ICS 35.030
CCS L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 47470-2026

Cybersecurity technology - Assessment criteria for secure software development capability

网络安全技术 软件安全开发能力评估准则

Issued on: April 30, 2026 **Implemented on: November 1, 2026**

Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC

Table of Contents

4 General Principles

4.1 Software security development capabilities The organization uses the software lifecycle as a framework to analyze the periods in which software security vulnerabilities exist, and constructs a security process and organization for software development. The management of security processes aims to identify potential security threats to software, reduce the likelihood of security vulnerabilities, and prevent software from being intentionally damaged or compromised. Forced to fail security objectives. An organization's software security development capability is acquired through the execution of eight security processes, which include security aspects in software development. The security process comprises five stages. comprehensive requirements analysis, security technology implementation, security testing, security release, and security maintenance. In terms of organizational management, it includes security governance. The three security processes are. management, development support, and security measurement and improvement. The safety process is systematically described according to three levels. process, process area, and basic practices. Among these, process is the highest level. This section describes the safety objective of performing this process, and a set of process areas that indicate that the objective has been successfully achieved; process areas are defined by their... The way the goal and output activities are defined translates into a lower-level process. A process area typically includes a name, a goal, and a set of outputs. Activities; basic practices are the set of activities that implement process domain objectives, used to further describe the intent and mechanisms of the activities. Work products are basic practices. For examples of work products from the process domain, see Appendix A for the outputs of the practice. Based on the three levels mentioned above, software security development consists of 8 security processes, 20 security process areas, and 119 basic practices. An organization's software

security development capability is its ability to achieve software security goals through the execution of process activities.

4.2 Ability Level Software security development capability levels are set at five levels, with higher capability levels indicating greater predictability of software security objectives and greater controllability of processes. The stronger the characteristics of effectiveness and execution, the more hierarchical the description of activity features are, with each evolutionary level building upon the previous level. Add new activity features or performance characteristics. The descriptions and activity characteristics of the ability levels are as follows:

a) Level 1. 1) Description. The organization possesses the capability to conduct basic software security development activities, and implements software security development in stages and selectively. Launch related activities; 2) Activity Characteristics. Initial Execution. The organization executes activities related to the software security development process based on internal or external security requirements. An effective mechanism has not been established to ensure the continued operation of related activities.

b) Level 2. 1) Description. The organization possesses the capability to conduct software security development activities in a planned and tracked manner, and can analyze security features. Verification ensures that the software development process is secure and controllable. 2) Activity Characteristics. Executed according to a plan. The organization gradually accumulates process assets and conducts measurement and analysis activities targeting business security objectives. The execution of the verification process conforms to applicable standards and procedures and is reproducible in similar software, but it has not been separated from the group. The organizational level forms a systematic capability.

c) Level 3. 1) Description. The organization possesses the capability to define standardized software security development activities and execute them systematically and in a standardized manner, and can analyze security... Problems were identified and improvement measures were proposed to ensure a consistent software security development process across the organization; 2) Activity Characteristics. Systematic Execution. Defining and standardizing software security development processes, procedures, documents, and tools at the organizational level. Platforms, etc., can be tailored to unique project or work characteristics, and can establish and maintain software security development process assets. The library utilizes tool platforms to conduct process management and development support activities.

d) Level 4. 1) Description. The organization possesses the capability to use metrics data for software security development governance and has the ability to quantitatively control security technology activities. The ability to ensure the efficient achievement of organizational security objectives; 2) Activity Characteristics. Quantitative Control of Execution. Measurable software security development goals are established at the organizational level, and metric indicators are set. The system supports the achievement of

security objectives and the control of business risks; it establishes and promotes the use of reusable, modular security assets. Libraries and automated testing toolchains systematically improve the efficiency of software security development.

e) Level 5. 1) Description. The organization possesses the ability to self-optimize software security development activities and processes in the face of complex situations, and can do so in a predictable manner. This involves changing and adjusting organizational-level security objectives and implementation processes. 2) Activity Characteristics. Continuous optimization of execution. Key organizational processes are identified through quantitative assessment of safety objectives and analysis of performance data. Identify and address common and recurring problems, proactively and predictively optimize and improve organizational processes, enhance the effectiveness of specific processes, and ensure the achievement of goals. The software security development process is continuously being optimized and developed.

4.3 Evaluation Model The software security development capability assessment model divides 119 basic practices into 20 process areas based on the software lifecycle, and assigns them to 8 security categories. Throughout the process, five different levels of activity characteristics are defined to provide relevant basic practices for evaluating an organization's implementation of refined process management. The ability to achieve software security goals. The model structure is shown in Figure 1.

5.1 Security Requirements Analysis

5.1.1 Process Description The security requirements analysis process consists of two process areas. establishing a security requirements baseline and supplementing security requirements. Security requirements are designed to achieve organizational goals. Driven by security objectives, we developed a system that aligns with the organization's business requirements through in-depth analysis of laws, regulations, industry oversight, and user access requirements. Establish a baseline of security requirements to ensure that the software complies with security standards during use, while protecting personal information and data security; through network security... The tracking and analysis of risks, including full-incident events, legacy testing defects, and potential vulnerabilities identified through threat modeling, will further inform the development of strategies to improve software security. Additional security requirements for the features. Organizations gain different levels of security requirements analysis capabilities by implementing basic practices in two process areas.

5.1.2 PA01 - Establishing a baseline for security requirements This process domain defines activities related to software compliance, personal information protection, data security, and enhancing software resilience, primarily including the following. content.

a) Summary Description. Analyze compliance requirements for information such as laws and regulations, user access, and industry standards, and identify security vulnerabilities in

conjunction with business scenarios. Risk assessment involves establishing a baseline of security requirements tailored to the organization's business needs, ensuring that software meets security compliance, personal information protection, and data security requirements. According to security requirements, it possesses anti-attack capabilities;

b) Objective. To ensure the integrity of security requirements in software development and to guarantee that activity definitions meet basic security requirements;

c) Basic Practice Level Description. The establishment of a safety requirements baseline is divided into 3 levels and 6 basic practices, as shown in Table 1.

5.1.3 PA02 - Supplementary Safety Requirements This process area defines supplementary security requirement activities that enhance software security competitiveness based on the baseline security requirements. These mainly include the following. content.

a) Summary Description. Based on user access requirements, policies and regulations, known security issues in the application software, and legacy security testing issues, Threat modeling identifies security issues, security requirements to meet security strategic planning, and user security vulnerabilities, all within the framework of security needs. Based on the existing framework, security requirements were developed to enhance the software's security competitiveness.

b) Objective. Based on security vulnerabilities encountered by users during actual use, identify corresponding security needs and explore competitive advantages that can improve product security. The security requirements of competitiveness;

c) Basic Practice Level Description. Supplemental security requirements are divided into 3 levels and 5 basic practices, as shown in Table 2.

5.2 Security Technology Implementation

5.2.1 Process Description The process of implementing security technology includes designing a security architecture, managing open-source and third-party components, standardizing secure coding, reviewing code security, and implementing security measures. The entire build process consists of five process areas. Software architecture security analysis and design are crucial foundations for software security, and continuous optimization and improvement of the software architecture are essential. Design can effectively improve the efficiency of secure software development. Meeting the security and compliance requirements of open-source and third-party components is essential for secure implementation. Requirements. Standardized secure coding and code security reviews are essential means of ensuring code security. Organizations achieve different levels of security technology implementation capabilities by implementing basic practices in five process areas.