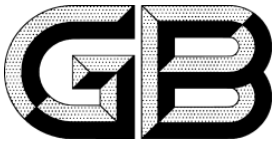
Chinastandards.org



chinastandards.org - PREVIEW

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

GB/T 20261-2020

Information security technology. System security engineering. Capability maturity model

Issued on: November 19, 2020 **Implemented on: June 1, 2021**

Issued by: SAMR; SAC

Preview: page 1 of 5 shown, full document available. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-20261-2020

Chinastandards.org

Table of Contents

Chinastandards.org · PREVIEW

Preview: page 2 of 5 shown, full document available. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-20261-2020

Foreword

This Standard was drafted in accordance with the rules given in GB/T 1.1-2009.

This Standard replaces GB/T 20261-2006, Information technology - Systems security engineering - Capability maturity model. Compared with GB/T 20261-2006, the main technical changes are as follows (see Annex G for the comparison of main changes).

- Modify some normative references (see Clause 2; Clause 2 of the 2006 edition);
- Add terms and definitions, namely "base practices; BP", "capability", "information security event", "information security incident", "process area; PA", "risk management";
- Modify the definitions of "assurance", "engineering group", "work product" in Terms and definitions; and modify "residual risk" to "residual risk" (see Clause 3; Clause 3 the 2006 edition).
- Remove the term "practices" (see 3.24 of the 2006 edition);
- Modify some clause and sub-clause titles, merge, adjust and delete some contents that are related or not suitable as national standards (see 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 5.1);
- Delete the original Clause 5, and adjust the original Clause 6 and Clause 7 to Clause

5 and Clause 6 (Clause 5, Clause 6 and Clause 7 of the 2006 edition);

- Add BP.06.03 Define Security Measures in Clause 6, and the additions and revisions of ISO/IEC 21827.2008 relative to ISO/IEC 21827.2002 (see Clause 6);
- Add Annex A and Annex B (see Annex A, Annex B);
- Modify the definition of the five levels of capability level in Annex C to be consistent with the description of the current standard GB/T 30271 and other standards;
- Modify the error message that the serial process area number does not match the process area description in Annex D (see D.6.1.1, D.7.7.3, D.9.3.3, D.11.1.1, D.11.4, D.11.4.1, D.12.3.1);
- Add Annex F to facilitate the mapping relationship between the standard model and the current security services (see Annex F);

Preview: page 3 of 5 shown, full document available. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-20261-2020

- Add a comparison table of major changes compared with GB/T 20261-2006 (see Annex G).

This Standard uses the redrafting method to modify and adopt ISO/IEC 21827.2008 Information technology - Security techniques - Systems Security Engineering - Capability Maturity Model(R) (SSE-CMM(R)).

Compared with ISO/IEC 21827.2008, this Standard makes many adjustments in structure. Annex A gives a comparison list in clause numbers between this Standard and ISO/IEC 21827.2008.

This Standard has technical differences compared with ISO/IEC 21827.2008.Annex B gives a list of the corresponding technical differences and their reasons.

This Standard makes the following editorial changes.

- Modify the standard name to Information security technology - System security engineering - Capability maturity model.

chinastandards.org · PREVIEW

1 Scope

This Standard specifies the Systems Security Engineering - Capability Maturity Model (SSE-CMM(R)). The SSE-CMM(R) is a process reference model focused upon the requirements for implementing security in a system or series of related systems that are the information technology security (ITS) domain.

2 Normative references

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

GB/T 18336.1-2015, Information Technology - Security Techniques - Evaluation Criteria for IT Security - Part 1.Introduction and General Model (ISO/IEC 15408-1.2009, IDT)

3 Terms and definitions

For the purposes of this document, the following terms and definitions, as well as those

Preview: page 4 of 5 shown, full document available. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-20261-2020

defined in GB/T 25069-2010, GB/T 29246-2017, GB/T 18336.1-2015 and GB/T 30271-2013, apply. For ease of use, some terms and definitions in GB/T 25069-2010 are repeated below.

4 Overview of System Security Engineering

Security engineering is becoming an increasingly critical discipline and should be a key component in multi-disciplinary, concurrent, engineering teams. This applies to the development, integration, operation, administration, maintenance, and evolution of systems and applications as well as to the development, delivery, and evolution of products.

5 Model System Architecture

An unwanted incident is made up of three components. threat, vulnerability, and impact. Vulnerabilities are properties of the asset that may be exploited by a threat and include weaknesses. If either the threat or the vulnerability is not present there can be no unwanted incident and thus no risk.

6 Security Base Practices

Security configuration of all devices (or equipment) requires management. This base practice recognizes that system security relies to a great extent on a number of interrelated components (hardware, software, and procedures) and that normal configuration management practices may not capture the interrelated dependencies required for secure systems.

.....

Chinastandards.org · PREVIEW

Preview: page 5 of 5 shown, full document available. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-20261-2020