BRICS 2022 CHINA

2022 BRICS Skills Competition

(BRICS Future Skills Challenge)

TECHNICAL DESCRIPTION

Cyber Security (Offline)

Catalogue

I. Brief Introduction

（I）Name and description of the skill competition

The name of the skill contest

Cyber Security

Skills Competition Description

Cyber Security of BRICS Skills Competition is through the competition for competitors familiar with the international competition cyber security project professional standards, test, test security operations, security audit, cyber security emergency response, digital forensic investigation, application security and cyber penetration, test team plan organization and team cooperation and other comprehensive professional quality, emphasize students 'innovation ability and practice ability training, improve students' professional ability and employment quality.

This event is held in the form of team competition, with 3 competitors from each team (1 captain).

Through team cooperation, we will break down technical barriers, achieve mutual empowerment, promote the ecological layout of international talents in the cyber security industry, and accelerate the construction of cyber security and related technical standards. Adhering to the international top competition "open cooperation" professional competitive spirit, service national strategy, deepen the integration, improve the level of "internationalization", participate in "Belt and Road" construction, "improve" LuBan workshop "talent training quality, accelerate the" post "fusion education reform, to build, to promote change, strengthen vocational education adaptability, cultivate with international vision, know the international rules of international personnel of" internationalization " technical skills, improve the level of BRICS Skills Competition and international influence.

Competition system

Cyber security offline competition will be realized by the cyber security technology offline training and competition system as the carrier.

（II）The relevance and importance of this document

This document contains information on the standards required for this skills competition, as well as the evaluation principles, methods, and procedures for managing the competition.

Each expert and competitor must understand and understand this technical

description.

If there is any conflict between the technical instructions in the different languages, the English version shall prevail.

II. Skills Standard

（I）General description of the skill standards

Skills standards define knowledge, understanding, and specific skills that are international best practice in technical and professional performance. It will reflect a global consensus on what the relevant job roles or professions are represented in industry and business.

The skill competition is designed to reflect the international best practices described by the skill standard and the extent to which it can reach. Therefore, the standard is a guide for the training and preparation required for skills competitions.

The standard is divided into different sections with titles and reference numbers.

Each fraction was assigned a percentage of the total score to indicate its relative importance in the criteria. This is often referred to as the "weights". The sum score for all percentages was 100. The weights determine the allocation of the scores in the scoring criteria.

By testing the items, the scoring scheme only evaluates the skills listed in the standard. They will reflect the criteria as fully as possible under the constraints of skills competitions.

The scoring scheme will be performed within the assigned score assigned in the criteria. A 5% change is allowed, but the weight assigned by the standard specification shall not be changed.

（II）Skills standard

1. General specifications for skill standards

standard specification	
1	**Work organization and management**
	Should know and understand that:
	Health and safety-related regulations, obligations and regulations
	Personal protective equipment must be used, such as: electrostatic protection, electrostatic discharge
	The importance of integrity and security in dealing with user equipment and information

	The importance of waste recycling and safe disposal
	Methods of planning, scheduling, and prioritization
	In all the course of the work practice, focus on the importance of accuracy, inspection and detail
	The importance of systematic work
	The 6S management of the working environment
	Should be able to:
	Compliance with health and safety standards, rules, and regulations
	Maintain a safe working environment
	Identify and use the appropriate personal electrostatic protection equipment
	Safand properly select, use, clean, maintain and store tools and equipment
	Abide by relevant regulations, plan work areas, maintain daily cleanliness, and maximize work efficiency
	Work effectively and check progress and results
	Adopt comprehensive and effective research methods to ensure that knowledge is constantly updated
	Actively try out new methods, new systems, and a willingness to accept change
2	Security provisions
	Should know and understand that:
	Information Technology risk management standards, policies, requirements, and processes
	Function and usage of network defense and vulnerability assessment tools
	Specific functions of the operating system
	Computer programming-related concepts, including computer language, programming, testing, debugging, deletion, and file types
	Cyber security and privacy principles and methods applied to software development
	Should be able to:
	Cyber security and privacy principles should be applied to management requirements when designing the master procedure testing and recording the assessment process (Related to confidentiality, integrity, availability, authentication, digital signature)
	Independent and comprehensive assessment of management, operational and technical security controls, and internal or inherited information technology systems Control improvements are evaluated to determine the overall effectiveness of the control

	Develop, create, and maintain new computer applications, software, or specialized applications
	Modify existing computer applications, software, or specialized applications
	Analyze the security status of new or existing computer applications, software, or professional applications to provide those available analytic result
	Conduct software system research and develop new functions to ensure cyber security protection functions
	Comprehensive technical research is conducted to evaluate the possible weak links in the cyber security system
	Plan, prepare, and implement the system tests
	Analyze, evaluate, and report the results according to the technical specifications and requirements
	Test and evaluate the security situation of the information system, covering the system development lifecycle
3	**Operation, maintenance, supervision, and management**
	Should know and understand that:
	Query language, such as SQL (Structured query language)
	Data backup and recovery, and a data normalization strategy
	Network protocols, such as TCP / IP, Dynamic Host Configuration (DHCP), Domain Name System (DNS), and Directory services
	Firewall concepts and features
	The concept of a cyber security architecture, including topologies, protocols, components, and principles
	System, network, and operating system reinforcement techniques
	Manage information technology, user security policies (for example: account creation, password rules, access control)
	Information Technology Security Principles and Methods
	Authentication, authorization, and access control methods
	Cyber security, vulnerabilities, and privacy principles
	Learning Management System and its Application in Management Learning
	The impact of Cyber security Law and other relevant regulations on its network planning
	Should be able to:
	Manage databases or database management systems

	Manage and implement processes and tools to ensure that organizations can identify, archive, and access knowledge assets and information content
	Handle problems, install, configure, troubleshoot, and provide maintenance and training to customer needs or consultation
	Complete the accuracy verification of the collected data
	Install, configure, test, run, maintain, and manage networks and firewalls, including hardware and software, to ensure that all information is shared, transmitted, and provide support for information security and information systems
	Install, configure, debug, and maintain servers (hardware and software) to ensure the confidentiality, integrity, and availability of information
	Manage accounts, set up firewalls, and install operating system patches
	Access control, the creation and management of accounts, and passwords
	Check the organization's existing computer systems and processes to help the organization operate more safely, faster and more efficiently
	Assist in monitoring information systems or networks, possible problems with information security within management agencies, or other aspects that need to be held accountable, including strategies, personnel, infrastructure, needs, policy implementation, emergency plans, security awareness, and other resources.
4	**Protection and defense**
	Should know and understand that:
	File System implementation (e. g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT])
	System files (such as log files, registry files, configuration files) contain relevant information and where these system files are stored
	The concept of cyber security architecture including topologies, protocols, stratification, and principles
	Industry technical standards and analytical principles, methods, and tools
	Threat investigations, reporting, investigation tools, and laws and regulations
	Cyber security event categories, responses, and handling methods

	Cyber defense and Vulnerability assessment tools and their capabilities
	Response to known security risks
	Authentication, authorization, and access methods
	Should be able to:
	Use safeguards and use information collected through different channels to identify, analyze, and report occurring, or possible, network events to protect information, information systems, and networks from threats
	Tests, implements, deploys, maintains, checks, manages the hardware infrastructure and software, and effectively manages the network and resources of the computer network protection service providers as required
	Monitor the network and timely record the unauthorized activities
	Effectively respond to a crisis or emergency in your field, and reduce direct and potential threats in your field of expertise
	Using mitigation and preparedness measures, respond to requirements and implement recovery to maximize survival and secure property and information
	Investigate and analyze relevant cyber security emergency response activities
	Assess the threats and vulnerabilities
	Evaluate risk levels and develop appropriate mitigation measures in operational and non-operational situations
5	**Analyse**
	Should know and understand that:
	Background and methods used by cyber-threat actors
	Methods and techniques used for the detection of the various available activities
	Network intelligence information collection capability and resource base
	Network threats and vulnerabilities
	Cyber security basics (e. g., encryption, firewall, authentication, trapping system, peripheral protection)
	Vulnerability information propagation sources (e. g., alerts, notifications, errata, and announcements)
	The structure, methods, and strategies of the development tools (e. g., sniffing, recording keyboards), and techniques (e. g., obtaining backdoor access, collecting confidential data, and performing vulnerability analysis of other systems in the network)

	Internal strategies for predicting, simulating threats, and coping
	Internal and external collaborative network operations and tools
	System forgery and judicial use cases
	Should be able to:
	Identify and evaluate cybersecurity offender activities
	Issue findings to help initialize or support law enforcement and anti-intelligence investigations or
	Analyze the information collected to find system weaknesses and potential links
	Analyze threat information from different channels, different disciplines and different agencies in the
	Synchronize and place intelligence information to find out possible meanings
	Apply the latest knowledge from one or more different countries, regions, organizations, and technical fields
	Apply language, culture, and technical expertise for information collection, analysis, and other cyber security activities
	Identify, preserve and use system development process legacy and used for analysis
6	**Collection and operation**
	Should know and understand that:
	Collection strategies, techniques, and tool applications
	Network information and intelligence gathering capability and the utilization of the resource base
	Transformation, tracking, and prioritization of information requirements and collection requirements
	Network operations plans, policies, and related resources
	Network operations policies, resources, and tools
	The concept of the network operation, the network operation terms, the principles, functions, boundaries, and effects of the network operation
	Should be able to:
	Use appropriate strategies to establish priority through the process of collection and management to
	Implement in-depth joint targeting and execute cyber security processes
	Collect information according to requirements and implement detailed plans and orders
	Support the collection of evidence about cyber threats to mitigate or protect them from possible or real-time cyber threats

7	Investigate
	Should know and understand that:
	Threat investigations, reporting, investigation tools, and laws and regulations
	Concepts and methods of malware analysis
	The process of collecting, packaging, transmitting, and storing electronic evidence, while also maintaining the chain of regulation
	Judicial process, including statements of facts and evidence
	Types and collections of persistence data
	Types and identification methods of digital forensic data
	The specific operational impact of the cyber security vulnerability
	Should be able to:
	Collect, process, preserve, analyze, and provide computer-related evidence to mitigate network vulnerability and support investigations into crime, fraud, counter-espionage, or law enforcement

2. Detailed documentation of the skill standards

In the process of design and construction of the cyber security project involved in this competition, there are mainly the following 18 standards. The participating teams should follow the following specifications in the implementation of the competition project:

Order	Standard	Chinese standard name
1	WSC2022_WSO554_	The Professional Standards for the Cyber Security Project of the World Skills Competition
2	GB/T 22239-2019	Basic Requirements for Cyber Security Level Protection of Information Security Technology
3	GB/T 28448-2019	Evaluation Requirements for Cyber Security Level Protection of Information Security Technology
4	GB 17859-1999	Code for Security Protection Classification of Computer Information System
5	GB/T 20271-2006	Information Security Technology and Information System General Security Technology Seeking
6	GB/T 20270-2006	Information Security Technology Network Basic Security Technical Requirements

7	GB/T 20272-2006	The Security Technical Requirements for the Operating System of Information Security Technology
8	GB/T 20273-2006	Security Technical Requirements for Information Security Technology and Database Management System
9	GA/T 671-2006	Technical Requirements for Computer System of Information Security Technology
10	GB/T 20269-2006	Information Security Technology and Information System Security Management Requirements
11	ISO OSI	The OSI Open System Interconnect Reference Model
12	IEEE 802.1	A LAN overview, architecture, network management, and performance measurement
13	IEEE 802.2	Logical link control LLC
14	IEEE 802.3	CSMA / CD and physical layer Technical Specification
15	IEEE 802.6	City Area Network (Metropolitan Area Networks) MAC Media Access Control Protocol DQDB and its physical layer technical specifications
16	IEEE 802.10	LAN Security Technical Standards
17	IEEE 802.11	WLAN Media Access Control Protocol CSMA / CA and its Physical Layer Technical Specification
18	ISO/IEC 27001	The Information Security Management System

3. The event involves knowledge points and skill points

Order number	Content module	Explain
Stage I (theory)	professional quality	Network security standard consciousness, security consciousness, discipline consciousness, etc
	network security	Router, switch, firewall, log audit, intrusion detection and other security network security equipment management and security configuration; Firewall routing, security policy, NAT, VPN and other configuration and testing; Network log system network detection, statistics, alarm and other configuration; The web application of firewall protection policy, filtering policy, alarm and other configuration; Wireless management, wireless network setting, security policy and other configuration and testing; Three-layer switch routing, second-floor security and other

		configuration and testing;
	Safe operation	Windows Server system and Linux system safety operation knowledge point assessment;
	Emergency response	Operating system and application system of log analysis, vulnerability analysis, system process analysis, memory analysis, system security reinforcement, program reverse analysis, coding conversion, encryption and decryption technology, data steganography, file analysis, network traffic package analysis, mobile application analysis, code audit and other commonly used penetration and protection management knowledge assessment;
Stage II	Safe operation	**Server System Safety Operation Management:** System security operation, database security operation, Web security operation, data integrity protection, application security operation, protective wall security management, event monitoring
		Linux System Security Operation Management: System security operation, database security operation, Web security operation, data integrity protection, application security operation, protective wall security management, event monitoring
Stage III	Emergency response	**Emergency response to safety incidents:** System log analysis, process analysis, memory file analysis, Trojan virus analysis Program reverse analysis, mobile application code analysis, malicious script analysis
		Digital Forensics and Investigation: Network traffic analysis, protocol traffic analysis, file analysis and forensics Encoding conversion, encryption and decryption, and data steganography
Stage IV	CTF takes the flag	**CTF takes the flag:** Vulnerability penetration test and its security programming SQL, Injection (S Q L injection) Vulnerability penetration Test and Security Programming Command Injection (Command Injection) Vulnerability penetration test and its security programming, File Upload (file upload) Vulnerability penetration test and its security programming, Directory Traversing (directory crossing) Vulnerability Penetration Testing and Its Security Programming XSS (Cross Site Script) Vulnerability Penetration Testing and Its Security Programming for CSRF (Cross Site Request Forgeries)

		Vulnerability penetration test and its security programming Cookie Stole (Cookie theft) The Application of Artificial Intelligence in Information Security Analysis and application of log book and network traffic Application service vulnerability exploit Binary vulnerability exploitation Reverse file analysis Cryptography analysis

III. Marking scheme

（I）Methods of marking

The four stages of this competition are automatically scored by computer. The competition field should be encrypted twice, and the submitted results should be encrypted three times. Encryption referee organizes encryption work and manages encryption results. The supervisor supervises the entire encryption process.

The first group of encrypted judges: organize the competitors to draw lots for the first time, generate the entry number, replace the personal identity information, fill in the encrypted record form and the competition certificate and other personal identity information certificates, and put it into the encrypted result sealed bag for separate storage.

The second group of encryption judges: organize the competitors to draw lots for the second time, determine the competition position number, replace the competitor entry number, fill in the secondary encryption record form together with the competitor entry number, and put it into the secondary encryption result sealed bag for separate storage.

The third group of encrypted judges: encrypt the performance of each stage for the third time, and the encrypted results will be submitted to the chief referee to organize the scoring referee for scoring and summary. The third encryption process file shall be sealed and kept by the encryption referee and kept separately.

All encryption results shall be signed by the corresponding encryption referee and supervisor.

After the results of the four stages are summarized and decrypted, the referee will review and sign, and the referee confirms and sends it to the staff into the system.

（II）The code of points

1. Judgment scoring method

The on-site referee team supervises the on-site machine evaluation points, the scoring referee is responsible for the results encryption of each stage, and the chief referee is responsible for the decryption and summary of the results and the whole process of the competition.

Competition site dispatched supervisors, referees, technical support teams, etc., clear division of labor. The field referee is responsible for communicating with the competitors and sending and receiving examination papers and other materials, the confirmation of equipment problems and the field adjudication; the technical support engineer is responsible for the emergency response of all station equipment and the equipment emergency treatment confirmed by the referee.

2. Method of achievement generation

The competition is scored by task, with a full score of 1000. Detailed scoring requirements are shown in the table below.

Competition stage	Stage name	Task stage	Score method
stage I weight 10%	Professional quality and theoretical skills	Question 1... N	Machine evaluation points
stage II weight 30%	Safe operation	Task 1... N	Machine evaluation points
Stage III weight 30%	Emergency response	Task 1... N	Machine evaluation points
Stage IV weight 30%	CTF takes the flag	Task 1... N	Machine evaluation points

3. Ranking rules

The third group of encrypted judges: encrypt the performance of each stage for the third time, and the encrypted results will be submitted to the chief referee to organize the scoring referee for scoring and summary. The third encryption process file shall be sealed and kept by the encryption referee and kept separately. Summarize the results according to the four stages. According to the score ranking, if the score is the same, compared with the fourth stage score, the highest score ranked high. If the total score is the same, the fourth stage is the same, compare the score of the third stage, the top, and so on.

IV. Competition project requirements

（I）Common precautions

1. Mobile storage devices, calculators, communication tools and reference materials cannot be carried and used during the competition.

2. Please check whether the listed hardware equipment, software list and material list are complete, and whether the computer equipment can be used normally according to the competition environment provided by the competition.

3. Read all the tasks in each section before taking any action. There may be some correlation between the various tasks.

4. During the operation process, the relevant results should be timely saved according to the answer requirements. After the competition, all the equipment will be kept in operation, and the evaluation will be based on the final submission.

5. After the completion of the competition, please keep the competition equipment, software and competition questions on the seat. Do not take all the items (including test papers) used in the competition away from the competition field.

6. It is forbidden to fill in marks unrelated to the competition. If violated, it can be regarded as 0 points.

（II）Competition time arrangement and score value weight

The "Network security" competition is divided into four stages: stage 1: professional quality and theoretical skills; stage 2: network security operation stage 3: emergency response to network security incidents; stage 4: CTF flag-winning challenge.

The competition time table and score weight are shown in the following table:

Competition stage	Stage name	Race Time (minutes)	weight	Score method
Stage I	Professional quality and theoretical skills	On Day 1,90 minutes am	10%	Machine evaluation points
Stage II	Safe operation	Day 1,210 minutes pm	30%	Machine evaluation points

Stage III	Emergency response	The next morning, am 210 minutes	30%	Machine evaluation points
Stage IV	CTF takes the flag	The next afternoon pm was 210 minutes	30%	Machine evaluation points
Amount to		720 Minutes	100%	

（III）Work content and requirements of each module

The content of the competition covers network security equipment security management, post professional quality and skills, network security operation management, system security operation management, security event emergency response, CTF flag winning attack and defense, etc., comprehensively examining the comprehensive ability of the competitors in network security projects.

The first stage: professional quality and theoretical skills; the second stage: network security operation;

Stage 3: emergency response to network security incidents; stage 4: CTF flag capture challenge

Order number	**Content module**	**Assessment content description**	**Assessment form**
Stage I	Professional quality	Network security standard consciousness, security consciousness, discipline consciousness, etc	Single choice / multiple choice / judgment questions
	Network security	Router, switch, firewall, log audit, intrusion detection and other security network security equipment management and security configuration; Firewall routing, security policy, NAT, VPN and other configuration and testing; Network log system network detection, statistics, alarm and other configuration; The web application of firewall protection policy, filtering policy, alarm and other configuration; Wireless management, wireless network setting, security policy and other configuration and testing; Three-layer switch routing, second-floor security and other configuration and testing;	
	Safe operation	Windows Server system and Linux system safety operation knowledge point assessment;	

	Emergency response	Operating system and application system of log analysis, vulnerability analysis, system process analysis, memory analysis, system security reinforcement, program reverse analysis, coding conversion, encryption and decryption technology, data steganography, file analysis, network traffic package analysis, mobile application analysis, code audit and other commonly used penetration and protection management knowledge assessment;	
Stage II	Safe operation	Windows Server System Operations: Server System Safety Operation Management: System security operation, database security operation, Web security operation, data integrity protection, application security operation, protective wall security management, event monitoring	Operation questions
		Linux System Operations: Linux System Security Operation Management: System security operation, database security operation, Web security operation, data integrity protection, application security operation, protective wall security management, event monitoring	
Stage III	Emergency response	Emergency response to safety incidents: System log analysis, process analysis, memory file analysis, Trojan virus analysis Program reverse analysis, mobile application code analysis, malicious script analysis	
		Digital Forensics and Investigation: Network traffic analysis, protocol traffic analysis, file analysis and forensics Encoding conversion, encryption and decryption, and data steganography	
Stage IV	CTF takes the flag	CTF takes the flag: SQL Injection (SQL injection) Command Injection (command injection) File Upload (File upload) Directory Traversing (catalog crossing) XSS（Cross Site Script） CSRF（Cross Site Request Forgeries） Cookie Stole (Cookie theft)	

		The Application of Artificial Intelligence in Information Security Analysis and application of log book and network traffic Application service vulnerability exploit Binary vulnerability exploitation Reverse file analysis Cryptography analysis	

V. Skill Management and Communication

（I）Panel

The skill expert group consists of one chief skills expert and experts selected by various countries, who is jointly responsible for further revising the technical documents of the remote final and the daily skills management.

（II）Discussion forum

Before the competition, the questions about the software and hardware preparation, the test environment deployment and other related questions, the participants can enter the forum section of the network security competition platform for feedback. The training and exchange of this competition, before, during and after the competition, will also be carried out through the forum.

VI. Safety requirements

Please refer to the following documentation of Health, Safety and Environment Policies and norms of the Organizing Committee of the BRICS Skills Competition.

VII. Materials and equipment

（I）List of infrastructure

①. Hardware and environment equipment:

Each executive committee group will provide 3 personal computers (Windows operating system) for formation.

The operation environment of the competition provides competitors with tools and software in the process of solving problems, and instcommon application software such as Office.

Order number	Software	Introduce
1	Windows 10	operating system
2	Microsoft Office 2016/2019	Document editing tool
3	VMware 15 or above versions	Virtual Machine running environment
4	Super-terminal SecureCRT / putty	Equipment debugging and connection tool
5	Google Chrome	browser

②. Provide the penetration tester and target machine virtual machine environment:

Order number	Software	Introduce
1	Windows 7\Windows XP\Windows 10	The Windows client operating system
2	Windows Server 2003\2008\2010\2012\2016\2018	The Windows server operating system
3	Ubuntu\Debian\Kali	Penetration tester operating system
4	Linux CentOS	The Linux server operating system

③. Site hardware:

Hardware	Quantity	Specific configuration	Remarks
Network security competition platform	1	1. Can complete the competition environment of knowledge and skills such as basic theory answer, safe operation and reinforcement, security event response, network security data forensics, CTF flag winning and so on, can effectively support the scale of 600 people, and have a centralized answer environment in the same scenario based on the competition content of this regulation. 2,2. Standard with 2 Gigabit Ethernet port, Intel processor, greater than or equal to 16G of memory, SSD hard disk. Can expand a variety of virtualization platforms, support. Holding cluster management, synchronous using incremental backup way, virtualization pipe Adopt standard libvirt interface; support multi-user concurrent online competition, Automatic scheduling target machine virtualization according to different actual combat tasks issued Template, the whole process is not manually configured address, VLAN and IP can be	

		determined according to the competition The competition is required to be set by itself; 3. Provide four-stage competition mode: theoretical answer, safe operation, emergency response and CTF flag winning, the system provides 500 + theoretical question bank, 50 + safe operation, emergency response, CTF flag winning scenarios; support situation display; stage can conduct detailed data export, average score, accuracy, answer, task score data statistical display; wrong question analysis: display TOP5, task error rate, task accuracy and other information.	
Exchange board	Several	Provide network management for the PC of the participating teams	Depending on the number of teams
Banners or large screens	1	CCVR 2022 * * * Branch Competition field " (* * * is the full name of the school)	
Spare parts	Several	Computer, camera, U disk, etc	The station hardware damage inside the site can be replaced at any time
supervisory control	1	Mobile phone or video recorder	The game was recorded throughout
Computer or mobile phone	1	Zoom meeting	For liaison with the main arena

④.Line configuration:

Project	Specific configuration
Network configuration	(Online games can be connected online, while offline games do not support networking) Station computers all support the Internet connection, the bandwidth is greater than 4M

（II）Suggested site and station layout

1. Test position layout requirements

(1) The competition site is full of light and good lighting; the power supply facilities are normal and safe; the site is clean and tidy.

(2) The competition venue shall be set up with isolation belts, and non-referees, competitors and staff are not allowed to enter the competition venue.

(3) There are security, fire, medical and equipment maintenance on standby to prevent emergencies.

(4) Safety channels and warning lines are set up in the competition field to ensure that the visitors, interviews and inspectors of the competition field are limited to the safe area to ensure the safe and orderly conduct of the competition.

2. Arrangement requirements of mobile monitoring equipment

The center line of the mobile monitoring equipment 1 requires a 45° away with the game operation display plane, which can monitor the game operation display and the side face of the competitors. The monitoring distance can monitor the range of 1 meter around the test site and a height of about 1.5 meters.

The mobile monitoring device 2 is placed on the test table, and its center line is about 45° away from the game operation display plane, which is required to maximize the complete display game screen (the display game screen can fill the mobile monitoring device as much as possible)