

Padrões e Conformidade

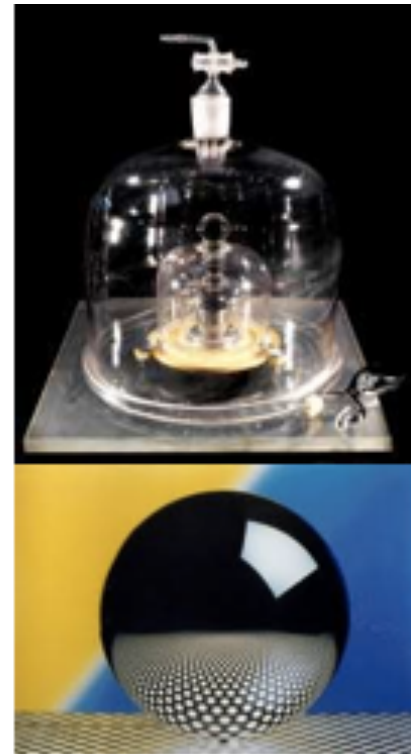
Padronização e Avaliação da
Conformidade na Área de Segurança





Que padrões...?

- › Padrões de referência de grandezas físicas
- › Padrões de segurança cibernética:
 - Definições claras e rigorosas das "referências"
 - Padrão versus norma
- › Exemplos de padrões
 - Algoritmo criptográficos (ex. AES)
 - Segurança de Hardware (ex. FIPS 140-2)
 - Arcabouço de gestão de riscos (ex. NIST CSF)
 - Esquemas de validação de software (ex. CC)
 - Sistema de Gestão de Segurança da Informação (ex. 27001)
 - Auditoria de Laboratórios (NVLAP Handbooks 150-17)



FIPS PUB 140-2

[CHANGE NOTICE \(03-01-2001\)](#)

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION
Supersedes FIPS PUB 140-1, 1994 January 11)

SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES

CATEGORY: COMPUTER SECURITY

SUBCATEGORY: CRYPTOGRAPHY

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

Issued May 25, 2001



U.S. Department of Commerce
Ronald L. Evans, Secretary

Technology Administration
Nancy J. Suss, Under Secretary for Technology

National Institute of Standards and Technology
John E. Simon, Jr., Director



Common Criteria

Common Criteria for Information Technology Security Evaluation

Part 1: Introduction and general model

April 2017

Version 3.1
Revision 5

Federal Information
Processing Standards Publication 197

November 26, 2001

Announcing the ADVANCED ENCRYPTION STANDARD (AES)

Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) and the Computer Security Act of 1987 (Public Law 100-215).

INTERNATIONAL
STANDARD

ISO/IEC
27001

First edition
2005-11-15

Information technology — Security
techniques — Information security
management systems — Requirements

Techniques de l'information — Techniques de sécurité — Systèmes
de gestion de sécurité de l'information — Exigences

Framework for Improving Critical Infrastructure Cybersecurity

Draft Version 1.1

National Institute of Standards and Technology

January 10, 2017

Reference Number
ISIRI-2017-0046

© January 2017



Histórico da Padronização

- › Padrões de medidas usados desde a antiguidade
 - Controle metrológico já existia no vale indu
- › Padronização de porcas e parafusos – séc. XVIII
- › Organizações Nacionais de Padronização – séc. XX
 - 1901: Engineering Standards Committee (Inglaterra)
 - 1917: Deutsches Institut für Normung (Alemanha)
 - 1918: American National Standard Institute (EUA)
 - 1918: Commission Permanente de Standardisation (França)
- › Padronização internacional:
 - formação da IEC (International Electrotechnical Commission) em 1906
 - fundação da ISA (depois ISO) em 1926 (resp. 1946)



Importância da Padronização

- › Padrões representam a convergência técnica entre os maiores especialistas em um assunto
 - Descrevem as melhores práticas em relação àquele assunto
- › Definem uma base conceitual e nomenclatura comum
 - Facilitam comunicação, medição, comércio e interoperabilidade
- › Promovem boas práticas para a economia:
 - facilitam a interação entre empresas
 - facilitam a conformidade a leis e regulações
 - aceleram a introdução de inovações
 - promovem a interoperabilidade entre produtos, serviços e processos – novos e existentes



Princípios para desenvolvimento de padrões

- › Padrões devem ser uma resposta a uma necessidade do mercado ou da sociedade
 - Para serem efetivos, padrões devem ser criados como uma resposta a uma necessidade de um setor do mercado ou da sociedade.
- › Padrões devem ser baseados na opinião de especialistas
 - Bons padrões envolvem uma forte participação e liderança de especialistas, os quais negociam todos os detalhes técnicos dos padrões
- › Padrões devem ser desenvolvidos numa base "multi-stakeholder"
 - Comitês técnicos responsáveis pelo desenvolvimento de padrões devem incluir especialistas do Governo, Indústria, Academia, Consumidores, Organizações Não-Governamentais e Sociedade, em geral.
- › Padrões devem ser baseados em consenso
 - Comentários de todos os stakeholders devem ser levados em consideração



Padronização de Telecom

- › ITU-T (ITU Telecommunication Standardization Sector)
 - 17-mai-1865: assinatura da Convention Télégraphique Internationale de Paris
 - › Padrões elétricos e operacionais de telefones e telégrafos
 - › Posteriormente, comunicações por rádio
 - Início do Século XX: CCIF, CCIR CCIT
 - 1956: CCITT (Comité Consultatif International Téléphonique et Télégraphique)
 - 1993: ITU-T
- › Histórico: padronização de aspectos físicos e elétricos de equipamentos de telecom



Padronização em TIC

- › Organizações internacionais formais
 - ISO/IEC, ITU-T
- › Outros fóruns internacionais
 - IETF
- › Organizações regionais relevantes
 - IEEE, ETSI
- › Instituições de Governos Nacionais relevantes
 - NIST, BSI, ANSSI
- › Instituições setoriais relevantes
 - PCI SSC, NERC



IEEE-SA

- › Institute of Electrical and Electronics Engineers Standards Association
- › Padrões em diversas áreas: TI, telecom, energia,...
- › Exemplos:
 - 802 Local Area Network (LAN)/Metropolitan Area Network (MAN) Standards Committee
 - tecnologias de rede: wifi (802.11), Bluetooth, Wimax,...



IETF

- › Internet Engineering Task-Force
- › Evolução da arquitetura da internet e operação da internet
- › Publica RFCs (Requests for Comments)
- › Exemplos:
 - Domain Name System (DNS) security, authentication protocols, routing protocol security, Internet Protocol (IP) version 6, public key infrastructure, e-mail security, event logging, network traffic encryption



ISO

- › International Organization for Standardization
- › Mais de 150 países membros
- › Aborda padrões de todas as áreas
- › Padrões de elétrica/eletrônica são desenvolvidos em conjunto com IEC (JTC1)
- › Exemplos:
 - Grupo SC17: cartões de identificação e identificação pessoal
 - Grupo SC27: técnicas de segurança de TI
 - Grupo SC31: identificação automática e captura de dados
 - Grupo SC37: padrões biométricos



Standards catalogue

35.030 - IT Security ^o

Including encryption

Filter: Published standards Standards under development Withdrawn standards Projects deleted

Standard and/or project (265)	Stage	TC
<input checked="" type="checkbox"/> IWA 17:2014 Information and operations security and integrity requirements for lottery and gaming organizations	90.93	ISO/TMBG
<input checked="" type="checkbox"/> ISO/IEC 7064:2003 Information technology -- Security techniques -- Check character systems	90.93	ISO/IEC JTC 1/SC 27
<input checked="" type="checkbox"/> ISO/IEC 9796-2:2010 Information technology -- Security techniques -- Digital signature schemes giving message recovery -- Part 2: Integer factorization based mechanisms	90.93	ISO/IEC JTC 1/SC 27
<input checked="" type="checkbox"/> ISO/IEC 9796-3:2007	90.93	ISO/IEC JTC 1/SC 27



ITU-T

- › ITU Telecommunication Standardization Sector
- › Produz padrões chamados *Recommendations*, para redes de comunicação
- › O grupo de estudo 17 (SG17) coordena os trabalhos relacionados a segurança entre todos os grupos de estudo do ITU-T.
- › Exemplos:
 - X.800: Security architecture for Open Systems Interconnection for CCITT applications
 - Recommendation ITU-T X.509 for electronic authentication over public networks



Padronização e Avaliação da Conformidade

- › Padrões frequentemente têm foco nos "requisitos"
 - Mas é importante saber avaliar se os padrões estão sendo alcançados
- › Testes de conformidade permitem avaliar o atendimento aos requisitos de um padrão
 - Realizados através de ensaios, inspeções, auditorias etc.
- › Avaliação da Conformidade têm seus próprios padrões (ISO série 17000)



Padronização versus Obscutantismo





Obscurantismo

- › Princípio através do qual se protege a Segurança de um sistema por meio do Segredo/Sigilo dos seus detalhes de implementação
- › Conceito predominante até o século XIX por meio da esteganografia
- › O tratamento cada vez mais “científico” da Segurança Cibernética - apoiado por disciplinas como Criptografia, Complexidade Computacional, Especificação Formal... - tem relegado o obscurantismo a uma posição bastante restrita.
- › O conceito ainda é bastante difundido em setores como Governo, Diplomacia, Militar/Defesa...





Padronização versus obscurantismo

- › Padronização versus obscurantismo: uma decisão técnica e política
 - Obscurantismo tem seu lugar em aplicações específicas
 - Mas para a maioria das aplicações, não é prático ou realístico
- › Desvantagens do obscurantismo
 - Não pode ser garantida ao longo do tempo
 - › Equipamentos criptográficos podem ser capturados por inimigo
 - › Desenvolvedores de software mudam de empresa (para o concorrente!)
 - Reduz a visibilidade pelos usuários a respeito das funcionalidades do sistema
 - › Como se ter certeza de que um equipamento sensível não está sujeito a manipulações?



Princípios de Criptografia de Kerckhoff

> DESIDERATA DE LA CRYPTOGRAPHIE MILITAIRE

JOURNAL

DES

SCIENCES MILITAIRES.

Janvier 1883.

LA CRYPTOGRAPHIE MILITAIRE.

1° Le système doit être matériellement, sinon mathématiquement, indéchiffrable ;

2° Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi ;

3° La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants ;

4° Il faut qu'il soit applicable à la correspondance télégraphique ;

5° Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes ;

6° Enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.



Por que padrões...

- › Permitem "refletir" para soluções locais as referências e boas práticas internacionais
- › Padrões forçam o exercício do método científico
 - Descrição rigorosa de conceitos, requisitos e métodos
 - Compreensão plena e domínio técnico
- › Padrões facilitam a propagação de informação
 - Estimulam a implantação de soluções de segurança
 - Caso do DES



Requisitos do Data Encryption Standard

- › The algorithm must provide a high level of security.
- › The algorithm must be completely specified and easy to understand.
- › The security of the algorithm must reside in the key; the security should not depend on the secrecy of the algorithm.
- › The algorithm must be available to all users.
- › The algorithm must be adaptable for use in diverse applications.
- › The algorithm must be economically implementable in electronic devices.
- › The algorithm must be efficient to use.
- › The algorithm must be able to be validated.
- › The algorithm must be exportable.



Impacto do Data Encryption Standard

- › *These standards were unprecedented. Never before had an NSA-evaluated algorithm been made public. [...] DES did more to galvanize the field of cryptanalysis than anything else. Now there was an algorithm to study: one that the NSA said was secure.*

Bruce Schneier, Applied Cryptography



Auditibilidade

- › Possibilidade de analisar todas as características e os detalhes de implementação de um sistema
- › A estrutura de Padronização Técnica e Avaliação da Conformidade leva o conceito de auditibilidade a um novo patamar
 - Modelos avaliação de riscos e especificação de requisitos são padronizadas
 - Metodologias de avaliação da conformidade - ensaios e testes de segurança - são claramente especificados
 - Até mesmo os procedimentos de auditoria são claramente descritos

Exemplo de Padrão (AES)

Exemplo saudável de transição
Academia -> Governo -> Indústria





Authors:
Joan Daemen
Vincent Rijmen

The Rijndael Block Cipher

AES Proposal

AES Proposal: Rijndael

Joan Daemen, Vincent Rijmen

Joan Daemen
Proton World Int.l
Zweefvliegtuigstraat 10
B-1130 Brussel, Belgium
daemen.j@protonworld.com

Vincent Rijmen
Katholieke Universiteit Leuven, ESAT-COSIC
K. Mercierlaan 94
B-3001 Heverlee, Belgium
vincent.rijmen@esat.kuleuven.ac.be

**Federal Information
Processing Standards Publication 197**

November 26, 2001

**Announcing the
ADVANCED ENCRYPTION STANDARD (AES)**

Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) and the Computer Security Act of 1987 (Public Law 100-235).

1. Name of Standard. Advanced Encryption Standard (AES) (FIPS PUB 197).

6. Applicability. This standard may be used by Federal departments and agencies when an agency determines that sensitive (unclassified) information (as defined in P. L. 100-235) requires cryptographic protection.

Other FIPS-approved cryptographic algorithms may be used in addition to, or in lieu of, this standard. Federal agencies or departments that use cryptographic devices for protecting classified information can use those devices for protecting sensitive (unclassified) information in lieu of this standard.

In addition, this standard may be adopted and used by non-Federal Government organizations. Such use is encouraged when it provides the desired security for commercial and private organizations.



International Organization for Standardization

Great things happen when the world agrees

Standards | All about ISO | Taking part | **Store**

Search

Standards catalogue | Publications and products

Home > Store > Standards catalogue > Browse by ICS > 35 > 35.030 > ISO/IEC 18033-3:2010

ISO/IEC 18033-3:2010 [Preview](#)

Information technology -- Security techniques -- Encryption algorithms -- Part 3: Block ciphers



This standard was last reviewed and confirmed in 2016. Therefore this version remains current.

ISO/IEC 18033 specifies encryption systems (ciphers) for the purpose of data confidentiality.

ISO/IEC 18033-3:2010 specifies block ciphers. A block cipher is a symmetric encipherment system with the property that the encryption algorithm operates on a block of plaintext, i.e. a string of bits of a defined length, to yield a block of ciphertext.

ISO/IEC 18033-3:2010 specifies following algorithms:

- 64-bit block ciphers: TDEA, MISTY1, CAST-128, HIGHT;
- 128-bit block ciphers: AES, Camellia, SEED.

NOTE The primary purpose of encryption (or encipherment) techniques is to protect the confidentiality of stored or transmitted data. An encryption algorithm is applied to data

Buy this standard

Format

Language

PDF

English

Paper

English

CHF 178 [Buy](#)

Got a question?

[Check out our FAQs](#)

Na prática

Onde esses "padrões de segurança" estão sendo aplicados?



Exemplo de aplicação: ICP-Brasil



Cartão utilizado para assinar documento e leitora usada para ler o cartão...



Atendem a requisitos definidos por padrões internacionais



Bureau International des Poids et Mesures



Equipamentos



Processos



Pessoas



Avaliados por laboratórios acreditados



Equipamentos que sofrem este tipo de avaliação no Brasil

Medidores Inteligentes



Equipamentos Criptográficos



Reg. Eletr. de Ponto



ABOUT THE CA/BROWSER FORUM

The CA/Browser Forum is governed by [Bylaws](#), which were first adopted in 2012. The Bylaws set forth the qualifications for [Membership in the Forum](#), and the types of participation that are allowed for non-voting members, interested parties, and others. The Forum is an unincorporated association of separate organizations.

to search type and hit enter

RECENT NEWS

- [Ballot Forum-9: Bylaws and Server Certificate Working Group Charter Updates May 21, 2019](#)
- [Ballot SC19: Phone Contact with DNS CAA Phone Contact v2 May 21, 2019](#)
- [Ballot SC17 version 7: Alternative registration numbers for EV certificates May 21, 2019](#)

Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates

6.2.7. Private Key Storage on Cryptographic Module

The CA SHALL protect its Private Key in a system or device that has been validated as meeting at least FIPS 140 level 3 or an appropriate Common Criteria Protection Profile or Security Target, EAL 4 (or higher), which includes requirements to protect the Private Key and other assets against known threats.



Outro exemplo: certificação de pessoas

- › Reconhecimento formal dos conhecimentos, habilidades, atitudes e competências do trabalhador, requeridos pelo sistema produtivo e definidos em termos de padrões ou normas acordadas.
[Glossário de Termos Técnicos -
Certificação e Avaliação de Competências (OIT / MTE)]
- › Reconhecimento formal por um organismo de certificação, de que uma pessoa atende a requisitos estabelecidos em normas específicas
[Texto-base do projeto ABNT/CEE-99 -
Terminologia para Certificação de pessoas]



Certificação de pessoas

› Avaliação de evidências

- Treinamento (frequência a um curso) - evidenciado por diploma ou certificado
- Experiência (tempo de atuação na área) - evidenciada por declarações e contratos de trabalho

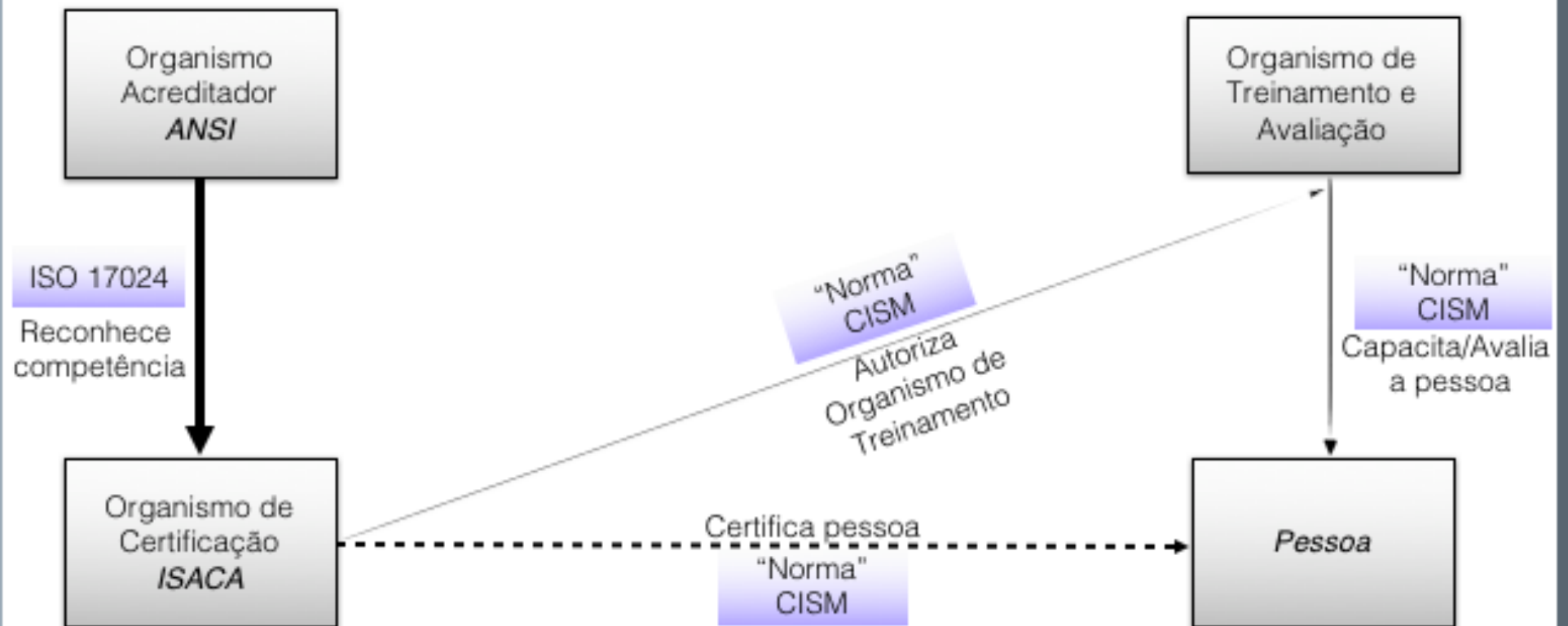


› Examinação de competência

- Exame teórico sobre campo específico do conhecimento
- Prova prática em condições reais de atuação



Exemplo de esquema de certificação de pessoas: ISACA/CISM





Certificação de pessoas - OCP

The screenshot shows the ANSI website with a navigation bar and a sidebar. The main content area displays accreditation information for the Information Systems Audit and Control Association (ISACA).


Information Systems Audit and Control Association

ANSI Accreditation ID: 0494

Organization: Information Systems Audit and Control Association
3701 Algonquin Road, Suite 1050, Rolling Meadows, IL, 60008, United States

Letter Code: ISACA

Website: <http://www.isaca.org>

Accreditation Certificate:  CMJCEQMM

Scope	Granted	Valid Through
Certified in Risk And Information Systems Control (CRISC)	12/4/2013	9/8/2020
Certified in The Governance Of Enterprise IT (CGEIT)	4/23/2011	9/8/2020
Certified Information Security Manager (CISM)	9/8/2005	9/8/2020
Certified Information Systems Auditor (CISA)	9/8/2005	9/8/2020

The image shows a formal ANSI Certificate of Accreditation. It features the ANSI logo at the top and bottom, and a signature in the center. The text on the certificate reads:

CERTIFICATE of ACCREDITATION
PERSONNEL CERTIFICATION

The American National Standards Institute hereby certifies that

Information Systems Audit and Control Association
3701 Algonquin Road, Suite 1050, Rolling Meadows, IL 60008, USA

ACCREDITATION NUMBER:
0494

meets the ANSI accreditation program requirements and those set forth in

ANSI/ISO/IEC 17024 General requirements for bodies operating certification systems of persons

for programs within the following

SCOPE OF ACCREDITATION:
ISO/IEC 17024-1:2003 Certified Risk and Information Systems Control (CRISC)
ISO/IEC 17024-1:2003 Certified the Governance of Enterprise IT (CGEIT)
ISO/IEC 17024-1:2003 Certified Information Security Manager (CISM)
ISO/IEC 17024-1:2003 Certified Information Systems Auditor (CISA)

James Hallenbeck
ANSI ACCREDITATION COORDINATOR

2014-09-08
0494-0001



Certificação de pessoas – Profissional



Padrões importantes para Segurança da Informação

Common Criteria, FIPS 140-2,
ISO/IEC série 27000, ISO série 17000



Common Criteria

ISO/IEC 15408





Padrões ISO/IEC Common Criteria

- › ISO/IEC 15408-1:2009
 - Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model
- › ISO/IEC 15408-2:2008
 - Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components
- › ISO/IEC 15408-3:2008
 - Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance components



Objetivo do Common Criteria

- › Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard and repeatable manner at a level that is commensurate with the target environment for use.

THE COMMON CRITERIA

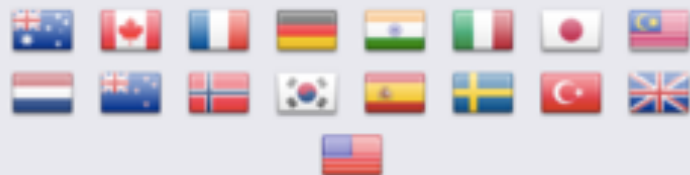
Common Criteria

The [Common Criteria for Information Technology Security Evaluation](#) (CC), and the companion [Common Methodology for Information Technology Security Evaluation](#) (CEM) are the technical basis for an international agreement, the [Common Criteria Recognition Arrangement](#) (CCRA), which ensures that:

- [Products](#) can be evaluated by competent and independent [licensed laboratories](#) so as to determine the fulfilment of particular security properties, to a certain extent or assurance;
- [Supporting documents](#), are used within the Common Criteria certification process to define how the criteria and evaluation methods are applied when certifying specific technologies;
- The certification of the security properties of an evaluated product can be issued by a number of [Certificate Authorizing Schemes](#), with this certification being based on the result of their evaluation;
- [These certificates](#) are recognized by all the signatories of the [CCRA](#).

The CC is the driving force for the widest available mutual recognition of secure IT products. This web portal is available to support the information on the status of the CCRA, the CC and the certification schemes, licensed laboratories, certified products and related information, news and events.

Certificate Authorizing Members



Certificate Consuming Members



CC v3.1. Release 5

Click [here](#) for information about the CC/CEM maintenance process.

CC v3.1 Release 5 consists of three parts. Make sure to download and use these files:

Part 1: Introduction and general model

PDF

 [CCPART1V3.1R5.pdf](#)

 [CCPART1V3.1R5_marked_changes.pdf](#)

Part 2: Security functional requirements

 [CCPART2V3.1R5.pdf](#)

 [CCPART2V3.1R5_marked_changes.pdf](#)

Part 3: Security assurance requirements

 [CCPART3V3.1R5.pdf](#)

 [CCPART3V3.1R5_marked_changes.pdf](#)

CEM v3.1 consists of one part:

PDF

CEM

 [CEMV3.1R5.pdf](#)

CEM

 [CEMV3.1R5_marked_changes.pdf](#)

Addenda to the CC and CEM

 [CCDB-2017-05-17-CCaddenda-Exact_Conformance.pdf](#)

INTERNATIONAL
STANDARD

ISO/IEC
15408-1

Third edition
2009-12-15

Corrected version
2014-01-15

**Information technology — Security
techniques — Evaluation criteria for IT
security —**

**Part 1:
Introduction and general model**

*Technologies de l'information — Techniques de sécurité — Critères
d'évaluation pour la sécurité TI — Partie 1: Introduction et modèle
général*

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.

ISO/IEC 15408-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*. The identical text of ISO/IEC 15408 is published by the Common Criteria Project Sponsoring Organisations as Common Criteria for Information Technology Security Evaluation. The common XML source for both publications can be found at <http://www.commoncriteriaportal.org/cc/>

This third edition cancels and replaces the second edition (ISO/IEC 15408-1:2005), which has been technically revised.

ISO/IEC 15408 consists of the following parts, under the general title *Information technology — Security techniques — Evaluation criteria for IT security*:

- *Part 1: Introduction and general model*
- *Part 2: Security functional components*
- *Part 3: Security assurance components*

This corrected version of ISO/IEC 15408-1:2009 incorporates miscellaneous editorial corrections related to the following:

- terminology: correction for the terms "security problem" and "security domains";
- clause 8.3: explanation of strict conformance, removal of former Figure 4.

Introduction

ISO/IEC 15408 permits comparability between the results of independent security evaluations. ISO/IEC 15408 does so by providing a common set of requirements for the security functionality of IT products and for assurance measures applied to these IT products during a security evaluation. These IT products may be implemented in hardware, firmware or software.

The evaluation process establishes a level of confidence that the security functionality of these IT products and the assurance measures applied to these IT products meet these requirements. The evaluation results may help consumers to determine whether these IT products fulfil their security needs.

ISO/IEC 15408 is useful as a guide for the development, evaluation and/or procurement of IT products with security functionality.

ISO/IEC 15408 is intentionally flexible, enabling a range of evaluation methods to be applied to a range of security properties of a range of IT products. Therefore users of the standard are cautioned to exercise care that this flexibility is not misused. For example, using ISO/IEC 15408 in conjunction with unsuitable evaluation methods, irrelevant security properties, or inappropriate IT products, may result in meaningless evaluation results.

Consequently, the fact that an IT product has been evaluated has meaning only in the context of the security properties that were evaluated and the evaluation methods that were used. Evaluation authorities are advised to carefully check the products, properties and methods to determine that an evaluation will provide meaningful results. Additionally, purchasers of evaluated products are advised to carefully consider this context to determine whether the evaluated product is useful and applicable to their specific situation and needs.

ISO/IEC 15408 addresses protection of assets from unauthorised disclosure, modification, or loss of use. The categories of protection relating to these three types of failure of security are commonly called confidentiality, integrity, and availability, respectively. ISO/IEC 15408 may also be applicable to aspects of IT security outside of these three. ISO/IEC 15408 is applicable to risks arising from human activities (malicious or otherwise) and to risks arising from non-human activities. Apart from IT security, ISO/IEC 15408 may be applied in other areas of IT, but makes no claim of applicability in these areas.

Certain topics, because they involve specialised techniques or because they are somewhat peripheral to IT security, are considered to be outside the scope of ISO/IEC 15408. Some of these are identified below.

- a) ISO/IEC 15408 does not contain security evaluation criteria pertaining to administrative security measures not related directly to the IT security functionality. However, it is recognised that significant security can often be achieved through or supported by administrative measures such as organisational, personnel, physical, and procedural controls.
- b) The evaluation of some technical physical aspects of IT security such as electromagnetic emanation control is not specifically covered, although many of the concepts addressed will be applicable to that area.
- c) ISO/IEC 15408 does not address the evaluation methodology under which the criteria should be applied. This methodology is given in ISO/IEC 18045.
- d) ISO/IEC 15408 does not address the administrative and legal framework under which the criteria may be applied by evaluation authorities. However, it is expected that ISO/IEC 15408 will be used for evaluation purposes in the context of such a framework.

- e) The procedures for use of evaluation results in accreditation are outside the scope of ISO/IEC 15408. Accreditation is the administrative process whereby authority is granted for the operation of an IT product (or collection thereof) in its full operational environment including all of its non-IT parts. The results of the evaluation process are an input to the accreditation process. However, as other techniques are more appropriate for the assessments of non-IT related properties and their relationship to the IT security parts, accreditors should make separate provisions for those aspects.
- f) The subject of criteria for the assessment of the inherent qualities of cryptographic algorithms is not covered in ISO/IEC 15408. Should independent assessment of mathematical properties of cryptography be required, the evaluation scheme under which ISO/IEC 15408 is applied must make provision for such assessments.

ISO terminology, such as "can", "informative", "may", "normative", "shall" and "should" used throughout the document are defined in the ISO/IEC Directives, Part 2. Note that the term "should" has an additional meaning applicable when using this standard. See the note below. The following definition is given for the use of "should" in ISO/IEC 15408.

should

within normative text, "should" indicates "that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required." (ISO/IEC Directives, Part 2).

NOTE ISO/IEC 15408 interprets "not necessarily required" to mean that the choice of another possibility requires a justification of why the preferred option was not chosen.

Information technology – Security techniques – Evaluation criteria for IT security –

Part 1: Introduction and general model

1 Scope

This part of ISO/IEC 15408 establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of the standard which in its entirety is meant to be used as the basis for evaluation of security properties of IT products.

Part one provides an overview of all parts of ISO/IEC 15408 standard. It describes the various parts of the standard; defines the terms and abbreviations to be used in all parts of the standard; establishes the core concept of a Target of Evaluation (TOE); the evaluation context and describes the audience to which the evaluation criteria are addressed. An introduction to the basic security concepts necessary for evaluation of IT products is given.

It defines the various operations by which the functional and assurance components given in ISO/IEC 15408-2 and ISO/IEC 15408-3 may be tailored through the use of permitted operations.

The key concepts of protection profiles (PP), packages of security requirements and the topic of conformance are specified and the consequences of evaluation, evaluation results are described. This part of ISO/IEC 15408 gives guidelines for the specification of Security Targets (ST) and provides a description of the organization of components throughout the model. General information about the evaluation methodology are given in ISO/IEC 18045 and the scope of evaluation schemes is provided.

2 Normative references

The following referenced documents are indispensable for the application of ISO/IEC 15408 part 1. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 15408-2, *Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components*

ISO/IEC 15408-3, *Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components*

ISO/IEC 18045, *Information technology – Security techniques – Methodology for IT security evaluation*



Conceitos-chave





Target of Evaluation (TOE)

- › the product or system that is the subject of the evaluation. The evaluation serves to validate claims made about the target. To be of practical use, the evaluation must verify the target's security features.



Protection Profile (PP)

- › a document, typically created by a user or user community, which identifies security requirements for a class of security devices (for example, smart cards used to provide digital signatures, or network firewalls) relevant to that user for a particular purpose. Product vendors can choose to implement products that comply with one or more PPs, and have their products evaluated against those PPs. In such a case, a PP may serve as a template for the product's ST (Security Target, as defined below), or the authors of the ST will at least ensure that all requirements in relevant PPs also appear in the target's ST document. Customers looking for particular types of products can focus on those certified against the PP that meets their requirements.



Security Target (ST)

- › the document that identifies the security *properties* of the target of evaluation. The ST may claim conformance with one or more PPs. The TOE is evaluated against the SFRs (Security Functional Requirements. Again, see below) established in its ST, no more and no less. This allows vendors to tailor the evaluation to accurately match the intended capabilities of their product. This means that a network firewall does not have to meet the same functional requirements as a **database** management system, and that different firewalls may in fact be evaluated against completely different lists of requirements. The ST is usually published so that potential customers may determine the specific security features that have been certified by the evaluation.



Collaborative Protection Profile (cPP):

- › A Protection Profile collaboratively developed by an International Technical Community endorsed by the Management Committee. A cPP and related Supporting Documents define the minimum set of common security functional requirements and the Achievable Common Level of Security Assurance. It addresses vulnerability analysis requirements to ensure certified products reach an Achievable Common Level of Security Assurance.



Article 2

Scope

It is mutually understood that, with respect to IT Products and Protection Profiles, the Participants plan to Recognise the Common Criteria Certificates which have been authorised by any other Certificate Authorising Participant in accordance with the terms of this Arrangement and in accordance with the applicable laws and regulations of each Participant. This Arrangement covers certificates with claims of compliance against Common Criteria assurance components of either:

- 1) a *collaborative Protection Profile (cPP)*, developed and maintained in accordance with Annex K, with assurance activities selected from Evaluation Assurance Levels up to and including level 4 and ALC_FLR, developed through an *International Technical Community* endorsed by the *Management Committee*; or
- 2) Evaluation Assurance Levels 1 through 2 and ALC_FLR².

The scope may be modified with the consent of the Participants in this Arrangement at any time, in accordance with the provisions of Article 14, by addition or removal of assurance levels or components.

² As detailed in Part 3 of the Common Criteria for Information Technology Security Evaluation.



Security Functional Requirements (SFRs)

- › specify individual security **functions** which may be provided by a product. The Common Criteria presents a standard catalogue of such functions. For example, a SFR may state **how** a user acting a particular **role** might be **authenticated**. The list of SFRs can vary from one evaluation to the next, even if two targets are the same type of product. Although Common Criteria does not prescribe any SFRs to be included in an ST, it identifies dependencies where the correct operation of one function (such as the ability to limit access according to roles) is dependent on another (such as the ability to identify individual roles).



Security Assurance Requirements (SARs)

- › descriptions of the measures taken during development and evaluation of the product to assure compliance with the claimed security functionality. For example, an evaluation may require that all source code is kept in a change management system, or that full functional testing is performed. The Common Criteria provides a catalogue of these, and the requirements may vary from one evaluation to the next. The requirements for particular targets or types of products are documented in the ST and PP, respectively.
- ›



Evaluation Assurance Level (EAL)

- › the numerical rating describing the depth and rigor of an evaluation. Each EAL corresponds to a package of security assurance requirements (SARs, see above) which covers the complete development of a product, with a given level of strictness. Common Criteria lists seven levels, with EAL 1 being the most basic (and therefore cheapest to implement and evaluate) and EAL 7 being the most stringent (and most expensive).



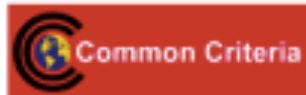
History

- › CC originated out of three standards:
 - ITSEC – The European standard, developed in the early 1990s by France, Germany, the Netherlands and the UK. It too was a unification of earlier work, such as the two UK approaches (the CESG UK Evaluation Scheme aimed at the defence/intelligence market and the DTI Green Book aimed at commercial use), and was adopted by some other countries, e.g. Australia.
 - CTCPEC – The Canadian standard followed from the US DoD standard, but avoided several problems and was used jointly by evaluators from both the U.S. and Canada. The CTCPEC standard was first published in May 1993.
 - TCSEC – The United States Department of Defense DoD 5200.28 Std, called the Orange Book and parts of the Rainbow Series. The Orange Book originated from Computer Security work including the Anderson Report, done by the National Security Agency and the National Bureau of Standards (the NBS eventually became NIST) in the late 1970s and early 1980s. The central thesis of the Orange Book follows from the work done by Dave Bell and Len LaPadula for a set of protection mechanisms.



Testing organizations

- › In Canada, the Standards Council of Canada (SCC) under Program for the Accreditation of Laboratories (PALCAN) accredits Common Criteria Evaluation Facilities (CCEF)
- › In France, the Comité français d'accréditation (fr) (COFRAC) accredits Common Criteria evaluation facilities, commonly called Centre d'évaluation de la sécurité des technologies de l'information (fr) (CESTI). Evaluations are done according to norms and standards specified by the Agence nationale de la sécurité des systèmes d'information (ANSSI).
- › In the UK the United Kingdom Accreditation Service (UKAS) accredits Commercial Evaluation Facilities (CLEF)
- › In the US, the National Institute of Standards and Technology (NIST) National Voluntary Laboratory Accreditation Program (NVLAP) accredits Common Criteria Testing Laboratories (CCTL)
- › In Germany, the Bundesamt für Sicherheit in der Informationstechnik (BSI)
- › In Spain, the National Cryptologic Center (CCN) accredits Common Criteria Testing Laboratories operating in the Spanish Scheme.
- › In The Netherlands, the Netherlands scheme for Certification in the Area of IT Security (NSCIB) accredits IT Security Evaluation Facilities (ITSEF).



ARRANGEMENT
on the
Recognition of Common Criteria Certificates
In the field of
Information Technology Security

July 2, 2014

Purpose of the Arrangement

The *Participants* in this Arrangement share the following objectives:

- a) to ensure that *Evaluations of Information Technology (IT) Products and Protection Profiles* are performed to high and consistent standards, and are seen to contribute significantly to confidence in the security of those products and profiles;
- b) to improve the availability of evaluated, security-enhanced *IT Products and Protection Profiles*;
- c) to eliminate the burden of duplicating *Evaluations of IT Products and Protection Profiles*;
- d) to continuously improve the efficiency and cost-effectiveness of the *Evaluation and Certification/Validation*¹ process for *IT Products and Protection Profiles*.

The purpose of this Arrangement is to advance those objectives by bringing about a situation in which *IT Products and Protection Profiles* which earn a *Common Criteria Certificate*, as per the requirements of the CC standard, can be procured or used without the need for further *Evaluation*. It seeks to provide grounds for confidence in the reliability of the judgements on which the original certificate was based by requiring that a *Certification/Validation Body (CB)* issuing *Common Criteria Certificates* should meet high and consistent standards.



Mutual recognition arrangement

- › As well as the Common Criteria standard, there is also a sub-treaty level Common Criteria MRA (Mutual Recognition Arrangement), whereby each party thereto recognizes evaluations against the Common Criteria standard done by other parties.
- › Originally signed in 1998 by Canada, France, Germany, the United Kingdom and the United States, Australia and New Zealand joined 1999, followed by Finland, Greece, Israel, Italy, the Netherlands, Norway and Spain in 2000.
- › The Arrangement has since been renamed Common Criteria Recognition Arrangement (CCRA) and membership continues to expand




Mutual recognition arrangement

- › Within the CCRA only evaluations up to EAL 2 are mutually recognized (Including augmentation with flaw remediation).
- › The European countries within the former ITSEC agreement typically recognize higher EALs as well. Evaluations at EAL5 and above tend to involve the security requirements of the host nation's government.
- › In September 2012, a majority of members of the CCRA produced a vision statement whereby mutual recognition of CC evaluated products will be lowered to EAL 2 (Including augmentation with flaw remediation). Further, this vision indicates a move away from assurance levels altogether and evaluations will be confined to conformance with Protection Profiles that have no stated assurance level. This will be achieved through technical working groups developing worldwide PPs, and as yet a transition period has not been fully determined.



CCRA new vision

- › Recognition of evaluations against only a collaborative Protection Profile (cPP) or Evaluation Assurance Levels 1 through 2 and ALC_FLR.
- › The emergence of international Technical Communities (iTC), groups of technical experts charged with the creation of cPPs.
- › A transition plan from the previous CCRA, including recognition of certificates issued under the previous version of the Arrangement.



Protections Profiles and Collaborative Protections Profiles



Protection Profiles













[Statistics](#)[Download CSV](#)[Collaborative Protection Profiles](#)[Archived Protection Profiles](#)

[expand/collapse all categories](#)

- [Access Control Devices and Systems – 3 Protection Profiles](#)
- [Biometric Systems and Devices – 2 Protection Profiles](#)
- [Boundary Protection Devices and Systems – 11 Protection Profiles](#)
- [Data Protection – 10 Protection Profiles](#)
- [Databases – 3 Protection Profiles](#)
- [ICs, Smart Cards and Smart Card-Related Devices and Systems – 71 Protection Profiles](#)
- [Key Management Systems – 4 Protection Profiles](#)
- [Mobility – 4 Protection Profiles](#)
- [Multi-Function Devices – 2 Protection Profiles](#)
- [Network and Network-Related Devices and Systems – 12 Protection Profiles](#)
- [Operating Systems – 2 Protection Profiles](#)
- [Other Devices and Systems – 49 Protection Profiles](#)
- [Products for Digital Signatures – 19 Protection Profiles](#)
- [Trusted Computing – 6 Protection Profiles](#)

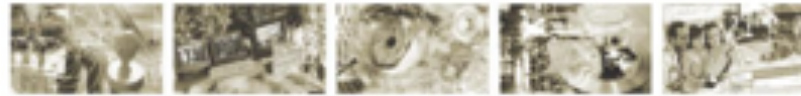
* A cPP without a Certification Report indicates that no determination of compliance to the CC/CEM (APE class) has yet been made. Consequently, the cPP is outside CCRA mutual recognition. Some schemes may certify a cPP upon first use in combination with an IT product evaluation. In that case, an evaluation of an IT product where the Security Target claims compliance to these collaborative Protection Profiles must include the relevant work units related to the ASE class.

Network and Network-Related Devices and Systems – 12 Protection Profiles

Protection Profile	Version	Assurance Level	Issued	Scheme	Certified
Extended Package for SIP Server	2.0	EAL1	2015-12-01	 US	Certification Report
Korean National Protection Profile for Network Device V1.1	1.1	EAL1+ ATE_FUN.1	2017-04-21	 KR	Certification Report
Anforderungen an die Kommunikationsinfrastruktur für sicherheitsrelevante Anwendungen (KISA)	Version 1.0	EAL4+ AVA_VAN.5	2016-08-11	 DE	Certification Report
Smart Meter of Turkish Electricity Advanced Metering Infrastructure Protection Profile	1.1	EAL2+ AVA_VAN.3	2014-09-03	 TR	Certification Report
Protection Profile for the Gateway of a Smart Metering System	Version 1.3	EAL4+ ALC_FLR.2 AVA_VAN.5	2014-04-04	 DE	Certification Report
DCSSI-PP_2008/08 - IP Encryptor (CC3.1), Version 1.0	1.9	EAL3+ ALC_FLR.3 AVA_VAN.3	2008-08-22	 FR	Certification Report
DCSSI-PP_2008/03 - Client VPN Application (CC3.1), Version 1.3	1.3	EAL3+ ALC_FLR.3 AVA_VAN.3	2008-07-10	 FR	Certification Report
Remote-Controlled Browsers Systems (ReCoBS), Version 1.0	1.0	EAL3+	2008-03-31	 DE	Certification Report
Konnektor im elektronischen Gesundheitswesen, Anforderungen an den Netzkonnektor, Version 1.05	1.05	EAL4+	2007-10-09	 DE	Certification Report
Low Assurance Protection Profile for a VPN gateway, Version 1.4	1.4	EAL1	2005-06-15	 DE	Certification Report
Configurable Security Guard (CSG), Version 3.3	3.3	EAL5	1999-04-01	 FR	Certification Report
Application VPN clients / Client VPN Application, Version 1.0	1.0	EAL2+	2006-10-10	 FR	Certification Report



Federal Office
for Information Security



- 1 Protection Profile for the Gateway of a Smart Metering
- 2 System (Smart Meter Gateway PP)
- 3 Schutzprofil für die Kommunikationseinheit eines intelligenten
- 4 Messsystems für Stoff- und Energiemengen

5

6



7

8 **SMGW-PP**

9 **Version 1.3 - 31 March 2014**

10 **(Final Release)**

11 **Certification-ID: BSI-CC-PP-0073**

1 PP introduction

1.1 Introduction

The increasing use of *green energy* and upcoming technologies around e-mobility lead to an increasing demand for functions of a so called smart grid. A smart grid hereby refers to a commodity¹ network that intelligently integrates the behaviour and actions of all entities connected to it – suppliers of natural resources and energy, its consumers and those that are both – in order to efficiently ensure a more sustainable, economic and secure supply of a certain commodity (definition adopted from [CEN]).

In its vision such a smart grid would allow to invoke consumer devices to regulate the load and availability of resources or energy in the grid, e.g. by using consumer devices to store energy or by triggering the use of energy based upon the current load of the grid². Basic features of such a smart use of energy or resources are already reality. Providers of electricity in Germany, for example, have to offer at least one tariff that has the purpose to motivate the consumer to save energy.

In the past, the production of electricity followed the demand/consumption of the consumers. Considering the strong increase in renewable energy and the production of energy as a side effect in heat generation today, the consumption/demand has to follow the – often externally controlled – production of energy. Similar mechanisms can exist for the gas network to control the feed of biogas or hydrogen based on information submitted by consumer devices.

An essential aspect for all considerations of a smart grid is the so called Smart Metering System that meters the consumption or production of certain commodities at the consumer's side and allows sending the information about the consumption or production to external entities, which is then the basis for e.g. billing the consumption or production.

This Protection Profile defines the security objectives and corresponding requirements for a Gateway which is the central communication component of such a Smart Metering System (please refer to chapter 1.4.2 for a more detailed overview). The PP is directed to developers of Smart Meter Gateways and informs them about the requirements that have to be implemented. It is further directed to stakeholders being responsible for purchasing Smart Meter Gateways.

The Target of Evaluation (TOE) that is described in this document is an electronic unit comprising hardware and software/firmware³ used for collection, storage and provision of Meter Data⁴ from one or more Meters of one or multiple commodities.

The Gateway connects a Wide Area Network (WAN) with a Network of Devices of one or more Smart Metering devices (Local Metrological Network, LMN) and the consumer Home Area Network (HAN), which hosts Controllable Local Systems (CLS). The security functionality of the TOE comprises

- protection of confidentiality, authenticity, integrity of data and
- information flow control

mainly to protect the privacy of consumers, to ensure a reliable billing process and to protect the Smart Metering System and a corresponding large scale infrastructure of the smart grid. The availability of the Gateway is not addressed by this PP.

1.2 PP Reference

Title:	Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP)
Version	1.3 (Final Release)
Date	31.03.2014
Authors	Dr. Helge Kreutzmann, M.Sc. Stefan Vollmer (BSI)
Registration	Bundesamt für Sicherheit in der Informationstechnik (BSI) Federal Office for Information Security, Germany
Certification-ID	BSI-CC-PP-0073
Evaluation Assurance Level:	The assurance level for this PP is EAL 4 augmented by AVA_VAN.5 and ALC_FLR.2.
CC-Version	3.1 Revision 4
Keywords	Smart Metering, Protection Profile, Meter, Gateway, PP

Collaborative Protection Profiles (cPP) and Supporting Documents (SD)

The lists below contain collaborative Protection Profiles and related Supporting Documents developed openly by international Technical Communities (ITC) consisting of vendors, test laboratories, CCRA nations, and academia.

cPPs with SDs that have completed review by the CCDB for compliance with the CC and CEM

The cPPs below include SDs that have completed CCDB review for compliance with the CC and CEM and are therefore available for use under the terms of the [Common Criteria Recognition Arrangement \(CCRA\)](#). Evaluations conducted against cPPs on this list are mutually recognized according to the terms of the CCRA.

<This list currently has no items.>

cPPs with SDs that are currently being reviewed by the CCDB for compliance with the CC and CEM

The following list contains collaborative Protection Profiles (cPPs) available for use. However, each Supporting Document (SD) listed below is currently being reviewed by the CCDB for compliance with the CC and the CEM. These documents are made available here in order to assist the ITC and to enable evaluations to take place as quickly as possible while the (necessarily thorough) CCDB review and voting process takes place. Not all schemes need to use these documents (although national endorsement statements may of course mandate their use). Those that do are encouraged to share experiences/recommendations with the ITC.

Products evaluated and certified using these documents are mutually recognized under the CCRA since the scheme performing the evaluation will ensure consistency with the CC and the CEM. Should the wider CCDB review find that an SD is not fully compliant; the ITC will be given notice of the necessary changes and a reasonable time to incorporate these before resubmitting to the CCDB review process. If an SD requires multiple CCDB reviews prior to approval, until the SDs are approved, the non-compliant parts of the SDs will be replaced by CEM activities. Once the documents have been approved by the CCDB they will be moved to the upper section and become mandatory.

[expand/collapse all categories](#)

☰ [Boundary Protection Devices and Systems – 2 Protection Profiles](#)

☰ [Data Protection – 5 Protection Profiles](#)

☰ [Network and Network-Related Devices and Systems – 2 Protection Profiles](#)

* A cPP without a Certification Report indicates that no determination of compliance to the CC/CEM (APE class) has yet been made. Consequently, the cPP is outside CCRA mutual recognition. Some schemes may certify a cPP upon first use in combination with an IT product evaluation. In that case, an evaluation of an IT product where the Security Target claims compliance to these collaborative Protection Profiles must include the relevant work units related to the ASE class.

■ Network and Network-Related Devices and Systems – 2 Protection Profiles

Protection Profile	Version	Assurance Level	Issued	Certified
<p>collaborative Protection Profile for Network Devices v2.0 + Errata 20180314</p> <ul style="list-style-type: none">• Protection Profile• Supporting Document• Endorsement Statement	2.0E	None	2018-03-14	Certification Report
<p>collaborative Protection Profile for Network Devices v1.0</p> <ul style="list-style-type: none">• Protection Profile• Supporting Document• Endorsement Statement	1.0	None	2015-02-27	Certification Report

collaborative Protection Profile for Network Devices v2.0 + Errata 20180314 Endorsement Statements

An important aspect of the cPP development process is that it encourages each CCRA Participant to make a public statement about their interest in the development and use of each cPP, through the creation of a Position Statement (PS) and, after the publication of the cPP, an Endorsement Statement (ES). These statements are intended to make clear the views of the CCRA Participant on the need for the relevant cPP, and the suitability of the interim deliverables (the ESR, SPD, etc.) to match the CCRA Participant's national requirements. This enables ITC members to make an informed estimate of the benefits that will justify their participation in the ITC.

At its most general level, an Endorsement Statement is a formal statement of commitment to a finalized cPP, with a description of how that commitment is realized (e.g. by listing conformance with the cPP as a mandatory, preferred or recommended procurement requirement for certain types of equipment and/or placing conformant products on an 'approved product list'). By contrast, a Position Statement allows free-format comment on a cPP/SD, or the interim deliverables from an ITC, but does not represent a formal commitment by its author.

Both Position Statements and Endorsement Statements may relate to one or more cPPs. If a statement relates to more than one cPP, then the content of the statement must identify which cPPs it relates to.

Endorsement Statements

Links to the endorsement statements are provided below:

- NIAP (United States): [Endorsement Statement](#)
- AISEP (Australia & New Zealand): [Endorsement Statement](#)



National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

NIAP CCEVS Endorsement Statement
Network Device collaborative Protection Profile
Version 2.0, dated 5 May 2017

6 July 2017
Version 1.0

STATEMENT: NIAP endorses the Network Device (ND) collaborative Protection Profile (cPP) Version 2.0, dated 5 May 2017. NIAP anticipates updates to this version of the cPP based on the ongoing TLS and NTP subgroup efforts and expects timely publication of a minor revision.

With this endorsement, products successfully evaluated against the ND cPP that demonstrate exact conformance to the cPP, and in compliance with all NIAP policies, will be placed on the NIAP Product Compliant List: https://www.niap-ccevs.org/CCEVS_Products/pcl.cfm

PURPOSE: The intent of this Endorsement Statement is to make it publicly known that NIAP CCEVS:

- recognizes a need for evaluated devices that are suitable for the use cases identified in the ND cPP, to include distributed network devices;
- considers the Security Problem Definition and resulting Security Functional Requirements appropriate for the intended use cases; and,
- believes the ND cPP's companion Supporting Document (SD) specifies objective, repeatable Evaluation Activities that are appropriate for the intended environment, and will produce comparable results.

SCOPE: NIAP will revisit its endorsement during each release of the ND cPP and SD. If NIAP continues to endorse subsequent releases of the ND cPP, an updated Endorsement Statement will be published.

Original Signed By

JANINE S. PEDERSEN
Director, NIAP

9800 Savage Road, STE 6940, Ft. Meade, MD 20755-6940
Phone: (410) 854-4458 Fax: (410) 854-6615
E-mail: scheme-comments@niap-ccevs.org
<http://www.niap-ccevs.org/cc-scheme>



Australian Government
Department of Defence

DEF: 00000000

AISEP ENDORSEMENT STATEMENT

**Network Device collaborative Protection Profile
Version 2.0, dated 05 May 2017**

1. The Australian Certification Authority (ACA) formally endorses the Network Device (ND) collaborative Protection Profile (cPP) Version 2.0, dated 05 May 2017.
2. The ACA recognises a need for evaluated devices that are suitable for the use cases identified in the ND cPP. The ACA believes that the ND cPP meets the intent of the ESR and considers the Security Problem Definition and resulting Security Functional Requirements appropriate for the intended use cases.
3. Products successfully evaluated against the ND cPP that demonstrate exact conformance (exact conformance is addressed under Addenda to the CC and CEM: CCDR-2017-05-17) to the cPP, and in compliance with all AISEP policies, will be placed on the ASD's Evaluated Products List (EPL): <https://www.asd.gov.au/infosec/epi/index.php>
4. The ACA will revisit its endorsement during each release of the ND cPP and Supporting Document (SD). If the ACA continues to endorse subsequent releases of the ND cPP and SD, an updated Endorsement Statement will be published.

Original Signed By

Hia Khan
Manager and Principal Certifier
Australian Certification Authority
Australian Information Security Evaluation Program

Department of Defence
PO BOX 5076
KINGSTON ACT 2604

<http://www.asd.gov.au/infosec/aisep/>

6 March 2018

collaborative Protection Profile for Network Devices

Version 2.0 + Errata 20180314

14-March-2018

0. Preface

0.1 Objectives of Document

This document presents the Common Criteria (CC) collaborative Protection Profile (cPP) to express the security functional requirements (SFRs) and security assurance requirements (SARs) for a network device. The Evaluation Activities that specify the actions the evaluator performs to determine if a product satisfies the SFRs captured within this cPP are described in [SD].

0.2 Scope of Document

The scope of the cPP within the development and evaluation process is described in the Common Criteria for Information Technology Security Evaluation [CC]. In particular, a cPP defines the IT security requirements of a generic type of TOE and specifies the functional and assurance security measures to be offered by that TOE to meet stated requirements [CC1, Section C.1].

0.3 Intended Readership

The target audiences of this cPP are developers, CC consumers, system integrators, evaluators and schemes.

Although the cPPs and SDs may contain minor editorial errors, cPPs are recognized as living documents and the ITCs are dedicated to ongoing updates and revisions. Please report any issues to the NDFW ITC.

0.4 Related Documents

Common Criteria¹

- [CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2012-09-001, Version 3.1 Revision 4, September 2012.
- [CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, CCMB-2012-09-002, Version 3.1 Revision 4, September 2012.
- [CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, CCMB-2012-09-003, Version 3.1 Revision 4, September 2012.
- [CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1, Revision 4, September 2012.

Other Documents

- [SD] Evaluation Activities for Network Device cPP, Version 2.0

collaborative Protection Profile for

0.1 Objectives of Document

This document presents the Common Criteria (CC) collaborative Protection Profile (cPP) to express the security functional requirements (SFRs) and security assurance requirements (SARs) for a network device. The Evaluation Activities that specify the actions the evaluator performs to determine if a product satisfies the SFRs captured within this cPP are described in [SD].

0.2 Scope of Document

The scope of the cPP within the development and evaluation process is described in the Common Criteria for Information Technology Security Evaluation [CC]. In particular, a cPP defines the IT security requirements of a generic type of TOE and specifies the functional and assurance security measures to be offered by that TOE to meet stated requirements [CC1, Section C.1].

Version 2.0 + Errata 20180314

14-March-2018

0. Preface

0.1 Objectives of Document

This document presents the Common Criteria (CC) collaborative Protection Profile (cPP) to express the security functional requirements (SFRs) and security assurance requirements (SARs) for a network device. The Evaluation Activities that specify the actions the evaluator performs to determine if a product satisfies the SFRs captured within this cPP are described in [SD].

0.2 Scope of Document

The scope of the cPP within the development and evaluation process is described in the Common Criteria for Information Technology Security Evaluation [CC]. In particular, a cPP defines the functional and assurance requirements [CC1,

integrators, evaluators

are recognized as living documents. Please report any

Evaluation,

CC 2012.

Evaluation,

CC 2012.

[CC1] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, CCMB-2012-09-003, Version 3.1 Revision 4, September 2012.

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1, Revision 4, September 2012.

Other Documents

[SD] Evaluation Activities for Network Device cPP, Version 2.0

1.2 TOE Overview

This is a Collaborative Protection Profile (cPP) whose Target of Evaluation (TOE) is a network device. It provides a minimal set of security requirements expected by all network devices that target the mitigation of a set of defined threats. This baseline set of requirements will be built upon by future cPPs to provide an overall set of security solutions for networks up to carrier and enterprise scale. A network device in the context of this cPP is a device composed of both hardware and software that is connected to the network and has an infrastructure role within the network. The TOE may be standalone or distributed, where a distributed TOE is one that requires multiple distinct components to operate as a logical whole in order to fulfil the requirements of this cPP (a more extensive description of distributed network device TOEs is given in section 3).

A Virtual Network Device (vND) is a software implementation of network device functionality that runs inside a virtual machine. This cPP expressly excludes evaluation of vNDs unless the product is able to meet all the requirements and assumptions of a physical ND as required in this cPP

This means:

- The virtualisation layer (or hypervisor or Virtual Machine Manager (VMM)) is considered part of the ND's software stack, and thus is part of the TOE and must satisfy the relevant SFRs (e.g. by treating hypervisor Administrators as Security Administrators)². vNDs that can run on multiple VMMs must be tested on each claimed VMM unless the vendor can successfully argue equivalence.
- The physical hardware is likewise included in the TOE (as in the example included above). vNDs must be tested for each claimed hardware platform unless the vendor can successfully argue equivalence.
- There is only one vND instance for each physical hardware platform.
- There are no other guest VMs on the physical platform providing non-network device functionality.



Supporting Document Mandatory Technical Document

Evaluation Activities for Network Device
cPP


March-2018

Version 2.0 + Errata 20180314

CCDB-2017-<month TBD>-<number TBD>

1.1 Technology Area and Scope of Supporting Document

- 1 This Supporting Document defines the Evaluation Activities associated with the collaborative Protection Profile for Network Devices [NDcPP].
- 2 The Network Device technical area has a number of specialised aspects, such as those relating to the secure implementation and use of protocols, and to the particular ways in which remote management facilities need to be assessed across a range of different physical and logical interfaces for different types of infrastructure devices. This degree of specialisation, and the associations between individual SFRs in the cPP, make it important for both efficiency and effectiveness that evaluation activities are given more specific interpretations than those found in the generic CEM activities.
- 3 This Supporting Document is mandatory for evaluations of products that claim conformance to any of the following cPP(s):
 - a) collaborative Protection Profile for Network Devices [NDcPP]
 - b) collaborative Protection Profile for Stateful Traffic Filter Firewalls [FWcPP].
- 4 Although Evaluation Activities are defined mainly for the evaluators to follow, the definitions in this Supporting Document aim to provide a common understanding for developers, evaluators and users as to what aspects of the TOE are tested in an evaluation against the associated cPPs, and to what depth the testing is carried out. This common understanding in turn contributes to the goal of ensuring that evaluations against the cPP achieve comparable, transparent and repeatable results. In general the definition of Evaluation Activities will also help Developers to prepare for evaluation by identifying specific requirements for their TOE. The specific requirements in Evaluation Activities may in some cases clarify the meaning of SFRs, and may identify particular requirements for the content of Security Targets (especially the TOE Summary Specification), user guidance documentation, and possibly supplementary information (e.g. for entropy analysis or cryptographic key management architecture – see section 6).



Exemplo de aplicação do Common Criteria

Common Criteria Testing Laboratory
Accreditation Program - NVLAP





National Voluntary Laboratory Accreditation Program – NIST NVLAP

- › NVLAP provides accreditation services through various laboratory accreditation programs (LAPs), which are established on the basis of requests and demonstrated need. Each LAP includes specific test or calibration standards and related methods and protocols assembled to satisfy the unique needs for accreditation in a field of testing or calibration.
- › Accreditation requirements are established in accordance with the U.S. Code of Federal Regulations (CFR, Title 15, Part 285), *National Voluntary Laboratory Accreditation Program*, and encompass the requirements of ISO/IEC 17025.

NATIONAL VOLUNTARY LABORATORY ACCREDITATION PROGRAM (NVLAP)

Common Criteria Testing

Requirements Documents

Common Criteria Testing LAP



Welcome

This site has been established for applicants to the Common Criteria Testing accreditation program. On this site you will find important program information and links to documents required for successful participation in the program.

[Requirements Documents >](#) CONTACT

NVLAP COMMON CRITERIA TESTING PROGRAM MANAGER

Bradley Moore
bradley.moore@nist.gov
(301) 975-5740

NISTHB 150-20

NVLAP Common Criteria Testing

Dana S. Lesman
National Voluntary Laboratory Accreditation Program
Standards Coordination Office
Laboratory Programs

<http://dx.doi.org/10.6028/NIST.HB.150-20>

June 2014



U.S. Department of Commerce
Ferry Frischer, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director

Contents

Foreword	v
Acknowledgments	vi
Introduction	vii
1 General information	1
1.1 Scope	1
1.2 Organization of handbook	1
1.3 Program description	1
1.4 References	2
1.5 Terms and definitions	3
1.6 Program documentation	4
2 LAP establishment, development and implementation	4
3 Accreditation process	4
3.1 General	4
3.2 Initial accreditation (see also Annex A)	5
3.3 NVLAP renewal of accreditation	6
3.4 Suspending and revoking accreditation	8
4 Management requirements for accreditation	9
4.1 Organization	9
4.2 Management system	9
4.3 Document control	10
4.4 Review of requests, tenders and contracts	10
4.5 Subcontracting of tests and calibrations	10
4.6 Purchasing services and supplies	10
4.7 Service to the customer	10
4.8 Complaints	10
4.9 Control of nonconforming testing and/or calibration work	10
4.10 Improvement	10
4.11 Corrective action	10
4.12 Preventive action	10
4.13 Control of records	11
4.14 Internal audits	11
4.15 Management reviews	11
5 Technical requirements for accreditation	11
5.1 General	11
5.2 Personnel	12
5.3 Accommodation and environmental conditions	13
5.4 Test and calibration methods and method validation	14
5.5 Equipment	14
5.6 Measurement traceability	15
5.7 Sampling	15
5.8 Handling of test items	15
5.9 Assuring the quality of test results	15
5.10 Reporting the results	16
6 Additional requirements	16
Annex A (informative) Initial accreditation	17
Annex B (normative) Written procedures	21

1 General information

1.1 Scope

1.1.1 The purpose of this handbook is to set out procedures and technical requirements for accreditation of Common Criteria Testing Laboratories (CCTLs).

1.1.2 This handbook complements and supplements the procedures and general requirements found in NIST Handbook 150. The scope of the Common Criteria Testing (ITST CC) program is the conduct of IT security evaluations using the Common Criteria and Common Evaluation Methodology, providing a measure of confidence that such laboratories are capable of performing Common Criteria Security evaluations under the requirements of the National Information Assurance Partnership (NIAP). IT security evaluations assess conformance of a Protection Profile (PP), Security Target (ST), or IT product with a specified set of Common Criteria requirements.

1.1.3 The interpretive comments and additional requirements contained in this handbook make the general NVLAP criteria specifically applicable to the ITST CC program. Specific circumstances under which departures from the NVLAP general procedures are allowable within the scope of the program are also addressed in this handbook.

Enter Date:

Enter NVLAP Lab Code:

NIST HANDBOOK 150-20 CHECKLIST COMMON CRITERIA TESTING

Instructions to the Assessor: This checklist addresses specific accreditation requirements prescribed in NIST Handbook 150-20, NVLAP Common Criteria Testing.

- All items on this checklist shall be addressed.
- Select "OK" for each item you observed or verified as compliant at the laboratory.
- Select "X" for each item that represents a nonconformity.
- Select "C" for each item on which you are commenting for other reasons.
- Place a "N/A" beside any item that does not apply.
- Record the item number and the nonconformity explanation and/or comment on the appropriate comment sheet.

Note: The numbering of the checklist items correlates to the numbering scheme in NIST Handbook 150-20, Clauses 4 and 5 and Annex B.

4 Management requirements for accreditation

4.1 Organization

- 4.1.1 The laboratory shall establish and maintain policies and procedures for maintaining laboratory impartiality and integrity in the conduct of information technology security evaluations. When conducting evaluations under the NIAP Common Criteria scheme, the laboratory policies and procedures shall ensure that:
- a) laboratory staff members cannot both develop and evaluate the same Protection Profile, Security Target, or IT product, and
- b) laboratory staff members cannot provide consulting services for and then participate in the evaluation of the same Protection Profile, Security Target, or IT product.
- 4.1.2 The laboratory shall have physical and electronic controls augmented with an explicit policy and set of procedures for maintaining separation, both physical and electronic, between the laboratory evaluators and laboratory consultants, product developers, system integrators, and others who may have an interest in and/or may unduly influence the evaluation outcome.

- 4.1.3 The management system shall include policies and procedures to ensure the protection of proprietary information. This protection shall specify how proprietary information will be protected from persons outside the laboratory, from visitors to the laboratory, from laboratory personnel without a need to know, and from other unauthorized persons.

- 4.1.4 The laboratory shall create and maintain a cross-reference document mapping clauses 4 and 5 and annexes A and B of Handbook 150 and clauses 4 and 5 and annex B of Handbook 150-20 to the laboratory's management system documentation.

4.2 Management system

- 4.2.1 The management system requirements are designed to promote laboratory practices that ensure technical accuracy and integrity of the security evaluation and adherence to quality assurance practices appropriate to Common Criteria testing. The laboratory shall maintain a management system that fully documents the laboratory's policies, practices, and the specific steps taken to ensure the quality of the IT security evaluations.

- 4.2.2 The reference documents, standards, and publications listed in NIST Handbook 150-20, 1.4 shall be available for use by laboratory staff developing and maintaining the management system and conducting evaluations.

- 4.2.3 Each applicant and accredited laboratory shall have written and implemented procedures as described in Annex B. See Annex B located at the end of this checklist.

4.4 Review of requests, tenders and contracts

- The procedures for review of contracts shall include procedures to ensure that the laboratory has adequate staff and resources to meet its evaluation schedule and complete evaluations in a timely manner.

FIPS 140-2

ISO/IEC 19790





FIPS 140-2

- › Padrão do Governo Americano (NIST) para segurança de módulos criptográficos
- › Requisitos contemplam tanto componentes de hardware quanto de software
- › Justificativa: a proteção do módulo criptográfico é necessária para manter a integridade e a confidencialidade da informação processada pelo módulo



ISO/IEC 19790:2012 [Preview](#)

Information technology -- Security techniques -- Security requirements for cryptographic modules

This standard was last reviewed and confirmed in 2018. Therefore this version remains current.

ISO/IEC 19790:2012 the security requirements for a cryptographic module utilised within a security system protecting sensitive information in computer and telecommunication systems. This International Standard defines four security levels for cryptographic modules to provide for a wide spectrum of data sensitivity (e.g. low value administrative data, million dollar funds transfers, life protecting data, personal identity information, and sensitive information used by government) and a diversity of application environments (e.g. a guarded facility, an office, removable media, and a completely unprotected location). This International Standard specifies four security levels for each of 11 requirement areas with each security level increasing security over the preceding level.

ISO/IEC 19790:2012 specifies security requirements specifically intended to maintain the security provided by a cryptographic module and compliance with this International Standard is not sufficient to ensure that a particular module is secure or that the security provided by the module is sufficient and acceptable to the owner of the information that is being protected.

Buy this standard

Format

PDF

Paper

Language

CHF 178



FIPS 140-2

- › Quatro níveis de segurança – objetivo de abranger uma ampla gama de ambientes e aplicações
- › Os requisitos de segurança cobrem áreas relacionadas ao projeto e à implementação do módulo
 - especificação do módulo criptográfico
 - portas e interfaces
 - papéis, serviços e autenticação (RBAC)
 - modelo de estados finitos
 - segurança física
 - ambiente operacional
 - gerenciamento de chaves criptográficas
 - EMI/EMC
 - auto-testes
 - garantia de projeto
 - mitigação de ataques



Níveis de Segurança

› Level 1

- Security Level 1 provides the lowest level of security. Basic security requirements are specified for a cryptographic module (e.g., at least one Approved algorithm or Approved security function shall be used). No specific physical security mechanisms are required in a Security Level 1 cryptographic module beyond the basic requirement for production-grade components. An example of a Security Level 1 cryptographic module is a personal computer (PC) encryption board.

› Level 2

- Security Level 2 improves upon the physical security mechanisms of a Security Level 1 cryptographic module by requiring features that show **evidence of tampering**, including tamper-evident coatings or seals that must be broken to attain physical access to the plaintext cryptographic keys and critical security parameters (CSPs) within the module, or pick-resistant locks on covers or doors to protect against unauthorized physical access.



› Level 3

- In addition to the tamper-evident **physical security mechanisms** required at Security Level 2, Security Level 3 attempts to prevent the intruder from gaining access to CSPs held within the cryptographic module. Physical security mechanisms required at Security Level 3 are intended to have a high probability of detecting and responding to attempts at physical access, use or modification of the cryptographic module. The physical security mechanisms may include the use of strong enclosures and tamper-detection/response circuitry that zeroes all plaintext CSPs when the removable covers/doors of the cryptographic module are opened.

› Level 4

- Security Level 4 provides the highest level of security. At this security level, the physical security mechanisms provide a **complete envelope of protection** around the cryptographic module with the intent of **detecting and responding to all unauthorized attempts at physical access**. Penetration of the cryptographic module enclosure from any direction has a very high probability of being detected, resulting in the immediate deletion of all plaintext CSPs.



Resumo

- › Nível 1
 - funções básicas de segurança
 - pelo menos um algoritmo "aprovado"
- › Nível 2
 - detecção de violação
- › Nível 3
 - segurança física
- › Nível 4
 - detecção e resposta a ataques físicos

FIPS PUB 140-2

[CHANGE NOTICES \(12-03-2002\)](#)

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION
(Supersedes FIPS PUB 140-1, 1994 January 11)

SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES

CATEGORY: COMPUTER SECURITY

SUBCATEGORY: CRYPTOGRAPHY

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

Issued May 25, 2001



U.S. Department of Commerce
Donald L. Evans, Secretary

Technology Administration
Phillip J. Broad, Under Secretary for Technology

National Institute of Standards and Technology
Arden L. Bement, Jr., Director

TABLE OF CONTENTS

1. OVERVIEW	1
1.1 Security Level 1	1
1.2 Security Level 2	2
1.3 Security Level 3	2
1.4 Security Level 4	3
2. GLOSSARY OF TERMS AND ACRONYMS	4
2.1 Glossary of Terms	4
2.2 Acronyms	8
3. FUNCTIONAL SECURITY OBJECTIVES	11
4. SECURITY REQUIREMENTS	12
4.1 Cryptographic Module Specification	13
4.2 Cryptographic Module Ports and Interfaces	14
4.3 Roles, Services, and Authentication	15
4.3.1 Roles	16
4.3.2 Services	16
4.3.3 Operator Authentication	17
4.4 Finite State Model	19
4.5 Physical Security	20
4.5.1 General Physical Security Requirements	21
4.5.2 Single-Chip Cryptographic Modules	23
4.5.3 Multiple-Chip Embedded Cryptographic Modules	24
4.5.4 Multiple-Chip Standalone Cryptographic Modules	25
4.5.5 Environmental Failure Protection/Testing	26
4.6 Operational Environment	27
4.6.1 Operating System Requirements	28
4.7 Cryptographic Key Management	30
4.7.1 Random Number Generators (RNGs)	30
4.7.2 Key Generation	31
4.7.3 Key Establishment	31
4.7.4 Key Entry and Output	31
4.7.5 Key Storage	33
4.7.6 Key Zeroization	33
4.8 Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)	33
4.9 Self-Tests	33
4.9.1 Power-Up Tests	34
4.9.2 Conditional Tests	35
4.10 Design Assurance	36
4.10.1 Configuration Management	36
4.10.2 Delivery and Operation	37
4.10.3 Development	37
4.10.4 Guidance Documents	38
4.11 Mitigation of Other Attacks	39

	<i>Security Level 1</i>	<i>Security Level 2</i>	<i>Security Level 3</i>	<i>Security Level 4</i>
Cryptographic Module Specification	Specification of cryptographic module, cryptographic boundary, Approved algorithms, and Approved modes of operation. Description of cryptographic module, including all hardware, software, and firmware components. Statement of module security policy.			
Cryptographic Module Ports and Interfaces	Required and optional interfaces. Specification of all interfaces and of all input and output data paths.		Data ports for unprotected critical security parameters logically or physically separated from other data ports.	
Roles, Services, and Authentication	Logical separation of required and optional roles and services.	Role-based or identity-based operator authentication.	Identity-based operator authentication.	
Finite State Model	Specification of finite state model. Required states and optional states. State transition diagram and specification of state transitions.			
Physical Security	Production grade equipment.	Locks or tamper evidence.	Tamper detection and response for covers and doors.	Tamper detection and response envelope. EFP or EFT.
Operational Environment	Single operator. Executable code. Approved integrity technique.	Referenced PPs evaluated at EAL2 with specified discretionary access control mechanisms and auditing.	Referenced PPs plus trusted path evaluated at EAL3 plus security policy modeling.	Referenced PPs plus trusted path evaluated at EAL4.
Cryptographic Key Management	Key management mechanisms: random number and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroization.			
	Secret and private keys established using manual methods may be entered or output in plaintext form.		Secret and private keys established using manual methods shall be entered or output encrypted or with split knowledge procedures.	
EMI/EMC	47 CFR FCC Part 15. Subpart B, Class A (Business use). Applicable FCC requirements (for radio).		47 CFR FCC Part 15. Subpart B, Class B (Home use).	
Self-Tests	Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical functions tests. Conditional tests.			
Design Assurance	Configuration management (CM). Secure installation and generation. Design and policy correspondence. Guidance documents.	CM system. Secure distribution. Functional specification.	High-level language implementation.	Formal model. Detailed explanations (informal proofs). Preconditions and postconditions.
Mitigation of Other Attacks	Specification of mitigation of attacks for which no testable requirements are currently available.			

Cryptographic Module Validation Program



Project Overview

What Is The Purpose Of The CMVP?

On July 17, 1995, NIST established the Cryptographic Module Validation Program (CMVP) that validates cryptographic modules to Federal Information Processing Standards (FIPS)140-1, *Security Requirements for Cryptographic Modules*, and other FIPS cryptography based standards. [FIPS 140-2](#), *Security Requirements for Cryptographic Modules*, was released on May 25, 2001 and supersedes FIPS 140-1. The CMVP is a joint effort between NIST and the Canadian Centre for Cyber Security (CCCS), a branch of the Communications Security Establishment (CSE).

Modules validated as conforming to FIPS 140-2 are accepted by the Federal Agencies of both countries for the protection of sensitive information.

Vendors of cryptographic modules use independent, accredited [Cryptographic and Security Testing \(CST\) laboratories](#) to test their modules. The CST laboratories use the [Derived Test Requirements \(DTR\)](#), [Implementation Guidance \(IG\)](#) and applicable CMVP programmatic guidance to test cryptographic modules against the applicable standards. NIST's Computer Security Division (CSD) and CCCS jointly serve as the Validation Authorities for the program, validating the test results and issuing certificates.

What Is The Applicability Of CMVP To The US Government?

FIPS 140-1 became a mandatory standard for the protection of sensitive data when the Secretary of Commerce signed the standard on January 11, 1994. [FIPS 140-2](#) supersedes FIPS 140-1 and the standard was signed on May 25, 2001.

The applicability statement from FIPS 140-2 (page iv):

7. Applicability. This standard is applicable to all Federal agencies that use cryptographic-based security systems to protect sensitive information in computer and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106. This standard shall be used in designing and implementing cryptographic modules that Federal departments and agencies operate or are operated for them under contract. Cryptographic modules that have been approved for classified use may be used in lieu of modules that have been validated against this standard. The adoption and use of this standard is available to private and commercial organizations.

NATIONAL VOLUNTARY LABORATORY ACCREDITATION PROGRAM (NVLAP)

[About NVLAP](#) [Directory of Accredited Laboratories](#)[Search Test Methods or Calibration Parameters](#)[Accreditation Programs](#)[Assessor Resources](#) [Publications and Forms](#)[Apply for NVLAP Accreditation](#) [Referencing NVLAP Accreditation and Use of ILAC Combined Mark](#)

Cryptographic and Security Testing LAP



The Cryptographic and Security Testing (CST) Laboratory Accreditation Program (LAP), initially named Cryptographic Module Testing (CMT), was established by NVLAP to accredit laboratories that perform cryptographic modules validation conformance testing under the Cryptographic Module Validation Program (CMVP). In response to other mandates and requests, additional testing has been added to the program to include algorithm testing for the Cryptographic Algorithm Validation Program (CAVP), testing to improving the identification and authentication of Federal employees and contractors for access to Federal facilities and information systems for the NIST Personal Identification Verification Program (NPIVP), test methods for the GSA FIPS 201 Evaluation Program which build upon NPIVP test methods as the GSA Precursor (GSAP), testing to validate the implementation of the Security Content Automation Protocol (SCAP) standards within security software modules, and conformance testing to methods supportive of the Department of Homeland Security's Identity and Privilege Credential Management; e.g. Transportation Worker Identification Credential (TWIC).

Proficiency Testing Requirements

At the present time, there is no ongoing established program for proficiency testing of laboratories accredited for cryptographic and security testing beyond the initial artifact testing that is completed by an initial applicant to the program.

Sistemas de Gestão de Segurança da Informação

Conceitos básicos e o arcabouço da
ISO27k

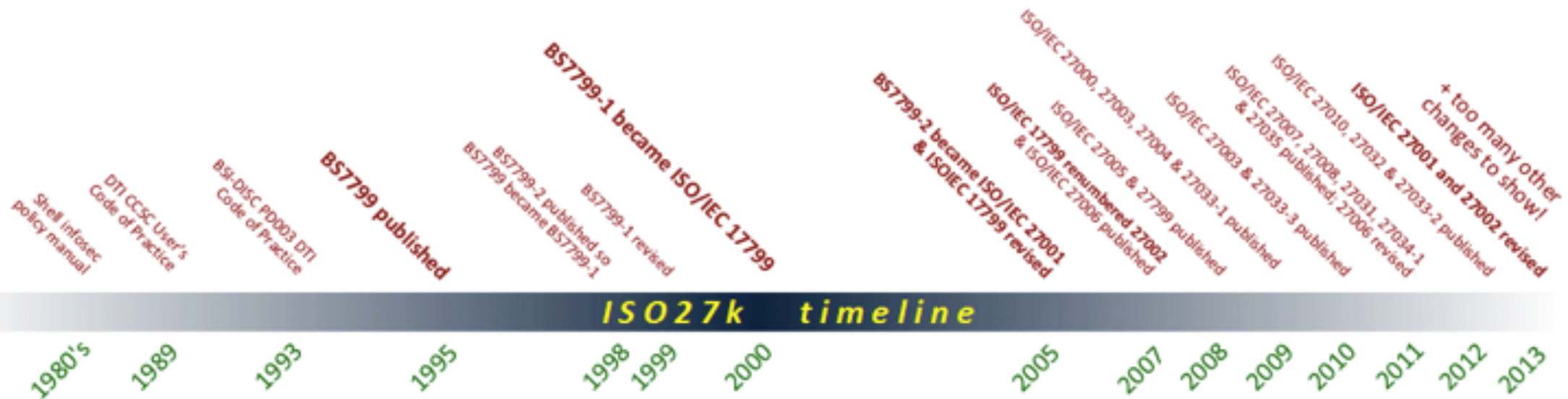


ISO 27k

Série de padrões de segurança da
informação



Histórico da série ISO27k



The ISO27k Standards - List contributed and maintained by [Gary Hinson](#)

#	Standard	Published	Title	Notes
1	ISO/IEC 27000	2018	Information security management systems — Overview and vocabulary	Overview/introduction to the ISO27k standards as a whole plus a glossary of terms; FREE!
2	ISO/IEC 27001	2013	Information security management systems — Requirements	Formally specifies an ISMS against which thousands of organizations have been certified compliant
3	ISO/IEC 27002	2013	Code of practice for information security controls	A reasonably comprehensive suite of information security control objectives and generally-accepted good practice security controls
4	ISO/IEC 27003	2017	Information security management system implementation guidance	Sound advice on implementing ISO27k, expanding section-by-section on the main body of ISO/IEC 27001
5	ISO/IEC 27004	2016	Information security management — Measurement	Much improved second version, with useful advice on security metrics
6	ISO/IEC 27005	2011	Information security risk management	Discusses information risk management principles in general without specifying particular methods. Out of date - needs revision

#	Standard	Published	Title	Notes
7	ISO/IEC 27006	2015	Requirements for bodies providing audit and certification of information security management systems	Formal guidance for the certification bodies, with several grammatical errors - needs revision
8	ISO/IEC 27007	2017	Guidelines for information security management systems auditing	Auditing the management system elements of the ISMS
9	ISO/IEC TR 27008	2011	Guidelines for auditors on information security controls	Auditing the information security elements of the ISMS
10	ISO/IEC 27009	2016	Sector-specific application of ISO/IEC 27001 - requirements	Guidance for those developing new ISO27k standards (i.e. ISO/IEC JTC1/SC27 - an internal committee standing document really)
11	ISO/IEC 27010	2015	Information security management for inter-sector and inter-organisational communications	Sharing information on information security between industry sectors and/or nations, particularly those affecting "critical infrastructure"
12	ISO/IEC 27011	2016	Information security management guidelines for telecommunications organizations based on ISO/IEC 27002	Information security controls for the telecoms industry; also called "ITU-T Recommendation x.1051"
13	ISO/IEC 27013	2015	Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1	Combining ISO27k/ISMS with IT Service Management/ITIL
14	ISO/IEC 27014	2013	Governance of information security	Governance in the context of information security; will also be called "ITU-T Recommendation X.1054"
15	ISO/IEC TR 27015	2012	Information security management guidelines for financial services	Applying ISO27k in the finance industry

#	Standard	Published	Title	Notes
16	ISO/IEC TR 27016	2014	Information security management - Organizational economics	Economic theory applied to information security
17	ISO/IEC 27017	2015	Code of practice for information security controls for cloud computing services based on ISO/IEC 27002	Information security controls for cloud computing
18	ISO/IEC 27018	2014	Code of practice for controls to protect personally identifiable information processed in public cloud computing services	Privacy controls for cloud computing
19	ISO/IEC TR 27019	2017	Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy industry	Information security for ICS/SCADA/embedded systems (not just used in the energy industry!), excluding the nuclear industry
20	ISO/IEC 27021	2017	Competence requirements for information security management professionals	Guidance on the skills and knowledge necessary to work in this field
21	ISO/IEC 27023	2015	Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002	Related advice for those updating their ISMSs from the 2005 to 2013 versions
22	ISO/IEC 27030	DRAFT	Guidelines for security and privacy in Internet of Things (IoT)	A standard about the information risk, security and privacy aspects of IoT
23	ISO/IEC 27031	2011	Guidelines for information and communications technology readiness for business continuity	Continuity (i.e. resilience, incident management and disaster recovery) for ICT, supporting general business continuity

#	Standard	Published	Title	Notes
24	ISO/IEC 27032	2012	Guidelines for cybersecurity	Ignore the vague title: this standard actually concerns Internet security
25	ISO/IEC 27033	-1 2015	Network security overview and concepts	Various aspects of network security, updating and replacing ISO/IEC 18028
26		-2 2012	Guidelines for the design and implementation of network security	
27		-3 2010	Reference networking scenarios - threats, design techniques and control issues	
28		-4 2014	Securing communications between networks using security gateways	
29		-5 2013	Securing communications across networks using Virtual Private Networks (VPNs)	
30		-6 2016	Securing wireless IP network access	
31	ISO/IEC 27034	-1 2011	Application security — Overview and concepts	Multi-part application security standard
32		-2 2015	Organization normative framework	
33		-3 DRAFT	Application security management process	
34		-4 DRAFT	Application security validation	Promotes the concept of a reusable library of information security control functions, formally specified, designed and tested
35		-5 2017	Protocols and application security control data structure	
36		-6 2016	Case studies	
37		-7 DRAFT	Application security assurance prediction framework	

#	Standard	Published	Title	Notes
38	ISO/IEC 27035	-1 2016	Information security incident management — Principles of incident management	Replaced ISO TR 18044 Actually concerns incidents affecting IT systems and networks, specifically
39		-2 2016	— Guidelines to plan and prepare for incident response	
40		-3 DRAFT	— Guidelines for ICT incident response operations??	Part 3 drafting project was cancelled and restarted
41	ISO/IEC 27036	-1 2014	Information security for supplier relationships – Overview and concepts (FREE!)	Information security aspects of ICT outsourcing and services
42		-2 2014	— Common requirements	
43		-3 2013	— Guidelines for ICT supply chain security	
44		-4 2016	— Guidelines for security of cloud services	
45	ISO/IEC 27037	2012	Guidelines for identification, collection, acquisition, and preservation of digital evidence	One of several IT forensics standards
46	ISO/IEC 27038	2014	Specification for digital redaction	Redaction of digital documents
47	ISO/IEC 27039	2015	Selection, deployment and operations of intrusion detection and prevention systems (IDPS)	IDS/IPS

#	Standard	Published	Title	Notes
48	ISO/IEC 27040	2015	Storage security	IT security for stored data
49	ISO/IEC 27041	2015	Guidelines on assuring suitability and adequacy of incident investigative methods	Assurance of the integrity of forensic evidence is absolutely vital
50	ISO/IEC 27042	2015	Guidelines for the analysis and interpretation of digital evidence	IT forensics analytical methods
51	ISO/IEC 27043	2015	Incident investigation principles and processes	The basic principles of eForensics
52	ISO/IEC 27050	-1 2016	Electronic discovery – overview and concepts	More eForensics advice
53		-2 DRAFT	Guidance for governance and management of electronic discovery	Advice on treating the risks relating to eForensics
54		-3 2017	Code of practice for electronic discovery	A how-to-do-it guide to eDiscovery
55		-4 DRAFT	ICT readiness for electronic discovery	Guidance on eDiscovery technology (tools, systems and processes)
56	ISO/IEC 27070	DRAFT	Security requirements for establishing virtualized roots of trust	Concerns trusted computing in the cloud
57	ISO/IEC 27102	DRAFT	Information security management guidelines for cyber insurance	Advice on obtaining insurance to reduce the costs of cyber incidents
58	ISO/IEC TR 27103	2018	Cybersecurity and ISO and IEC standards	Explains how ISO27k and other ISO and IEC standards relate to 'cybersecurity' (without defining the term!)

#	Standard	Published	Title	Notes
59	ISO/IEC 27550	DRAFT	Privacy engineering	How to address privacy throughout the lifecycle of IT systems
60	ISO/IEC 27551	DRAFT	Requirements for attribute-based unlinkable entity authentication	Seems more like an authentication standard than ISO27k ... scope creep?
61	ISO/IEC 27552	DRAFT	Extension to ISO/IEC 27001 and to ISO/IEC 27002 for privacy management — Requirements and guidelines	Explains extensions to an ISO27k ISMS for privacy management
62	ISO 27799	2016	Health informatics — Information security management in health using ISO/IEC 27002	Infosec management advice for the health industry

PRINCIPAL

COLABORAÇÕES

HISTÓRICO

Código > ISO/IEC 27000:2018

Status : Em Vigor

Data de Publicação : 07/02/2018

Título Idioma Principal : Information technology – Security techniques – Information security management systems – Overview and vocabulary

Título Idioma Secundário : Technologies de l'information – Techniques de sécurité– Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire

Comitê : ISO/IEC/JTC 1 Information technology

Nº de Páginas : 27

Organismo : ISO - International Organization for Standardization

Idioma : Inglês

Preço (R\$) : 552,00

Resumo :



Normas Recomendáveis para a aplicação da
ISO/IEC 27000:2018



ICS/CIN :

01.040.35 Tecnologia da informação (Vocabulários)



Palavras-Chave :

**INTERNATIONAL
STANDARD**

**ISO/IEC
27000**

Fifth edition
2018-02

**Information technology — Security
techniques — Information security
management systems — Overview and
vocabulary**

*Technologies de l'information — Techniques de sécurité — Systèmes
de management de la sécurité de l'information — Vue d'ensemble et
vocabulaire*

Information technology — Security techniques — Information security management systems — Overview and vocabulary

1 Scope

This document provides the overview of information security management systems (ISMS). It also provides terms and definitions commonly used in the ISMS family of standards. This document is applicable to all types and sizes of organization (e.g. commercial enterprises, government agencies, not-for-profit organizations).

The terms and definitions provided in this document

- cover commonly used terms and definitions in the ISMS family of standards;
- do not cover all terms and definitions applied within the ISMS family of standards; and
- do not limit the ISMS family of standards in defining new terms for use.



Definições importantes

**3.2
attack**
attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset

**3.14
control**
measure that is modifying risk (3.61)

**3.21
event**
occurrence or change of a particular set of circumstances

Note 1 to entry: An event can be one or more occurrences, and can have several causes.

Note 2 to entry: An event can consist of something not happening.

Note 3 to entry: An event can sometimes be referred to as an "incident" or "accident".

[SOURCE: ISO Guide 73:2009, 3.5.1.3, modified — Note 4 to entry has been deleted.]

**3.28
information security**
preservation of confidentiality (3.10), integrity (3.36) and availability (3.2) of information

Note 1 to entry: In addition, other properties, such as authenticity (3.6), accountability, non-repudiation (3.48), and reliability (3.55) can also be involved.

**3.74
threat**
potential cause of an unwanted incident, which can result in harm to a system or organization (3.50)

**3.61
risk**
effect of uncertainty on objectives (3.49)

Note 1 to entry: An effect is a deviation from the expected — positive or negative.

Note 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

Note 3 to entry: Risk is often characterized by reference to potential "events" (as defined in ISO Guide 73:2009, 3.5.1.3) and "consequences" (as defined in ISO Guide 73:2009, 3.6.1.3), or a combination of these.

Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated "likelihood" (as defined in ISO Guide 73:2009, 3.6.1.1) of occurrence.

Note 5 to entry: In the context of information security management systems, information security risks can be expressed as effect of uncertainty on information security objectives.

Note 6 to entry: Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization.

**3.77
vulnerability**
weakness of an asset or control (3.14) that can be exploited by one or more threats (3.74)

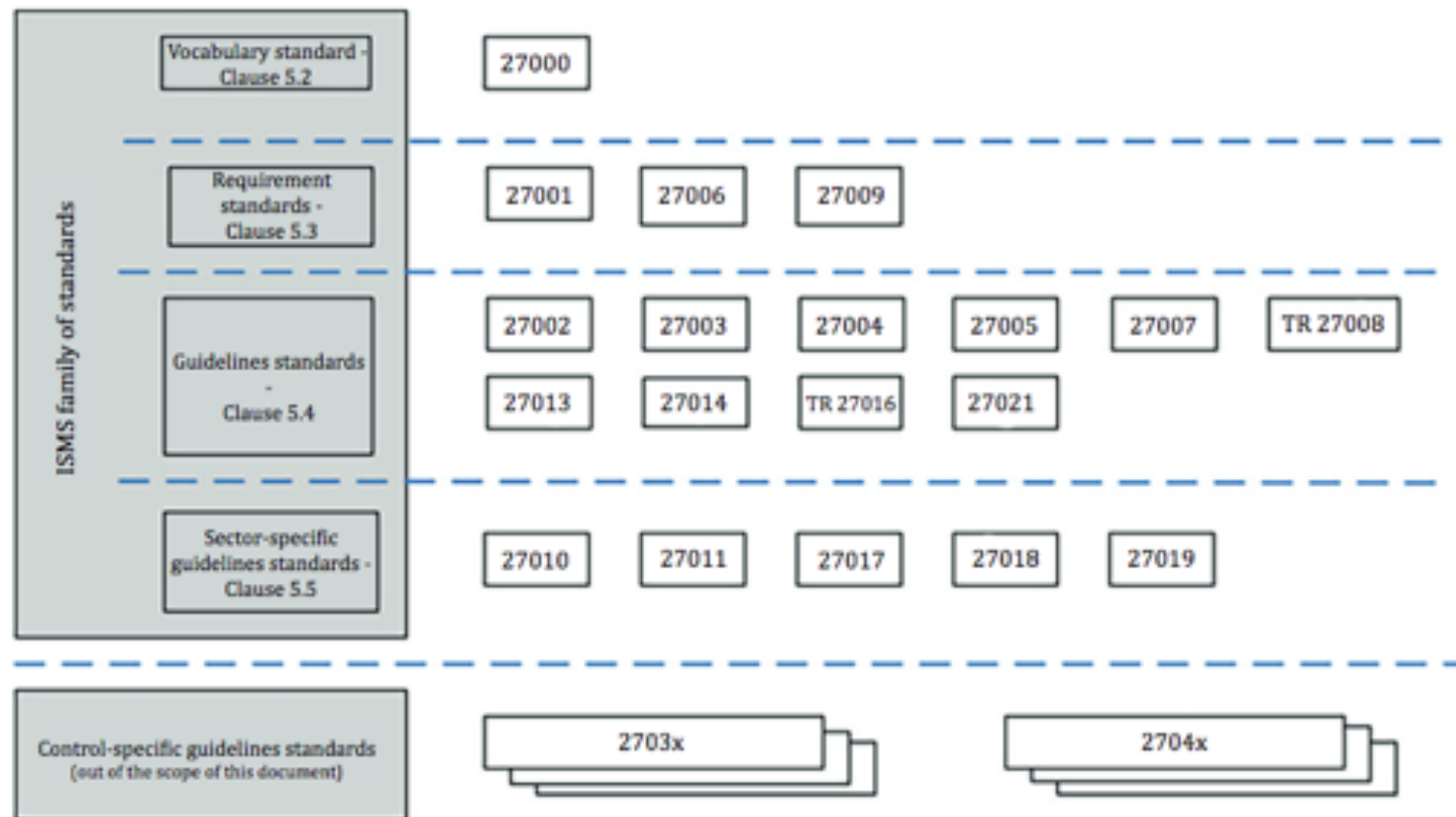
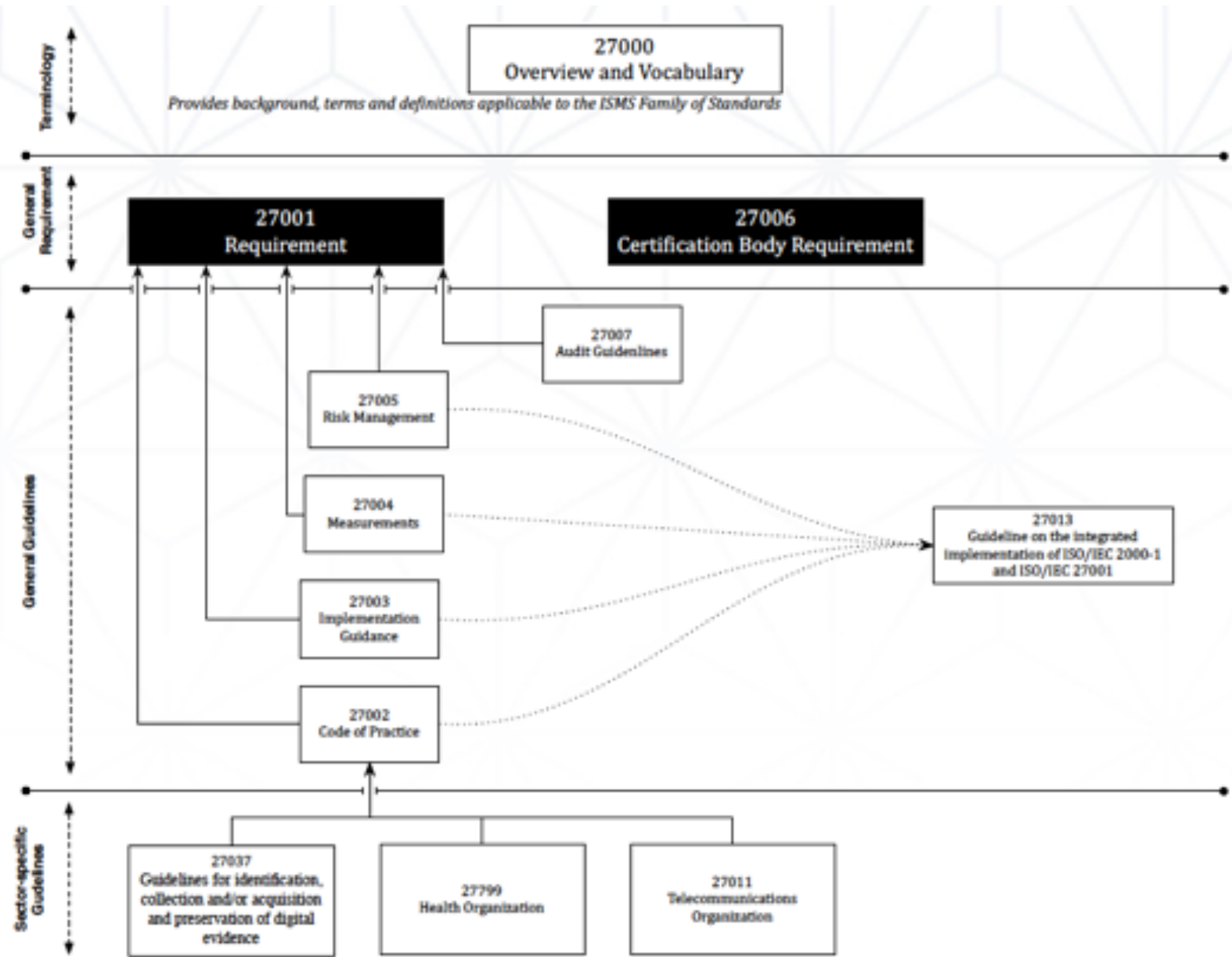


Figure 1 — ISMS family of standards relationships





Uso de cada padrão...

- › ·ISO/IEC 27001 — Information technology - Security Techniques - Information security management systems
- › ·ISO/IEC 27002 — Code of practice for information security management
- › ·ISO/IEC27003 — Information security management system implementation guidance
- › ·ISO/IEC 27004 — Information security management — Measurement
- › ·ISO/IEC 27005 — Information security risk management
- › ·ISO/IEC 27006 — Requirements for bodies providing audit and certification of information security management systems
- › ·ISO/IEC 27007 — Guidelines for information security management systems auditing
- › ·ISO/IEC 27035 — Information security incident management
- › ·ISO/IEC 27037 — Guidelines for identification, collection, acquisition and preservation of digital evidence

OBRIGATÓRIO

IMPORTANTE

REFERÊNCIA

SUPOORTE

Código > ABNT NBR ISO/IEC 27005:2011

Status : Em Vigor

Data de Publicação : 17/11/2011

Válida a partir de : 17/12/2011

Título Idioma Principal : Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação

Título Idioma Secundário : Information technology - Security techniques - Information security risk management

ISBN : 978-85-07-03066-9

Origem : ABNT NBR ISO IEC 27005:2011

Comitê : ABNT/CB-021 Computadores e Processamento de Dados

Nº de Páginas : 87

Organismo : ABNT - Associação Brasileira de Normas Técnicas

Idioma : Português

Preço (R\$) : 250,95

Resumo : Esta Norma fornece diretrizes para o processo de gestão de riscos de segurança da informação.

**NORMA
BRASILEIRA**

**ABNT NBR
ISO/IEC
27005**

Segunda edição
17.11.2011

Válida a partir de
17.12.2011

**Tecnologia da informação — Técnicas de
segurança — Gestão de riscos de segurança da
informação**

*Information technology — Security techniques — Information security risk
management*

6 Visão geral do processo de gestão de riscos de segurança da informação

Uma visão de alto nível do processo de gestão de riscos é especificada na ABNT NBR ISO 31000:2009 e apresentada na Figura 1.



Figura 1 – O processo de gestão de riscos

3.9

risco

efeito da incerteza nos objetivos

[ABNT ISO GUIA 73:2009]



ABNT
ISO
GUIA 73

Primeira edição 2009

Gestão de riscos – Vocabulário

Risk management – Vocabulary



Vulnerabilidade versus Ameaça (27005)

A presença de uma vulnerabilidade não causa prejuízo por si só, pois precisa haver uma ameaça presente para explorá-la. Uma vulnerabilidade que não tem uma ameaça correspondente pode não requerer a implementação de um controle no presente momento, mas convém que ela seja reconhecida como tal e monitorada, no caso de haver mudanças. Convém notar que um controle implementado incorretamente, com mau funcionamento ou sendo usado de forma errada pode, por si só, representar uma vulnerabilidade. Um controle pode ser eficaz ou não, dependendo do ambiente no qual ele opera. Inversamente, uma ameaça que não tenha uma vulnerabilidade correspondente pode não resultar em um risco.

Código > ISO/IEC 27006:2015

Status : Em Vigor

Data de Publicação : 30/09/2015

Título Idioma Principal : Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems

Título Idioma Secundário : Technologies de l'information -- Techniques de sécurité-- Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information

Comitê : ISO/IEC/JTC 1 Information technology

Nº de Páginas : 35

Organismo : ISO - International Organization for Standardization

Idioma : Inglês

Preço (R\$) : 552,00

Resumo : ISO/IEC 27006:2015 specifies requirements and provides guidance for bodies providing audit and certification of an information security management system (ISMS), in addition to the requirements contained within ISO/IEC 17021-1 and ISO/IEC 27001. It is primarily intended to support the accreditation of certification bodies providing ISMS certification. The requirements contained in this International Standard need to be demonstrated in terms of competence and reliability by any body providing ISMS certification, and the guidance contained in this International Standard provides additional interpretation of these requirements for any body providing ISMS certification. NOTE This International Standard can be used as a criteria document for accreditation, peer assessment or other audit processes.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 17021-1:2015, *Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements*

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are

indisp
refere

ISO/IE
of mar

ISO/IE
system

ISO/IE
system

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 17021-1, ISO/IEC 27000 and the following apply.

3.1

certification documents

documents indicating that a client's ISMS conforms to specified ISMS standards and any supplementary documentation required under the system

4 Principles

The principles from ISO/IEC 17021-1, 4 apply.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are

indisp
refere

ISO/IE
of mar

ISO/IE
system

ISO/IE
system

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 17021-1, ISO/IEC 27000 and the following apply.

3.1
certific
docume
docume

5 General requirements

5.1 Legal and contractual matters

The requirements of ISO/IEC 17021-1, 5.1 apply.

4 Pr

The pri

5.2 Management of impartiality

The requirements of ISO/IEC 17021-1, 5.2 apply. In addition, the following requirements and guidance apply.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are

indisp
refere

ISO/IE
of mar

ISO/IE
system

ISO/IE
system

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 17021-1, ISO/IEC 27000 and the following apply.

3.1
certific
docume
docume

5 General requirements

5.1 Legal and contractual matters

The re

6 Structural requirements

The requirements of ISO/IEC 17021-1, 6 apply.

5.2

The r
guida

7 Resource requirements

7.1 Competence of personnel

The requirements of ISO/IEC 17021-1, 7.1 apply. In addition, the following requirements and guidance apply.

4 Pr

The pri

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are

indisp
refere

ISO/IE
of mar

ISO/IE
system

ISO/IE
system

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 17021-1, ISO/IEC 27000 and the following apply.

3.1
certific
docume
docume

5 General requirements

5.1 Legal and contractual matters

The re

6 Structural requirements

The requirements of ISO/IEC 17021-1, 6 apply.

5.2

The r
guida

7 Resource requirements

7.1

The r
guida

7.1.1 IS 7.1.1 General considerations

7.1.1.1 Generic competence requirements

The certification body shall ensure that it has knowledge of the technological, legal and regulatory developments relevant to the ISMS of the client which it assesses.

The certification body shall define the competence requirements for each certification function as referenced in Table A.1 of ISO/IEC 17021-1. The certification body shall take into account all the requirements specified in ISO/IEC 17021-1 and [7.1.2](#) and [7.2.1](#) of this International Standard that are relevant for the ISMS technical areas as determined by the certification body.

NOTE [Annex A](#) provides a summary of the competence requirements for personnel involved in specific certification functions.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are

indisp
refere

ISO/IE
of mar

ISO/IE
system

ISO/IE
system

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 17021-1, ISO/IEC 27000 and the following apply.

3.1
certific
docume
docume

5 General requirements

5.1 Legal and contractual matters

The re

6 Structural requirements

The requirements of ISO/IEC 17021-1, 6 apply.

4 Pr

The pri

5.2

The r
guida

7 Resource requirements

7.1

The r
guida

7.1.1 IS 7.1.1 General considerations

7.1.1.1 Generic competence requirements

The certification body shall ensure that it has knowledge of the technological, legal and regulatory developments relevant to the ISMS of the client which it assesses.

The certifi
referenc
requireme
relevant fo

NOTE
certificatio

7.1.2.1.3 Information security management system standards and normative documents

Auditors involved in ISMS auditing shall have knowledge of:

a) all requirements contained in ISO/IEC 27001.

Collectively, all members of the audit team shall have knowledge of:

b) all controls contained in ISO/IEC 27002 (if determined as necessary also from sector specific standards) and their implementation, categorized as:

Código de prática

Conhecer a norma ABNT NBR ISO/IEC 27002:2013 e
selecionar, relacionar e combinar
seus controles.

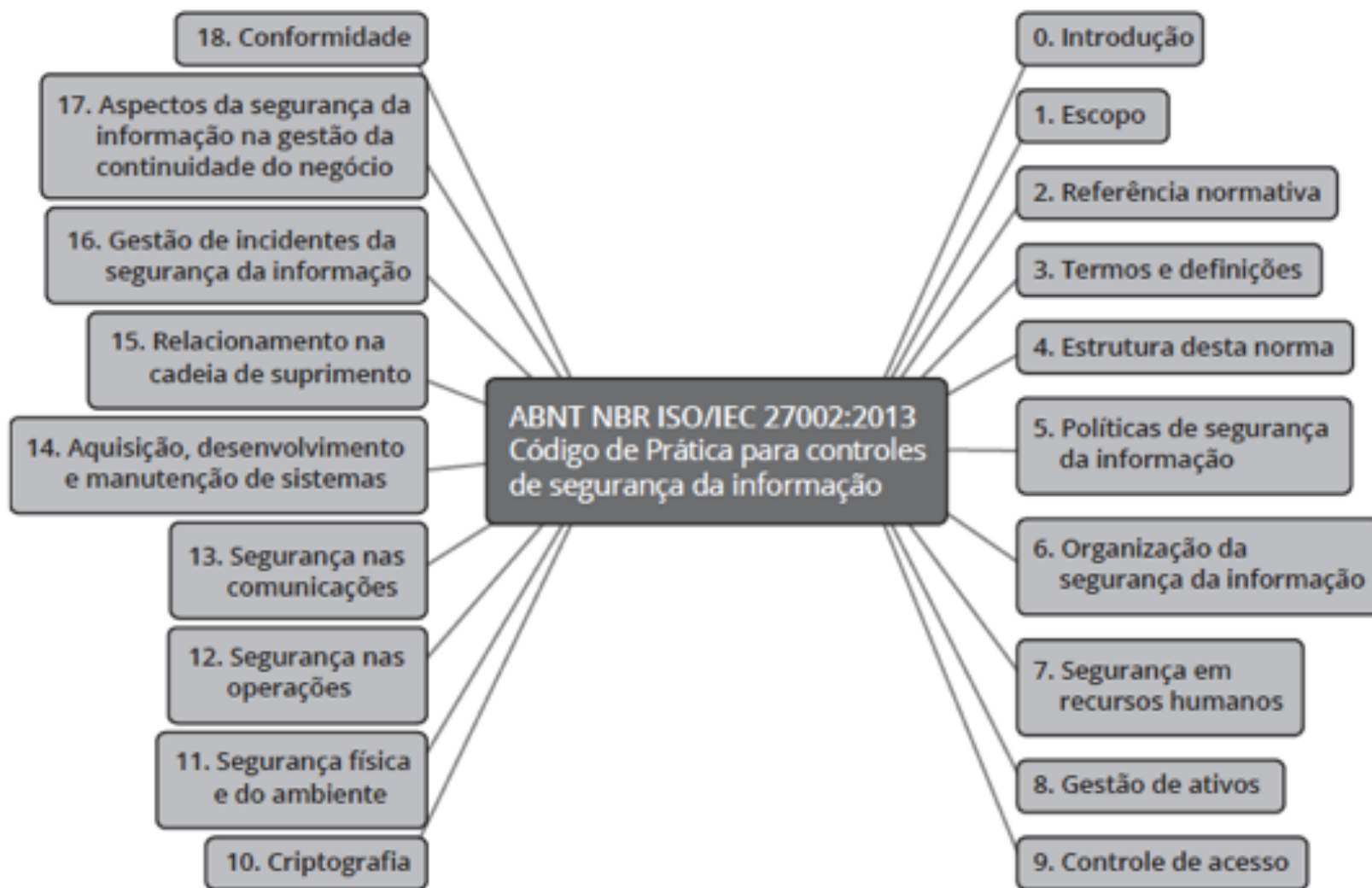
Estrutura e seções da norma ABNT NBR ISO/IEC 27002:2013 e
seus objetivos.

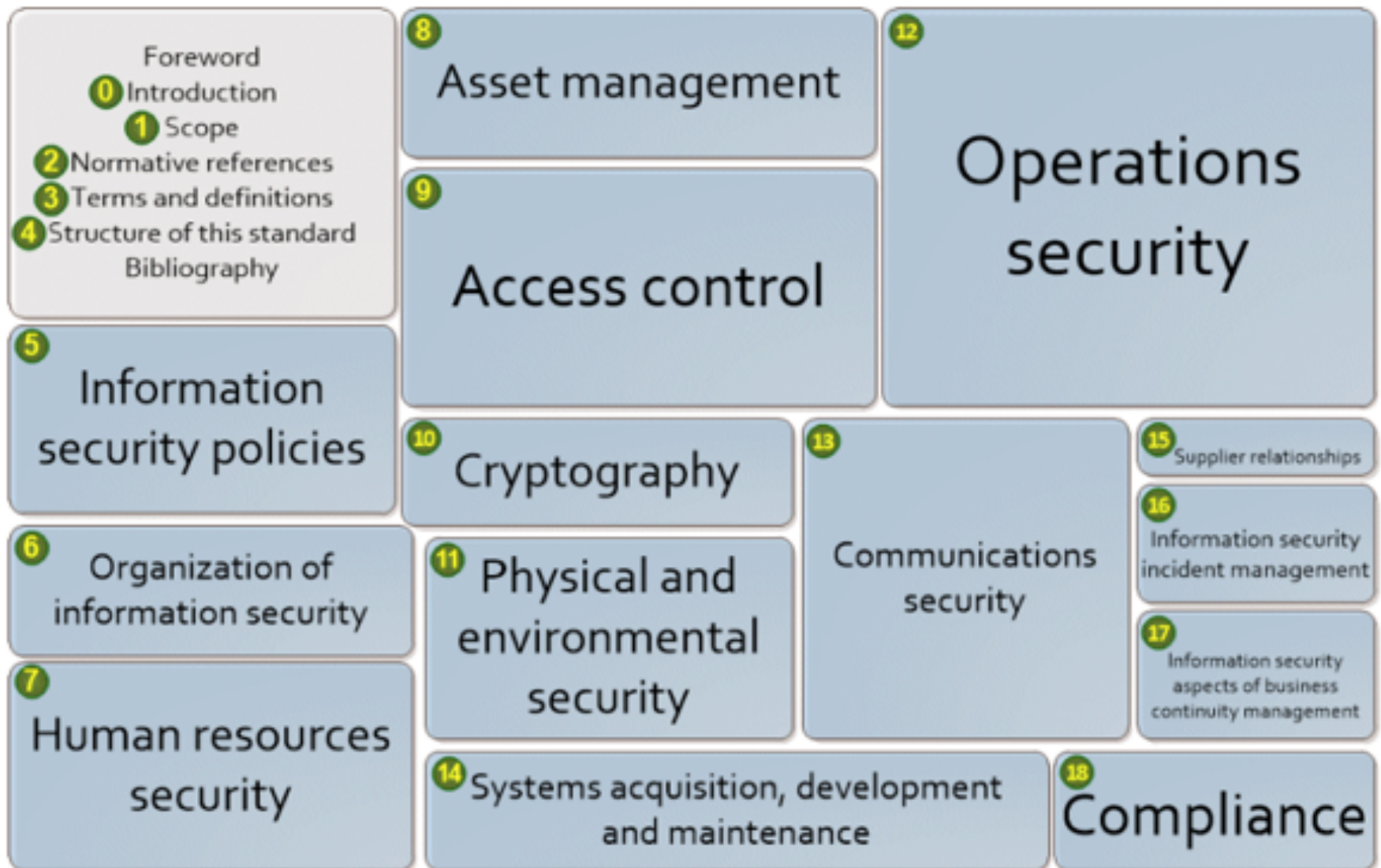




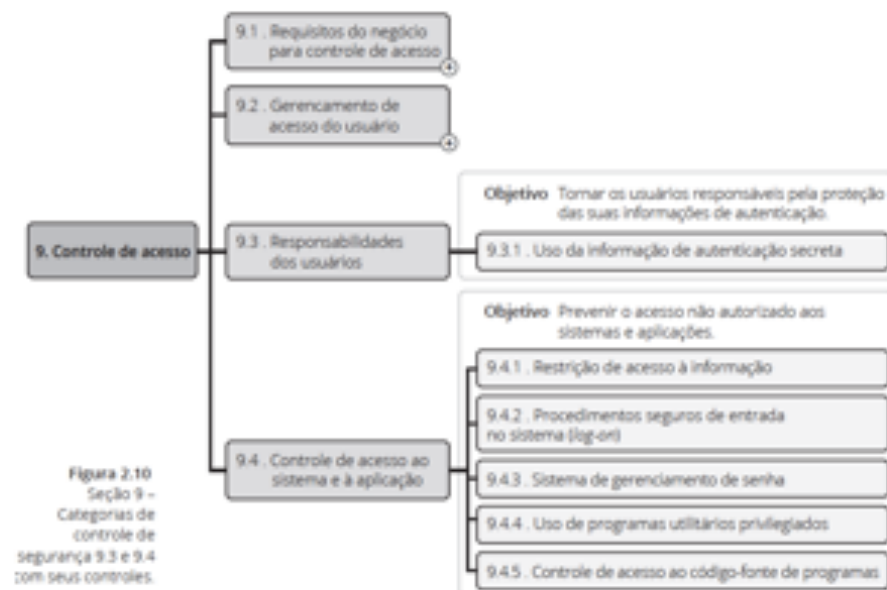
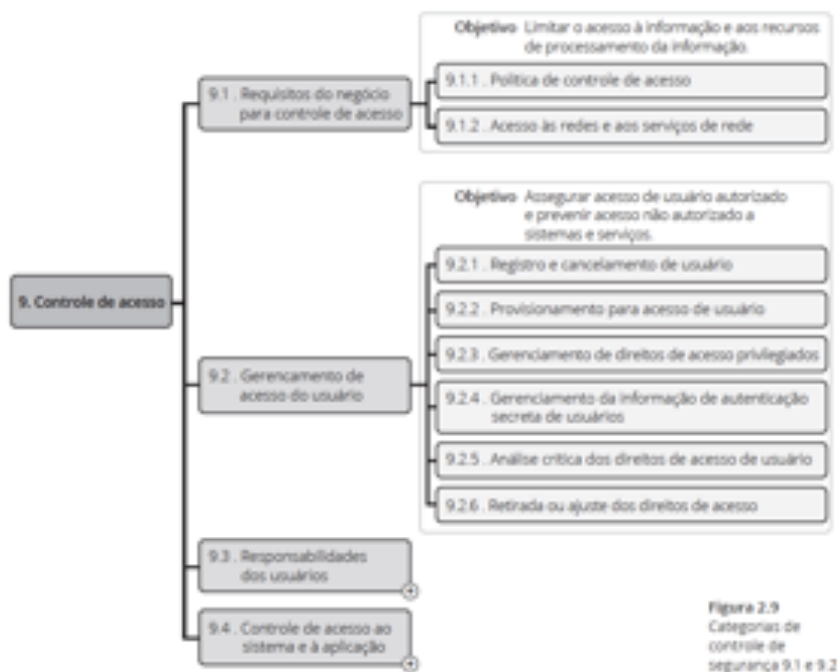
Estrutura da 27002

- › Apresentação da norma ABNT NBR ISO/IEC 27002:2013:
- › Possui 14 seções.
- › Possui 35 objetivos de controle.
- › A versão atual possui 114 controles.





Exemplo: Seção 9 – Controle de acesso



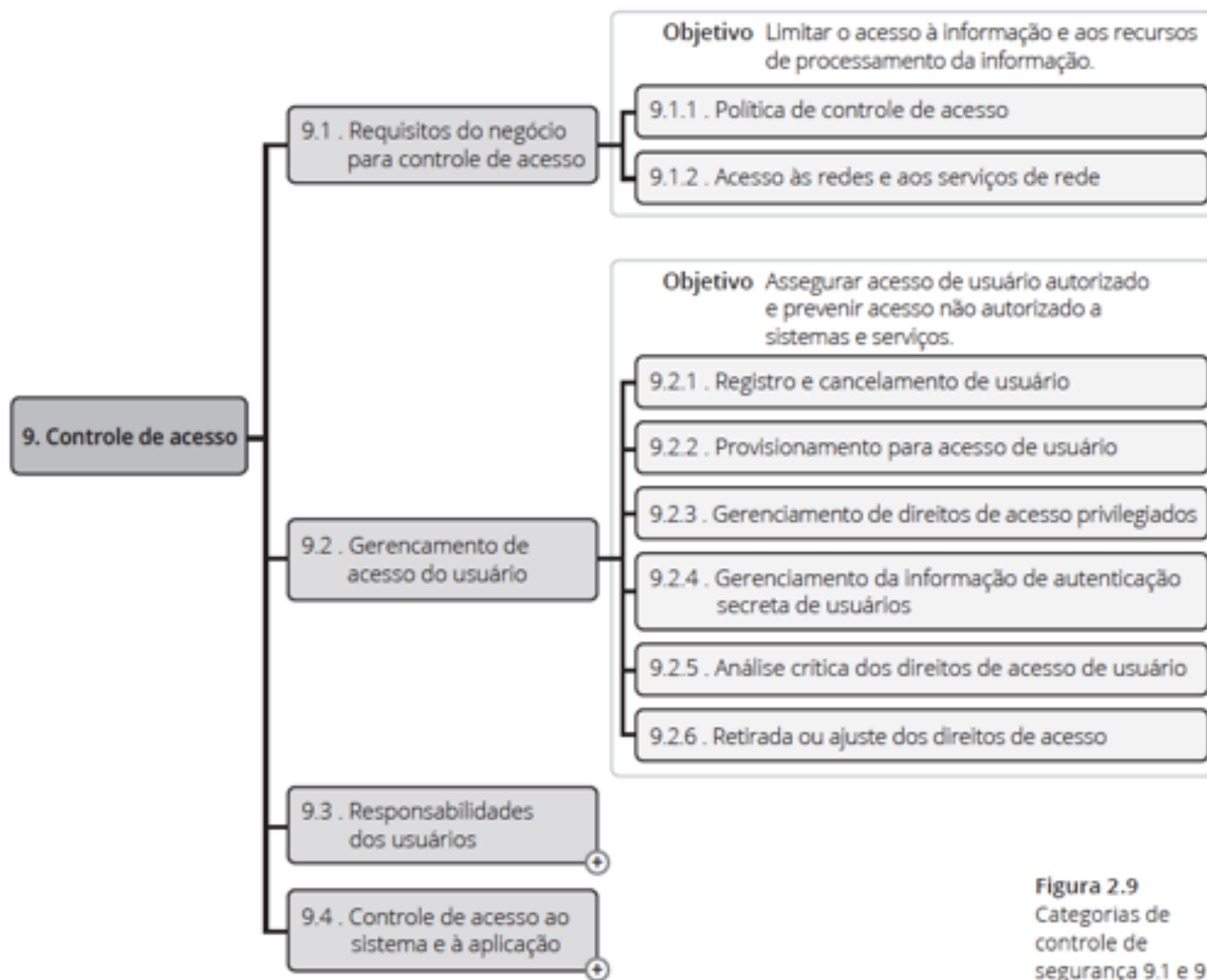


Figura 2.9
Categorias de controle de segurança 9.1 e 9.2

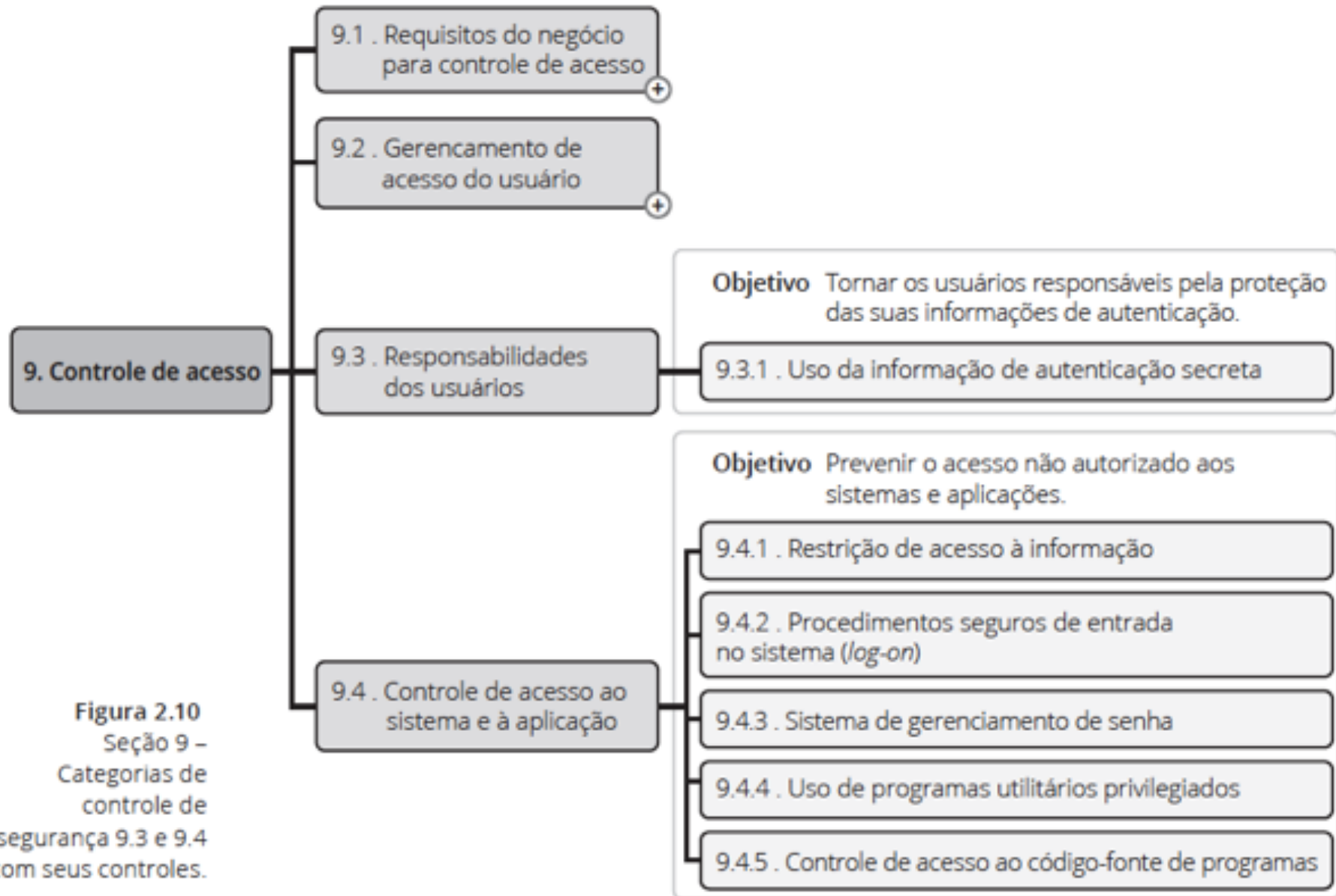


Figura 2.10
 Seção 9 –
 Categorias de
 controle de
 segurança 9.3 e 9.4
 com seus controles.

Sistema de Gestão da Segurança da Informação

Apresentar uma visão geral e escopo do Sistema de Gestão da
Segurança da
Informação (SGSI), assim como uma análise crítica e
detalhamento dos controles.
Modelos SGSI.



**NORMA
BRASILEIRA**

**ABNT NBR
ISO/IEC
27001**

Segunda edição
08.11.2013

Válida a partir de
08.12.2013

**Tecnologia da informação — Técnicas de
segurança — Sistemas de gestão da segurança
da informação — Requisitos**

*Information technology — Security techniques — Information security
management systems — Requirements*

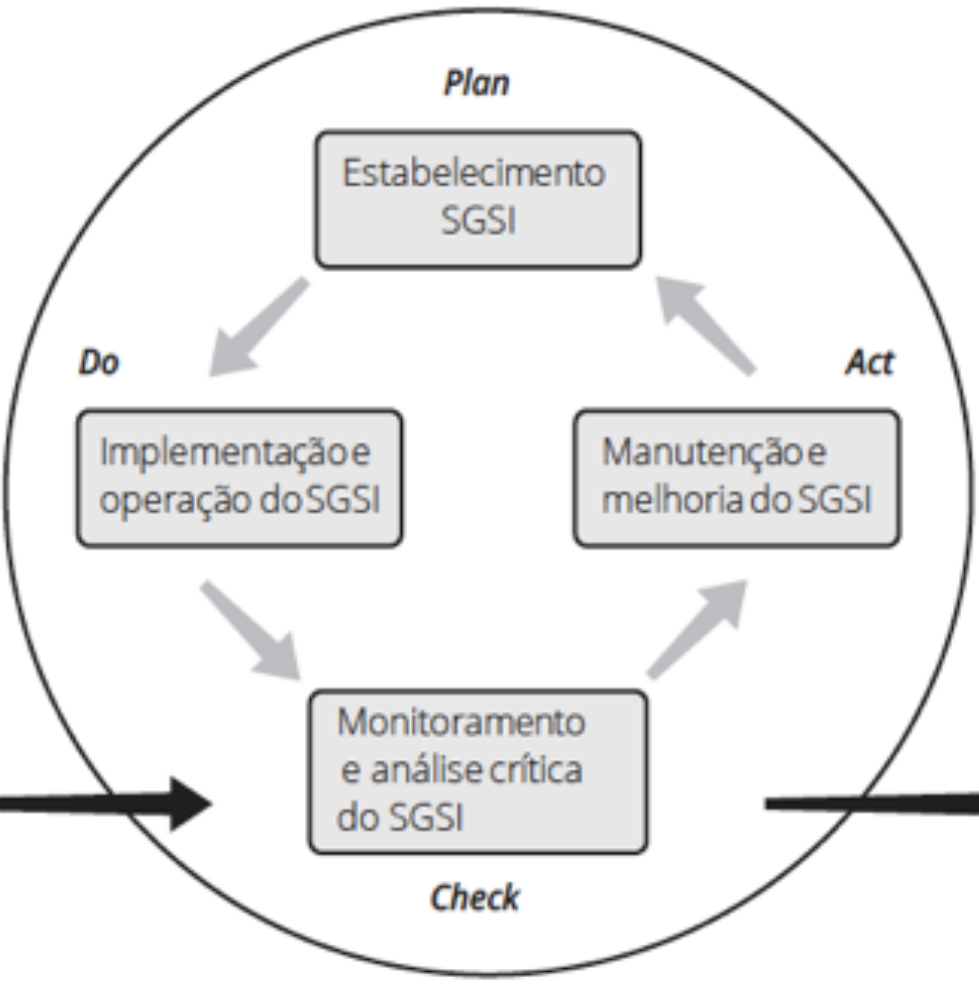


Visão geral e escopo

- › O Modelo de Sistema de Gestão de Segurança da Informação (SGSI) integra a estratégia
- › da organização, sendo influenciado por fatores como:
 - › Necessidades e objetivos.
 - › Requisitos de segurança.
 - › Processos.
 - › Estrutura organizacional.

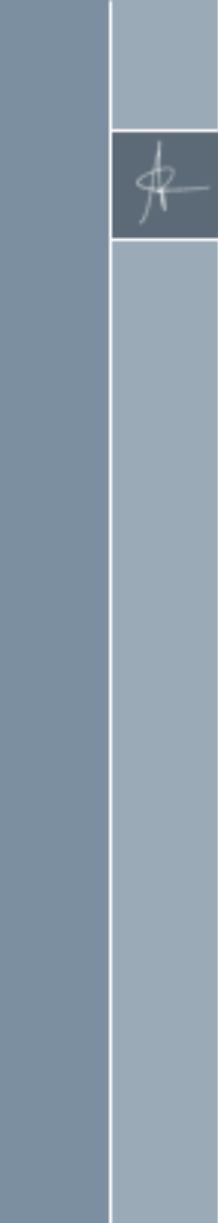
Partes interessadas

Expectativas e requisitos de segurança da informação




Partes interessadas

Segurança da informação gerenciada

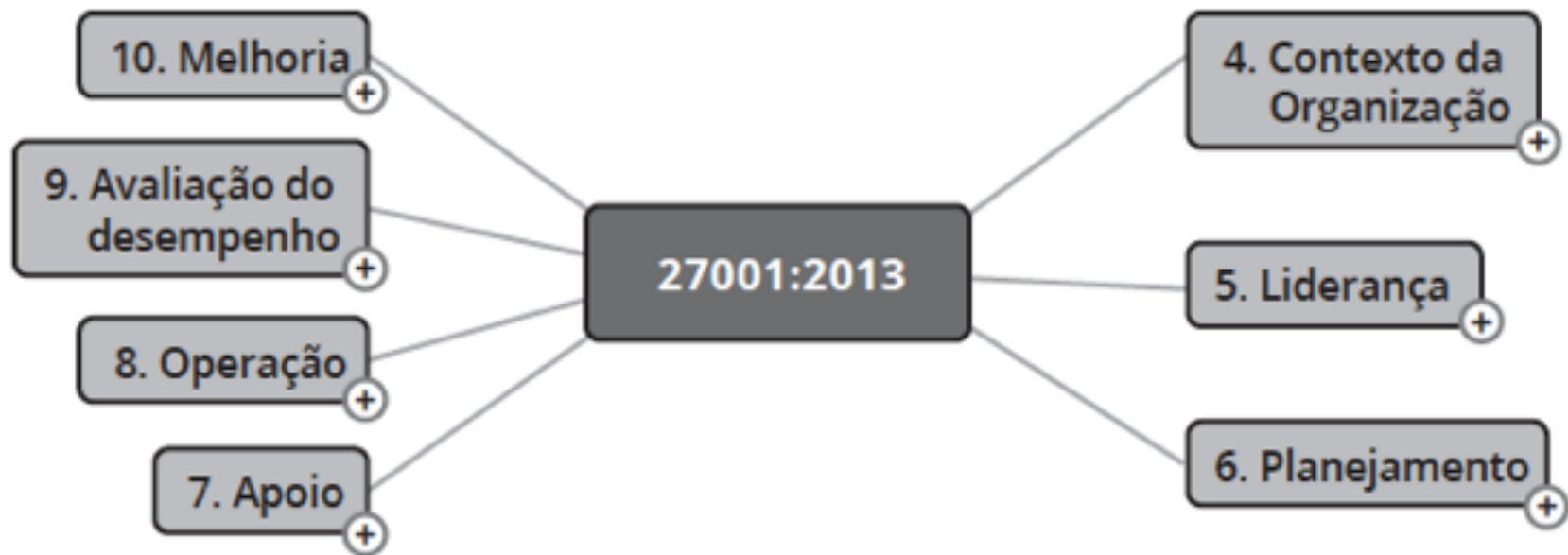


Sistema de Gestão da Segurança da Informação (SGSI)

- › Requisitos gerais:
 - › A organização deve estabelecer, implementar, operar, monitorar, analisar criticamente,
 - › manter e melhorar o SGSI.
 - › Estabelecendo e gerenciando o SGSI.
 - › Requisitos da documentação.
- 



Estrutura da Norma





4. Contexto da Organização

- › Entendendo a organização e seu contexto.
- › Entendendo as necessidades e as expectativas das partes interessadas.
- › Determinar o escopo do sistema de gestão da segurança da informação.
- › Sistema de gestão da segurança da informação.



5. Liderança

- › Liderança e comprometimento.
- › Política.
- › Autoridades, responsabilidades e papéis organizacionais.



6. Planejamento

- › 6.1 Ações para contemplar riscos e oportunidades.
 - Geral.
 - Avaliação de riscos de segurança da informação.
 - Tratamento de riscos de segurança da informação.
- › 6.2 Objetivo de segurança da informação e planejamento para alcançá-los.



7. Apoio

- › Recursos.
- › Competência.
- › Conscientização.
- › Comunicação.
- › Informação documentada.
 - Geral.
 - Criando e atualizando.
 - Controle da informação documentada.



8. Operação

- › Planejamento operacional e controle.
- › Avaliação de riscos de segurança da informação.
- › Tratamento de riscos de segurança da informação.



9. Avaliação do desempenho

- › Monitoramento, medição, análise e avaliação.
- › Auditoria interna.
- › Análise crítica pela Direção.



10. Melhoria

- › Não conformidade e ação corretiva.
- › Melhoria contínua.



A. Anexo

- › Controles e objetivos de controle.
- › Alinhados com a ABNT NBR ISO/IEC 27002:2013 (Seções 5 a 18).

Anexo A (normativo)

Referência aos controles e objetivos de controles

Os controles e objetivos de controles listados na Tabela A.1 são derivados diretamente e estão alinhados com aqueles listados na ABNT NBR ISO/IEC 27002:2013^[1], Seções 5 a 18, e devem ser usados em alinhamento com 6.1.3

Tabela A.1 – Objetivos de controle e controles

A.5 Políticas de segurança da informação		
A.5.1 Orientação da Direção para segurança da informação		
Objetivo: Prover orientação da Direção e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.		
A.5.1.1	Políticas para segurança da informação	Controle Um conjunto de políticas de segurança da informação deve ser definido, aprovado pela Direção, publicado e comunicado para os funcionários e partes externas relevantes.
A.5.1.2	Análise crítica das políticas para segurança da informação	Controle As políticas de segurança da informação devem ser analisadas criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.

ISO 27001 vs. ISO 27002 - Dejan Kosutic

If you came across both the [ISO 27001](#) and the ISO 27002, you probably noticed that ISO 27002 is much more detailed, much more precise – so, what's the purpose of ISO 27001 then?

First of all, you cannot get certified against ISO 27002 because it is not a management standard. What does a management standard mean? It means that such a standard defines how to run a system, and in case of ISO 27001, it defines the information security management system (ISMS) – therefore, [certification against ISO 27001 is possible](#).

This management system means that information security must be planned, implemented, monitored, reviewed, and improved. It means that management has its distinct responsibilities, that objectives must be set, measured and reviewed, that internal audits must be carried out and so on. All those elements are defined in ISO 27001, but not in ISO 27002.

The controls in ISO 27002 are named the same as in Annex A of ISO 27001 – for instance, in ISO 27002 control 6.1.6 is named Contact with authorities, while in ISO 27001 it is A.6.1.6 Contact with authorities. But, the difference is in the level of detail – on average, ISO 27002 explains one control on one whole page, while ISO 27001 dedicates only one sentence to each control.

Finally, the difference is that ISO 27002 does not make a distinction between controls applicable to a particular organization, and those which are not. On the other hand, ISO 27001 prescribes a risk assessment to be performed in order to identify for each control whether it is required to decrease the risks, and if it is, to which extent it should be applied.

The question is: why is it that those two standards exist separately, why haven't they been merged, bringing together the positive sides of both standards? The answer is usability – if it was a single standard, it would be too complex and too large for practical use.

Every standard from the ISO 27000 series is designed with a certain focus – if you want to build the foundations of information security in your organization, and devise its framework, you should use ISO 27001; if you want to



27001 vs 27002

Anexo A (normativo)

Referência aos controles e objetivos de controles

Os controles e objetivos de controles listados na Tabela A.1 são derivados diretamente e estão alinhados com aqueles listados na ABNT NBR ISO/IEC 27002:2013^[1], Seções 5 a 16, e devem ser usados em alinhamento com 6.1.3

Tabela A.1 – Objetivos de controle e controles

A.5 Políticas de segurança da informação		
A.5.1 Orientação da Direção para segurança da informação		
Objetivo: Prover orientação da Direção e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.		
A.5.1.1	Políticas para segurança da informação	Controle Um conjunto de políticas de segurança da informação deve ser definido, aprovado pela Direção, publicado e comunicado para os funcionários e partes externas relevantes.
A.5.1.2	Análise crítica das políticas para segurança da informação	Controle As políticas de segurança da informação devem ser analisadas criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.

5 Políticas de segurança da informação

5.1 Orientação da direção para segurança da informação

Objetivo: Prover orientação da Direção e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

5.1.1 Políticas para segurança da informação

Controle

Convém que um conjunto de políticas de segurança da informação seja definido, aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes.

Diretrizes para implementação

Convém que, no mais alto nível, a organização defina uma política de segurança da informação, que seja aprovada pela direção e estabeleça a abordagem da organização para gerenciar os objetivos de segurança da informação.

Convém que as políticas de segurança da informação contemplem requisitos oriundos de:

- estratégia do negócio;
- regulamentações, legislação e contratos;
- ambiente de ameaça da segurança da informação, atual e futuro.

Convém que a política de segurança da informação contenha declarações relativas a:

- definição de segurança da informação, objetivos e princípios para orientar todas as atividades relativas à segurança da informação;
- atribuição de responsabilidades, gerais e específicas, para o gerenciamento da segurança da informação para os papéis definidos;
- processos para o tratamento dos desvios e exceções.

No nível mais baixo, convém que a política de segurança da informação seja apoiada por políticas específicas do tema, que exigem a implementação de controles de segurança e que sejam estruturadas para considerar as necessidades de certos grupos de interesse dentro da organização ou para cobrir tópicos específicos.

São exemplos de tais temas de política:

- controle de acesso (ver Seção 9);
- classificação e tratamento da informação (ver 8.2);
- segurança física e do ambiente (ver Seção 11);
- tópicos orientados aos usuários finais:
 - uso aceitável dos ativos (ver 6.1.3);
 - mesa limpa e tela limpa (ver 11.2.9);
 - transferência de informações (ver 13.2.1);
 - dispositivos móveis e trabalho remoto (ver 6.2);
 - restrições sobre o uso e instalação de software (ver 12.6.2);
- backup (ver 12.3);

Avaliação da Conformidade





Conceitos Básicos





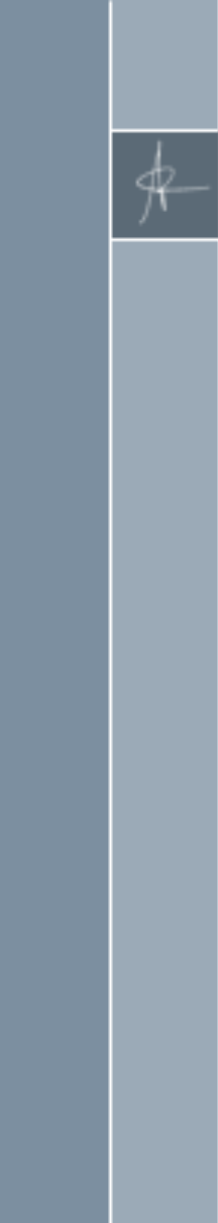
O que é avaliação da conformidade

- › Conjunto de técnicas e atividades que têm por objetivo garantir que um produto, processo, serviço, sistema de gestão, pessoa ou organização atende a um conjunto de requisitos.
 - Exemplos dessas técnicas e atividades incluem estimação, auditoria, calibração, avaliação, exame, inspeção, e teste
 - Podem resultar numa declaração de conformidade pelo fornecedor, numa certificação ou numa acreditação
- › Requisitos específicos para produto, processo, serviço, sistema de gestão, pessoa ou organização são encontrados em documentos normativos tais como regulações, padrões e códigos de prática



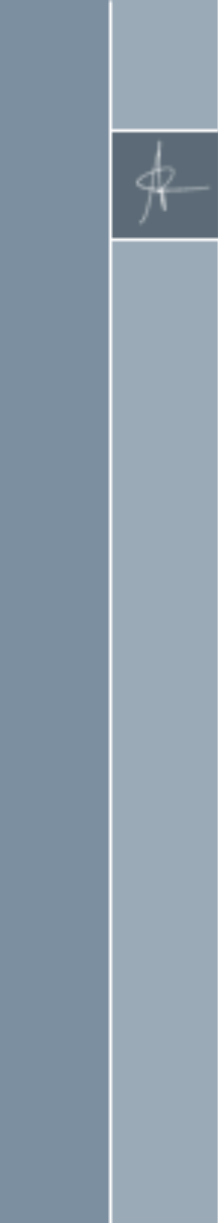
Padrões e Avaliação da Conformidade

- › A ISO (International Organization for Standardization) e a IEC (International Electrotechnical Commission) possuem publicações internacionais sobre avaliação da conformidade
 - Essas publicações internacionais são amplamente reconhecidas e usadas nos mais diversos setores e atores para atividades de avaliação da conformidades




Regulação, padrões e avaliação da conformidade

- › Regulações são usadas em todo o mundo e a maioria dos exemplos faz referência a métodos de avaliação da conformidade para atestar o atendimento a requisitos descritos em padrões
 - Tais padrões podem ser internacionais, nacionais, ou mesmo locais
 - Em alguns casos, apenas partes dos padrões são mandatórios
- › Regulações podem incluir requisitos para a avaliação da conformidade



Regulação, padrões e avaliação da conformidade

- › Basear a avaliação da conformidade em padrões internacionais favorece o reconhecimento do processo como bem-fundamentado e legítimo.
 - › Avaliação da conformidade de acordo com padrões internacionais evita que regulações adicionem custos desnecessários e questionamentos quanto a barreiras técnicas ao comércio
- 



Técnicas de avaliação da conformidade

- › **Avaliação (assessment)** da competência técnica de uma organização;
- › **Auditoria** de um sistema de gestão de uma organização;
- › **Avaliação (evaluation)** de um produto, processo ou serviço em relação a um conjunto de requisitos;
- › **Exame** da competência de uma pessoa;
- › **Inspeção** de uma instalação, produto ou serviço;
- › **Teste** de uma característica de produto.



Padrões mais relevantes

- › ISO/IEC DIS 17000 [Under development]
 - Conformity assessment -- Vocabulary and general principles
- › ISO/IEC 17011:2017
 - Conformity assessment -- Requirements for accreditation bodies accrediting conformity assessment bodies
- › ISO/IEC 17020:2012
 - Conformity assessment -- Requirements for the operation of various types of bodies performing inspection
- › ISO/IEC 17021 (várias partes)
 - Conformity assessment -- Requirements for bodies providing audit and certification of management systems
- › ISO/IEC 17025:2017
 - General requirements for the competence of testing and calibration laboratories



Padrões mais relevantes

- › ISO 17034:2016
 - General requirements for the competence of reference material producers
- › ISO/IEC 17040:2005
 - Conformity assessment -- General requirements for peer assessment of conformity assessment bodies and accreditation bodies
- › ISO/IEC 17043:2010
 - Conformity assessment -- General requirements for proficiency testing
- › ISO/IEC 17065:2012
 - Conformity assessment -- Requirements for bodies certifying products, processes and services
- › ISO/IEC 17067:2013
 - Conformity assessment -- Fundamentals of product certification and guidelines for product certification schemes











ORGANISMOS DE AVALIAÇÃO DA CONFORMIDADE





Organismos de Avaliação da Conformidade

	Padrão internacional	Primeira Parte	Segunda Parte	Terceira Parte
Laboratório de Ensaios e Calibração	ISO/IEC 17025			
Organismos de Inspeção	ISO/IEC 17020			
Organismos de Certificação de Pessoas	ISO/IEC 17024			
Organismos de Certificação de Produtos, Processos e Serviços	ISO/IEC 17065			
Organismos de Certificação de Sistemas de Gestão	ISO/IEC 17021			