications organizations give priority to essential communications in case of emergencies, managing unavailability of less important communications in compliance with regulatory requirements.

Audience

The audience of this Recommendation | International Standard consists of telecommunications organizations and those responsible for information security; together with security vendors, auditors, telecommunications terminal vendors and application content providers. This Recommendation | International Standard provides a common set of general security control objectives based on ISO/IEC 27002, telecommunications sector-specific controls and information security management guidelines allowing for the selection and implementation of such controls.

INTERNATIONAL STANDARD
ITU-T RECOMMENDATION

Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations

1 Scope

The scope of this Recommendation | International Standard is to define guidelines supporting the implementation of information security controls in telecommunications organizations.

The adoption of this Recommendation | International Standard will allow telecommunications organizations to meet baseline information security management requirements of confidentiality, integrity, availability and any other relevant security property.

2 Normative references

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

- ISO/IEC 27000, *Information technology – Security techniques – Information security management systems – Overview and vocabulary.*
- ISO/IEC 27002:2013, *Information technology – Security techniques – Code of practice for information security controls.*

3 Definitions and abbreviations

3.1 Definitions

For the purposes of this Recommendation | International Standard, the definitions given in ISO/IEC 27000 and the following apply:

3.1.1 co-location: Installation of telecommunications facilities on the premises of other telecommunications carriers.

3.1.2 communication centre: Building where facilities for providing telecommunications business are sited.

3.1.3 essential communications: Communications whose contents are necessary for the prevention of or relief from disasters and for the maintenance of public order in adverse conditions.

3.1.4 non-disclosure of communications: Requirement not to disclose the existence, the content, the source, the destination and the date and time of communicated information.

3.1.5 priority call: Telecommunications made by specific terminals in the event of emergencies, which should be handled with priority by restricting public calls.

NOTE – The specific terminals may span different services (voice over Internet protocol (VoIP), public switched telephone network (PSTN) voice, Internet protocol (IP) data traffic, etc.) for wired and wireless networks.

3.1.6 telecommunications applications: Applications such as Voice over IP (VoIP) that are consumed by end-users and built upon the network based services.

3.1.7 telecommunications business: Business to provide telecommunications services in order to meet the demand of others.

3.1.8 telecommunications equipment room: A secure location or room within a general building where equipment for providing telecommunications business are sited.

3.1.9 telecommunications facilities: Machines, equipment, wire and cables, physical buildings or other electrical facilities for the operation of telecommunications.